Document Title:	Examining the Creation, Distribution, and Function of Malware On-Line
Author:	Bill Chu, Ph.D., Thomas J. Holt, Ph.D., Gail Joon Ahn, Ph.D.
Document No.:	230111
Date Received:	March 2010
Award Number:	2007-IJ-CX-0018

Examining the Creation, Distribution, and Function of Malware On-Line

Award Number: 2007-IJ-CX-0018

Bill Chu, Ph. D.

The University of North Carolina at Charlotte

Thomas J. Holt, Ph. D.

Michigan State University

Gail Joon Ahn, Ph. D.

Arizona State University

This document is a research report submitted to the U. S. Department of Justice. Opinions or points of view expressed are those of the authors and do not reflect the official position or policies of the U. S. Department of Justice.

Abstract

The global adoption of the Internet and World Wide Web has engendered the growth of significant threats from computer criminals around the world. Computer crimes are costly, and many appear to be perpetrated by computer hackers in foreign countries, particularly Russia and Eastern Europe. These attackers often use malicious software, or malware, to automate attacks and enable multiple forms of cybercrime. Recently, a great deal of attention has been given to a new form of malware used by computer hackers called bots. This malware essentially takes over an infected computer, allowing it to receive commands remotely. Bots are also bought and sold in virtual markets operating out of Russia. Researchers have, however, only begun to explore the prevalence and origins of this form of malware and its potential as an attack tool. Thus, this study examined the social and technical aspects surrounding the creation, distribution, and use of bots through both a criminological and computer science examination of bots and malware.

Specifically, 13 bots were captured in the wild and analyzed using honeynet technologies to determine their utility and function in a simulated computing environment. The findings suggest that these bots had a significant impact on system functionality by changing system protocols, including adding and removing files. The bots also attempted to connect to command and control IRC servers around the world, though the majority appeared to reside in the United States. Five of the bots were able to connect to a command and control channel and received commands to scan other systems online, participate in Denial of Service Attacks, infect another system, and open communication sessions with other computers.

The creation and sale of bots and malware in the on-line black market were also examined using a sample of 909 threads collected from 10 publicly accessible web-forums in Eastern Europe and Russia. The findings suggest that a service economy has developed around

the spread of bots, including distributed denial of service attack providers, spam distribution, and bulletproof web hosting. Malware is also available through these forums, such as trojan horse programs, encryption tools, and iframe malware uploading and downloading services. Credit card and identity documents were also readily available, along with hijacked ICQ numbers.

In order to better understand the social dynamics of this market, the normative orders of this community were explored using grounded theory methodology. The results suggest that three interrelated norms shape the relationships between buyers and sellers: price, customer service, and trust. Price is critical as the cost of goods affect the likelihood that an individual would be able to compete in the market. Customer service reflects the quality of products available, discounts for volume purchases, and real time support to their customers. Finally, trust refers to the lack of regulation within the markets, increasing the risk of engaging in a purchase with a vendor. Individuals who demonstrate that they were trustworthy could gain clients, while those who attempt to cheat other actors were publicly derided.

As a whole, this study demonstrates the key role that bots and other malicious software play in the facilitation of cybercrime across the globe. Bots have various utility in the wild, and receive commands from IRC channels around the globe. Though malicious software takes some skill to create, the forums examined demonstrate that bot masters generate a profit from their infrastructure by selling access to attack services that enables hackers of any skill to participate in attacks ranging from Distributed Denial of Service attacks to spam. Thus, there is a significant need to disrupt botnets and the markets that facilitate the distribution of malware and hack tools.

Table of Contents

Executive Summary

The Internet and World Wide Web have dramatically changed the way people communicate and do business around the world. These changes have far reaching consequences, affecting business, banks, government, and home computer users. As a result of the growth and penetration of computer technology, the threat posed by computer criminals has become increasingly significant. Computer crimes are costly, and many appear to be perpetrated by computer hackers in foreign countries, particularly Russia and Eastern Europe. These attackers often use malicious software programs, or malware, that automate a variety of attacks and enable different criminal acts.

Recently, a great deal of attention has been given to a new form of malicious code used by computer hackers and attackers called bots. Technical analyses of bots indicate that they operate around the world and can be used to facilitate all manner of computer and cybercrime. Thus, they pose a serious threat to government, businesses, and computer users around the globe. Furthermore, a small body of research suggests that bots and services generated from bots can be purchased in open markets operating on Internet Relay Chat channels in Russia and Eastern Europe. Researchers have, however, only begun to explore the prevalence and origins of this form of malware and its potential as an attack tool. In addition, few studies have considered how web forums may facilitate the sale and trade of bots and other malware. This study examined the social and technical aspects surrounding the creation, distribution, and use of bots through a criminological and computer science examination of multiple data sets.

Specifically, 13 bots were collected in the wild using a tool called MWCollect that can capture the binary of the malware. Once obtained, each program was analyzed using honeynet technologies to determine their functionality and activity in a simulated computing environment.

The findings suggest that these bots had significant impacts on the system by changing system protocols, including adding and removing files, dlls, and registry information. Two of these bots also attempted to download other executable programs hosted on other websites, including a compromised server hosting a legitimate business website in the United States. All of the bots attempted to connect to Internet Relay Chat (IRC) command and control servers around the world, including Hungary, Malaysia, and China. The majority of command and control servers, however, operated in the United States. Nine of these bots were able to connect to the IRC command and control channel, and four required a password to log in to the channel. Five of the bots were able to connect to the channel and received commands to scan other systems online, participate in Denial of Service Attacks, infect other systems, and open communication sessions with other computers. Thus, only some of the bots were active, but they appeared to serve a variety of functions by botmasters in the wild.

The creation and sale of bots and malware were also explored through a qualitative examination 909 threads from 10 publicly accessible web-forums in Eastern Europe and Russia designed to facilitate the creation, sale, and purchase of malware and hacking. The content of these forums were translated from Russian to English using a certified translator and native speaker, and analyzed by hand using grounded theory methodology. The findings demonstrate that these forums act as advertising spaces where individuals could either sell or seek out various resources related to cybercrime or on-line deviance. Individuals would create a thread and list their products or request various items, indicating the cost of a good or service, preferred payment method, and contact information. Most individuals preferred to communicate via ICQ, which is an instant messaging protocol, though some provided email addresses or accepted private messages through the forum's internal communication system. Payments were accepted through electronic systems such as WebMoney or Yandex, as they allow the immediate transfer of funds between individual accounts.

Examining the ads posted in these forums demonstrated that a service economy has developed to facilitate cybercrime, particularly in the sale of malware. Malware was the most prevalent item sold in these forums, comprising 34 percent of the total sales related threads. Individuals actively requested or sold bots, trojan horse programs, encryption tools, and iframe malware uploading and downloading services. Trojans were the most prevalent item sold, at an estimated average price of $742.59 per item.

Unique cybercrime services composed the second largest resource sold, consisting of 30 percent of the market. Individuals sold distributed denial of service attack services, spam creation and distribution resources, and bulletproof web hosting for malicious content. Additionally, individuals could hire out hacking services to compromise emails and servers, and obtain access to VPN and proxy networks. Most of these services depended on botnets to function, particularly spam distribution, DDoS services, and proxy providers. Additionally, these services were relatively inexpensive, as the average cost of a DDoS attack was $14.26 and spam distribution services were an average of $50.91.

Stolen data comprised the third resource available in these forums, at 13 percent of the overall market. For example, individuals sold malware log files containing sensitive information from victim computers, such as usernames, passwords, and account information. Fraudulently obtained on-line accounts were also sold, including PayPal and Internet casino accounts at an average of $156.79 per account. Credit card numbers were also readily available, and sold in bulk lots at an average price of $10.66 per card. Individuals also offered scanned passports and other identity documents to engage in fraud in the real world. The fourth resource sold were hijacked ICQ numbers that could be obtained in a range of numbers at an average cost of $4.44 per number. Finally, 13 percent of the products sold were gray market items such as video game accounts and other services.

A range of older variants of malicious software were also posted for free in several of the forums, enabling access to sophisticated attack tools at no cost to the individual. These tools affected the price and sale of certain malware in the market, as individuals who sold otherwise free resources were derided by others. Free software were, however, sometimes incomplete, and infected with some form of malware. Thus, individuals had to exercise caution should they attempt to utilize these tools.

In order to understand the social dynamics of this market, the normative orders of this community were explored using grounded theory methodology. The results suggest that three interrelated norms shape the relationships between buyers and sellers: price, customer service, and trust. Price refers to the cost of goods that affect the likelihood that an individual would be able to compete in the market. The importance of customer service reflects the notion that respected sellers had high quality products, gave special discounts, and real time support to their customers and maintain a strong presence in the market. Finally, trust is a key component of the market based on the lack of regulation between participants, increasing the risk of engaging in a purchase from a vendor. Those individuals who demonstrate that they are trustworthy were more likely to gain clients, while those who attempt to cheat other actors were publicly derided.

The analysis of bots presented supports the notion that botnet command and control channels have particularly short life spans, as only five of the channels sent requests to the infected image. Furthermore, since the majority of the bots in this sample attempted to connect to IRC channels in the United States there is a need for careful monitoring of websites and servers for malicious traffic. Such measures may be one way to effectively reduce botnet traffic in the wild. Additionally, the ways that the bots in this sample were used support the notion that bots have significant utility for cybercrimes, whether to infect other systems or surreptitiously collect information on other systems on the same network as the zombie node.

The findings of the qualitative portion of this study suggest that a wide range of tools and services are available and sold for profit in a market environment that encourages and supports a variety of cybercrime. Individuals could procure spam, DDoS attack services, iframe exploit infections, web hosting, and proxy services for low costs from the forums in this sample. Credit cards, bank account information, and sensitive personal information were also sold in bulk lots at variable prices. Finally, free tools were readily available though not necessarily fully functional when downloaded.

As a whole, the products sold and normative orders of this market suggest that buyers need little technical knowledge in order to access or utilize these resources. As a consequence, these forums simplify and engender identity theft and computer-based financial crimes. At the same time, forum exchanges were largely unregulated, and participants engaged in transactions at their own risk. The normative orders that structure relationships between buyers and sellers in these forums also emphasized the lack of formal controls over actor behavior. Price, customer service, and trust affect the likelihood that an individual may purchase goods from a seller, but do not eliminate the risk or likelihood of loss. Thus, these markets operate in much the same way as real world criminal markets, like prostitution, drug sales, and stolen goods.

The combined findings of this study emphasize the significant threat that botnets play in cybercrime. Compromised, or zombie nodes are spread out globally and the infections may not be easily identified by end users. Bot masters can utilize their infrastructure to engage in a variety of attacks, and offered their services to engage in cybercrime for profit. They are, however, part of a wider spectrum of malware, as noted in the threads from the forums examined in this study. As a result, any attempt to effectively reduce or impact the creation and use of botnets specifically, and cybercrime generally, will require a combination of both technological solutions and traditional policing practices. In fact, principals of situational crime prevention and intelligence-led policing may be useful in affecting cybercrime.

For example, actively collecting and running malware in an emulated computing environment like a honeynet can enable law enforcement agencies to understand the scope and nature of an active botnet in the wild. The information generated from such an analysis includes tactical information such as the location of a command and control server. If the server is hosted in the U.S., federal law enforcement agencies can notify the owner and request the server be shut down, or monitor the channel to gather further information. This sort of information gathering could prove invaluable to develop cases against bot masters, and potentially successful prosecutions given the number of channels hosted in the U.S.

The forums identified in this study also provide a platform for botherders to lease their botnets for various services. Thus, it is critical that these forums play a key role in active law enforcement investigations. In addition, the participants and exchanges observed suggest that cybercrime markets are structured much like real world drug and stolen goods markets. Many of the same policing strategies used to deal with these offenses may be employed to investigate, disrupt, and reduce their presence on-line. For example, the market forces and structures identified in this study can be used as a roadmap for federal law enforcement to infiltrate the market with reduced likelihood of detection. Undercover agents can create fictitious identities and use these covers to register in multiple forums. In turn, using the findings of this study, agents can more rapidly conform to the behaviors and processes of the market to identify key buyers and sellers and gather information on active offenders through participation in these forums. This will facilitate the collection of actionable intelligence, and develop profiles of key buyers and sellers.

The data generated from these investigations can also be used to conduct stings affecting both buyers and sellers in these markets. Undercover agents can purchase a good or service from a seller and use this as a means to build a case against the individual and any of their known associates. Arrests of single individuals in street crimes, however, appear to have little impact on the operations of open air markets due to the freelance nature of sales and the range of available locations to sell products. If this principal is applied to cybercrime markets, then the arresting agency may be better served using any potential charges as a means to encourage cooperation on the part of the offender in order to create a larger case against multiple sellers in a single forum, or across multiple sites. This would facilitate a larger impact on the supply side of the cybercrime market than may otherwise be observed with single arrests.

There may also be some practicality in attempting to disrupt these markets through surreptitious use of the social processes that undergird the forums. In particular, trust between participants is critical to establish an individual's reputation, and maintain customers. When an individual is accused of cheating, the exchanges can become heated and lead to disruption and reduced social cohesion. Undercover agents operating under false identities in the forums could make comments about the quality of a product or a seller's actions. Posting bad reviews could affect a seller's reputation and, if repeated often, may lead to mistrust among participants and network disruption. Such a measure may prove useful in affecting the organization and relationships that undergird the cybercrime market.

All of these investigative techniques outlined above require a significant financial investment in federal law enforcement resources. It is imperative that financial resources be allocated to the Secret Service, Federal Bureau of Investigation, and other federal agencies that combat the problem of cybercrime. For example, the language barriers identified in the cybercrime markets indicate the need for language training and translation services to properly investigate websites and forum content. Additionally, funds are needed to engage in undercover purchases of malicious software and hacking services to build cases against cybercriminals. The computer and communications technology necessary to properly investigate cybercrimes also requires significant financial investment. Thus, greater financial investments must be made at the federal level to improve our capacity to investigate cybercrimes.

There is also a need for increased international collaboration in law enforcement agencies to improve the response to cybercrime. The use of the Russian language in all of these forums, coupled with the presence of job postings for positions in Russia and Eastern Europe, suggests that the participants are either living in Russia or Russian speaking individuals living abroad. In addition, several web hosting providers noted that their servers resided in Malaysia or other parts of Asia. The varied locations of command and control servers in the botnet analyses also indicate the global spread of botnets. As a result, it is necessary that the Department of Justice and other law enforcement agencies carefully consider and develop improved extradition treaties and frameworks to ensure cooperation across agencies, such as the Russian FSB and other federal law enforcement agencies around the world.

Another important policy implication is the need for more stringent legal frameworks to prosecute the creators of malicious software and individuals who sell access to these tools. There are several laws in the United States pertaining to computer intrusions, identity theft, spam distribution, and intellectual property theft. The existing statutes do not, however, provide punitive sanctions for the sale of malicious software, or of identity information. Developing statutes that clearly elaborate these actions as illegal can improve the ability of law enforcement and prosecutors to build cases targeting these actors. In turn, this may help to increase the risks of cybercrime for actors and improve the power of federal prosecutors to pursue cybercrime investigations.

Finally, the victims of malicious software play an important role in the prevention of cybercrime. Zombie machines in botnets, as well as those who experience malicious software infections facilitate a variety of cybercrimes. Individual computer users and system administrators must take care to act as place mangers to prevent infection and protect their machines. This is challenging given the limited knowledge of computer security principals among home users, and the responsibilities of administrators and security personnel within corporate settings. Steps must be taken to increase awareness among home users on the potential vectors for infection and the importance of owning, updating, and regularly using protective software. Increased collaboration between law enforcement agencies and private industry is also needed to improve awareness of the corporate response to infection and attacks. In turn, this can help to destabilize botnets and the platforms that engender spam and identity theft.

I. Introduction

The Internet and World Wide Web have dramatically changed the way people communicate and do business around the world (see Furnell 2002; Jewkes and Sharpe 2003; Wall 2001). These changes have far reaching consequences, affecting many facets of modern life. Businesses depend on the Internet to draw in commerce and make information available on demand. Banking and financial industries have implemented new technology enabling customers to gain access to their funds and accounts with relative ease. Home computer users around the globe can now use this technology around the clock with home-based high-speed dedicated Internet access regardless of their familiarity and skill with computers.

As a result of the growth and penetration of computer technology, the threat posed by computer criminals has become increasingly significant. In fact, the number of computer security incidents reported to the US Computer Emergency Response Team (CERT) has grown in tandem with the number of individuals connected to the Internet (Longstaff et al. 1997). Data from CERTs around the world also suggest that the number of computer attacks have increased significantly since 2001 (Holt 2003). Computer crimes are also costly, as US businesses incurred an average of loss of $289,000 per security incident in 2008 alone (Computer Security Institute 2009). Many of these attacks appear to be perpetrated by computer hackers in foreign countries, particularly Russia and Eastern Europe (Denning 2001; Taylor, Caeti, Loper, Fritsch, and Liederbach 2006). Often, their intrusions are completed through the use of malicious programs, or malware, that automate a variety of attacks (Denning 2001; Furnell 2002). Malware constitutes a computer-focused crime, as they are generated by and function solely on computer networks with no real world parallel (Wall 2001). These programs can cause a significant amount of damage to computer networks, such as the Melissa virus which infected computers worldwide causing at least $80 million in damages (Taylor et al. 2006). In addition, new variations and types of malware are being constantly created and identified every day (Symantec Corporation 2003; Taylor et al. 2006).

One of the most prominent and damaging types of malware presently functioning on-line are bots which enable an attacker to compromise and infect multiple computers at once (Bacher, Holz, Kotter, and Wicherski 2005; Cooke and McPherson 2005; Ianelli and Hackworth 2005; Rajab, Zarfoss, Monrose, and Terzis 2006; Symantec Corporation 2003). Bots are distributed by hackers through trojan horse programs or other methods to infect a computer system. Once a machine is infected, the code then installs a bot program, making the machine a “zombie” (Bacher et al. 2005; Cooke and McPherson 2005). This means that the computer can now receive commands and be controlled by another user through Internet Relay Chat (IRC) channels, which are a type of real time communication enabled over the Internet (Bacher et al. 2005; Cooke and McPherson 2005; Ianelli and Hackworth 2005; Rajab et al. 2006). The infected machine then surreptitiously contacts a pre-programmed IRC channel to wait for commands from the bot operator. Multiple machines that are infected with this malware will contact the channel, creating a botnet, or network of zombie machines (Bacher et al. 2005; Cooke and McPherson 2005; Rajab et al. 2006).

The spread of bot malware can enable its operator to engage in a wide range of cybercrimes, including the distribution of spam, phishing, and secondary malware distribution (Bacher et al. 2005; Choo 2007; Ianelli and Hackworth 2005; James 2005; Keizer 2005; Wall 2007). Botnets can also be used to perform Distributed Denial of Service (DDoS) attacks, where each computer in the network attempts to contact a computer or server (Bacher et al. 2005; Taylor et al. 2006). The target system becomes flooded with requests and cannot handle the volume, resulting in a loss of services to users. This is an extremely costly form of cybercrime for companies, as they can lose millions of dollars in revenue if customers cannot access their services (Computer Security Institute 2009).

Evidence suggests the number of nodes in a botnet can reach hundreds of thousands of machines depending on the operator (Cooke and McPherson 2005; Dagon, Zou, and Lee 2006). In fact, a 20 year old hacker was recently arrested by the Federal Bureau of Investigation for maintaining a botnet with over 100,000 nodes (Goodin 2008). Due to the spread of infections, zombie nodes appear to exist in multiple time zones across the world (Dagon et al. 2006). The size of a botnet is critical, as the number of machines constitute a force multiplier for computer attackers to leverage the power of thousands of systems to their needs (Bacher et al. 2005; Choo 2007). At the same time, they allow attackers to conceal their identities behind common computer users who may be unaware that their machines are involved in cybercrime incidents.

Taken as a whole, bots constitute a significant threat to computer users around the globe. In fact, bot infections in corporate environments cost an average of $345,600 per respondent in 2008 alone (Computer Security Institute 2009). While there is some knowledge on the ways that bots are developed and operate, there is little research exploring the ways that bots are created and their role within the attack resources of computer attackers. A recent study suggests that access to existing botnets are sold in on-line black markets operating on IRC (Bacher et al. 2005; Franklin, Paxson, Perrig, and Savage 2007; Thomas and Martin 2006). Many of these markets operate out of Eastern Europe and Russia, and allow skilled programmers to create and profit from the sale of new malicious code (Franklin et al. 2007; Thomas and Martin 2006). Individuals sell access to their infected machines for a variety of attacks including spam and

DDoS attacks (Bacher et al. 2005; Thomas and Martin 2006). As a consequence, these markets enable a great deal of unskilled computer users to engage in cybercrime.

Few researchers in the academic community have, however, attempted to systematically examine the creation, distribution, and attack functions of bots circulating on-line. This information is vital to improve law enforcement and computer security responses to this threat, though it requires a combination of social and computer science research. Thus, this study examines the problem of bots and their role in the active hacker community through two examinations. The first involves a technical analysis of bots using a tool called MW Collect to capture bots that are active in the wild. Then, this malware was run in a honeynet which provides a simulated environment to determine their attack potential and methods. This data considers the functionality of active bots in the wild. In addition, a qualitative analysis was conducted with a series of threads from publicly accessible web forums that facilitate the creation, sale, and exchange of malware and bots. This data examines the role that bots play in facilitating various cybercrimes and the utility of bots relative tools and tactics in the hacker community. These two examinations provide significant insights on the methods and tactics of bot masters, malware writers, and cybercrime in general.

Botnet Functionality and Use

In order to understand the botnet threat, it is necessary to consider their place within the larger spectrum of malicious software. There are a variety of malware used by computer hackers and criminals around the globe. For example, trojan horse programs are used by computer attackers to distribute and conceal malicious code (Furnell 2002). The program is disguised as some type of file or product that individuals would want to open. Once activated, the program executes some form of malicious code, such as a virus. Viruses are programs written by individuals that modify programs or systems to perform various malicious functions (Kapersky 2003; Taylor et al. 2006). These programs can conceal their presence on computer systems and networks and may be able to propagate themselves. Worms, however, do not involve as much user interaction as other malware because of its ability to use system memory and self-replicate (Nazario 2003). Specifically, worms can spread across computer networks by utilizing system memory to send copies of malcode to other systems that have a flaw allowing the code to activate. Humans can also facilitate worm spread by also simply opening e-mails that have the worm code embedded in the file (Nazario 2003).

These primary forms of malicious code have also been combined into one form of malware called “blended threats” (Chien and Szor 2002; Gordon 2003; Taylor et al. 2006). The use of blended threats by computer attackers has increased over the past few years, particularly bots which enable an attacker to compromise and infect multiple computers at once (Symantec Corporation 2003; Bacher et al. 2005). Initially, bot programs were created to act as an automated agent for a user or program in order to simplify processes and actions (Choo 2007; Rajab et al. 2006). Bot programs were designed primarily to manage Internet Relay Chat (IRC) channel processes, such as generate automatic responses or block and remove actors from the channel (Choo 2007). The functionality of bot programs were then co-opted by computer hackers and exploited as a means to attack IRC channels (Choo 2007; Rajab et al. 2006). Subsequently, they were combined with other forms of malicious software, such as trojan horse and worm programs to facilitate distribution and exploitation of vulnerabilities to attack systems globally (Choo 2007; Rajab et al. 2006).

Bot malware is delivered by hackers through a variety of mechanisms, most notably e-mail attachments, infections via web browser exploits or through peer to peer file sharing networks (see Bacher et al. 2005; Choo 2007; Cooke and McPherson 2005). In some instances, bot programs can also be installed through existing malware infections that provide backdoor access to a victim machine (Choo 2007). Once the code is executed, the machine runs a shellcode script that downloads and installs the bot program (see Bacher et al. 2005; Rajab et al. 2006).

The likelihood of infection can depend, in part, on the use of protective software programs to reduce attacks against networked systems, such as firewalls, intrusion detection systems, and anti-virus programs that detect and quarantine malicious software (PandaLabs 2007; Symantec Corporation 2003). For example, Sophos (2006) demonstrated that an unprotected computer would have a 50 percent chance of becoming a zombie node of a botnet within 30 minutes of being connected to the Internet. The value of protective software is, however, moderated by the frequency with which they are updated and utilized. Recent studies on malicious software indicate that security measures to prevent attacks may not be truly effective (see PandaLabs 2007). Almost 25 percent of personal computers around the world that use a variety of security solutions have malicious software loaded into their memory, compared with 33.28 percent of unprotected systems (PandaLabs 2007). As a result, many computers and individuals can be victimized despite the presence and use of antivirus and other protective software programs.

The issue of protective software failure has particular salience for bot malware as they can be packed, or compressed and hidden, to obviate detection by antivirus products (Choo 2007). Bot code can also be configured to disable protective software and patch the system to reduce the likelihood that the machine will be further compromised by another hacker (Choo 2007; Dagon et al. 2007; Stewart 2006). Additionally, bot programs can be automatically updated remotely by a bot master through a command and control, or C&C, system (Bacher et al.

2005; Choo 2007; Dagon et al. 2007; Karasaridis, Rexroad, and Hoeflin 2007; Rajab et al. 2006). The most commonly identified C&C method for botnets appears to be via an IRC channel hosted on a compromised server that has been manipulated to reduce detection from administrators and zombie nodes (Houle and Weaver 2001; Rajab et al. 2006). This may be due to the fact that IRC was designed for rapid data dissemination directly across a wide number of machines. Thus, bot masters can control a large number of infected systems through IRC with much more ease than through other methods (see Dagon et al. 2007; Rajab et al. 2006).

Once a machine is infected with bot malware, the zombie nodes contact the C&C through a server address provided in the executable file of the bot binary (see Bacher et al. 2005; Rajab et al. 2006). The victim machine then identifies the IP address of the server, and attempts to connect to the IRC channel. Bot masters may also utilize an authentication system, such as a password, to limit other hackers from gaining access to their botnet (Rajab et al. 2006; Karasaridis et al. 2007). Additionally, botnets appear to move the location of their C&Cs frequently, as noted by Karasaridis, Rexroad, and Hoeflin (2007) who found that botnets spent an average of two to three days in a single location.

If the victim machine is able to connect to the C&C channel, it will then execute any command issued. Bots typically receive scanning commands to search for other machines on the victim subnet, as well as data mining commands to identify information about the victim machine (see Rajab et al. 2006). Download requests are also common, as a means to install other malicious software or updates to the victim machines (Rajab et al. 2006). A small percentage of botnets also receive attack commands, most notably flooding other systems to engage in Distributed Denial of Service attacks (Bacher et al. 2005; Dagon et al. 2007; Rajab et al. 2006). Spam is also regularly distributed through botnets, due in part to their ability to conceal the location and identity of the sender (Collins et al. 2007). For example, a study by Mathieson (2006) found that 70 percent of spam related to penny stocks and other fraudulent information was distributed via a botnet.

Zombie nodes within a botnet can also serve as proxies or launch points for a variety of attacks, as the bot master can direct a variety of traffic through any computers in the network (Rajab et al. 2006). Bot networks can also be used to host phishing sites and validate credit card numbers, though this appears to account for a small percentage of actual bot use in the wild (Bacher et al. 2005; James 2005; Rajab et al. 2006). Finally, botnets can be used to rapidly distribute new viruses and malware across the Internet (Bacher et al. 2005; Choo 2007; Collins et al. 2007; Provos, Mavrommatis, Rajab, and Monrose 2008; Rajab et al. 2006).

Malicious Software and Stolen Data Markets

In light of the significant utility and spread of botnets, it is critical to understand how and why hackers create and gain access to these tools. Explorations of the hacker community indicate that hackers exist within a subculture that values profound and deep connections to technology (Furnell 2002; Holt 2007; Holt, Soles, and Leslie 2008; Jordan and Taylor 1998; Taylor 1999). This subculture is also a meritocracy where others are judged based on their capacity to utilize computers in unique and innovative ways (Holt 2007; Holt et al. 2008; The Honeynet Project 2001; Jordan and Taylor 1998; Taylor 1999; Thomas 2002). Research suggests they are driven by a variety of motives, particularly status, ego, cause, entre into social groups (see Gordon 2000; Gordon and Ma 2003; Holt 2007; The Honeynet Project 2001; Jordan and Taylor 1998; Taylor 1999; Wall 2007) and most notably economic gain (Furnell 2002; Gordon and Ma 2003; The Honeynet Project 2001; James 2005). Hackers also have shifting ethical beliefs of hackers concerning the consequences of their actions, as demonstrated by their willingness to share hacking tools and sensitive or fraudulently obtained information in public outlets on-line (Furnell 2002; Holt 2007; Holt and Kilger 2008; Holt et al. 2008; Jordan and Taylor 1998). Thus, developing and releasing a highly functional program like a bot is a sensible act for a hacker as they may gain respect and status among their peers, and some recognize they may be able to capitalize on their skills to generate a profit.

To that end, there is growing evidence that a marketplace has developed, particularly in Internet Relay Chat (IRC) channels, for stolen data, malicious software, and phishing resources to be sold (Franklin et al. 2007; Honeynet Research Alliance 2003; Thomas and Martin 2006). Specifically, the channels allow hackers to sell or request credit card numbers and financial information obtained through phishing, database compromises, and other means. Research suggests hackers sold credit card and bank accounts, pin numbers, and supporting customer information obtained from victims around the world in lots of tens or hundreds of accounts (Franklin et al. 2007; Honeynet Research Alliance 2003; Thomas and Martin 2006). Individuals also offered cash out services to obtain funds from electronic accounts, as well as checking services to validate accounts and their available balances (see Franklin et al. 2007; Honeynet Research Alliance 2003; Thomas and Martin 2006). Spam and phishing related services were also available in IRC channels, such as bulk e-mail lists to use for spamming and email injection services to facilitate responses from victims. Some sellers also offered spam distribution and Distributed Denial of Service (DDoS) services, as well as web hosting on compromised servers (see Franklin et al. 2007; Honeynet Research Alliance 2003; Thomas and Martin 2006).

The development of these markets facilitates cybercrime by making technical or complex attacks available as a paid service (Franklin et al. 2007; Honeynet Research Alliance 2003; Thomas and Martin 2006). The channels are, however, risky as individuals may not receive the products that they pay for, or obtain invalid or useless data. As a result, IRC markets attempt to identify trustworthy participants, and refer to sellers who demonstrate honesty and reliable products as "verified sellers" (Franklin et al. 2007). Participants in these markets regularly lose funds from dishonest sellers who conduct fraudulent transactions. These sellers are referred to as rippers, as a reflection of the fact that their activities "rip off" customers (Franklin et al. 2007). Beyond these labels, there appear to be few internal regulatory mechanisms for participants in these channels. As a result, they may be vulnerable to certain methods of destabilization, such as using complaints against sellers as a means to sew distrust between participants (see Franklin et al. 2007).

Though these studies emphasize that there is a burgeoning marketplace for hackers to dispose of information obtained through compromises, few have considered the products, structure and content of markets that operate outside of IRC channels, and what commonalities exist across these settings. For example, web forums operate throughout Russia and Eastern Europe as a means for hackers to connect with others and obtain goods and services to facilitate hacking (see Basher et al. 2005; Holt et al. 2008; Taylor et al. 2006). In order to understand the role that forums play in the creation, distribution, and sale of bots and malicious software, this study utilized a qualitative analysis of 909 threads from 10 active web forums in Russia and Eastern Europe that are involved in the creation, sale, and distribution of malicious software. The findings provide insights on the resources and information available, as well as the cost of goods and services in these markets. Additionally, this study considers the social dynamics that shape relationships between buyers and sellers in these forums.

Rationale for Research

Taken as a whole, it is clear that bots play an important role in the facilitation of cybercrimes. The creation and distribution of these tools appears to be driven by an economic imperative among hackers. There is, however, a need for further research to systematically examine the technical and social dynamics that drive the creation, distribution, and use of bots and malware. Exploring this phenomenon in tandem can clearly elaborate the motives and utility of bots and malware creators and users. Additionally, the findings can illustrate the economic and personal risks that computer users around the world face from this problem, as well as improve the law enforcement and computer security policy and response. This study utilizes both information technology and criminological research methods to examine the social and technical aspects of bots. First, a technical analysis of 13 bots gathered in the wild is examined to understand their attack potential and methods. This data provides information on the functionality of active bots, and their utility for cybercrime.

In addition, a qualitative analysis of threads from 10 publicly accessible web forums that facilitate the creation, sale, and exchange of bots, malware, and stolen data was conducted. This research examines the prevalence and cost of malicious software, hacking services, and stolen data in the market, as well as the exchange of information and free programs that engender cybercrimes. Furthermore, this study considers the social dynamics and subcultural norms that shape the relationships between actors within this environment. The findings improve our knowledge of the utility of bots and other malware to compromise computers and engage in a variety of cybercrimes across the world. The results from both analyses are used to develop strategies to reduce the prevalence and incidence of cybercrime.

II. Methods

The technical and social research processes used in this study provide a thorough and comprehensive examination of bots in order to improve our understanding of this unique and increasingly significant form of computer attacks. Each method is discussed in detail below.

BOT ANALYSES

The technical component of this project utilized the honeynet testbed located at the University of North Carolina at Charlotte as it provided a real world environment to perform various network security related activities (see The Honeynet Project 2001). A variety of open source tools and techniques were used to analyze bots and their malicious traffic. This involved a four stage process beginning with bot collection, then a closed environment traffic analysis to initially examine the bot, and finally open environment traffic analyses to determine how the bot interacts with other live computers on the Internet.

Tools Used in Architecture

In order to understand the techniques of this analysis, it is necessary to consider the tools used in this research. The primary tools used to obtain bots for this analysis were Nepenthes and the Mwcollect alliance collection tool. Nepenthes is a low interaction honeypot that captures bots and other malware by emulating vulnerabilities. When an attacker scans for vulnerability, Nepenthes will trick them into thinking they have discovered a real machine on a network with a real vulnerability (Bacher et al. 2005). Once the malware is downloaded on the machine, it is saved and not executed. The Mwcollect Alliance tool was developed and is managed by the German Honeynet Team and is a central collection place for malware. Most of the malware was collected using Nepenthes and is uploaded either automatically or manually to the collection server. Currently there are over 20,000 instances of malware from all over the world on this server.

The Truman Sandnet was then used to run malware in a closed environment. The sandnet is comprised of a Linux server and a Windows client. The Linux server has fake servers to emulate the Internet. It records traffic associated with each binary and has a queue where malware can be loaded and ran in a first come first serve manner. The Windows client is booted by the Linux server's emulated network and it runs the malware that is in the Linux server's queue. Each run takes about 30 minutes and after it runs the packet capture data is stored on the system for further analysis.

The open environment traffic analysis was performed on our implementation of a honeypot with a monitoring device called a honeywall (The Honeynet Project 2003). The honeywall records all network traffic in and out of the honeynet network. All traffic out of the network is considered malicious since no one should be using the machines inside the honeynet. Mechanisms are also in place to thwart any significant involvement in a network attack from the honeynet environment. Thus, this resource allows a bot to connect to the larger network and receive commands from the bot master, but not participate in any actual attack.

The honeypot used a Windows XP Service Pack 1 image, as this is a relatively vulnerable system to attack. This image could be removed and reinstalled with minimal difficulty on the part of the research team. A number of other software tools were used in the analysis to examine the infected windows image and potential network traffic created by the bot. Sebek was used as a key logger for the image the bot was being ran on. Sebek is able to capture the processes used by the bot, such as svchost.exe, ftp.exe or cmd.exe. The program Perileyez was used to provide an md5sum of the image before and after running the bot. The bot was allowed to run for five to ten minutes before taking the final Perlieyez image. This information allowed the researchers to identify any processes, services, and ports affected by the bot. Wireshark was used to analyze the network packets generated by the bot. InstallWatch was also run on the image as a back-up if Sebek happened to fail, as this tool generates reports that show programs installed and changes to the registry. Finally, two anti-virus engines were also used to help classify the bots captured. Specifically, Norton 10 Corporate and ClamAV software were used as a means of triangulation in identifying the malware.

Implementation of Tools

There was a four step process used to analyze the bots captured in this project. The first step was to collect a bot through a Nepenethes sensor. The research team collected thousands of bots using Nepenethes. This sensor emulated modules within the Windows XP services, due to the large number of Windows machines currently connected to the Internet. This limits our findings to Windows systems only, though they comprise the largest percentage of systems online at any given time (Bacher et al. 2005). Consequently, this provides a more representative sample of malware than those bots designed to target Mac or Linux systems. Once the malware was downloaded to Nepenthes, its md5sum, timestamp, source, and protocol of the download were collected. This information was used to track and catalogue the bots. In fact, there were thousands of bots captured through this method.[1]

The second step in the analysis process involved analysis through the Truman Sandnet system to determine its functionality. The Truman Sandnet program allows the bot to be run off-line to record the embedded strings and determine its capabilities. This may include dictionaries for dictionary attacks, IRC commands for bot controllers and hard coded DNS addresses to

[1] One of the pieces of malware included in this sample was not technically a bot, but rather a trojan designed to facilitate the installation of adware on an infected system. This malware mimicked the actions of a bot, and was therefore included in this sample.

connect to certain command and control centers. In addition, the program uses a perl script that simulates attacks using commands found in the strings. Using this method, a command can be issued to the bot on the Windows part of the sandbox from one of the emulated servers in the Linux part of the sandbox. The bot will then attempt to perform the requested command and all the traffic it generates is captured on the Linux part of the sandbox for further analysis.

The third portion of the analysis utilized the honeynet to connect the bot to the Internet. After running the bot through the Sandnet program, it was then installed on the Honeypot, or single machine within the honeynet so that it can safely be connected to the Internet. This honeypot was connected to a honeywall that monitors all its traffic in and out of the system. A connection limiting constraint was placed on the honeywall using the Linux IP tables firewalling system so after a predetermined amount of packets going outbound from our honeypot was recorded, the rest of the packets were be dropped. This kept the zombie node from participating in attacks against other systems. After the bot was installed on the system it attempted to call back to its command and control hub. Once the connection was established all transmissions between the honeypot and other machines were recorded using a program called Sebek that runs in the kernel and records commands sent to the honeypot before it goes through encryption.

Finally, after the bot ran for a one to two week period, it was shut down and all the traffic generated was analyzed. This data was recorded in Pcap format so it could be easily read by automated analysis tools such as Tcpdump and Wireshark. These programs enable more accurate and rapid data analysis, and can be examined by multiple researchers to consider the functionality of these programs. Thirteen bots were run through these procedures from April to

December 2007 (see Table 1 for detail).[2] The bots in this analysis were selected based on their activity within the Sandnet, as they appeared more active than the other malware collected. They provide a convenient, yet purposive sample, in light of the volume of malware collected. The findings of this research are presented in detail below, describing the command and control channel locations, functionality and activity within the honeynet.

Table 1: Descriptive Data on Bots Run Through the Honeynet

Bot	Observation Period	AV Classification
1	4/30/07-5/11/07	W32.Spybot.Worm Worm.SdBot-500224
2	5/12/07-5/25/2007	W32.Spybot.Worm
3	5/22/07-5/29/2007	Worm.SdBot-500224
4	7/2/07-7/5/07	W32.Spybot.Worm
5	7/9/07-7/12/07	Trojan.SdBot-6530
6	7/16/07-7/23/07	None
7	7/16/07-7/23/07	TR/CryptExe.A
8	7/17/07-7/23/07	Backdoor.rbot.xfv
9	8/21/07-8/26/07	Trojan.Vundo
10	10/8/07-10/15/07	Dialer.Trafficjam
11	10/16/07-10/29/07	W32.IRCBot
12	11/6/07-11/12/07	Trojan.SdBot-6699
13	11/26/07-12/3/07	Trojan.SdBot-4953

[2] Due to time constraints and system errors, the analyses presented are limited to 13 bots. Others were collected and run, but a catastrophic data error caused their log files to be lost completely. Thus, the findings are limited to this window of time.

QUALITATIVE RESEARCH

The second component of this study involves a qualitative criminological examination of active malware markets and forums that facilitate hacking on-line. The research team developed a sample of six publicly accessible web forums that trade in bots and other malicious code, as well as four forums that provide information on programming, malware, and hacking. Regardless of the information provided, these forums act as on-line discussion groups where individuals can present issues or discuss problems. They are composed of threads which begin when an individual creates a post within a forum, asking a question or making a statement. Other people respond to the remarks with posts of their own that are connected together to create threads. In this way, threads are composed of posts that center on a specific topic under a forum's general heading. Since posters respond to the ideas of others, the exchanges present in the threads of a forum demonstrate relationships between individuals. This data is critical to understand the ways individuals become established and reliable actors in malware markets, as well as the methods of sellers and buyers. The content also provides concrete detail on the quantity, quality and price of bots, malicious software, and other services sold and the payment methods used. Finally, this data provides pertinent information on the ways that malware is created and developed through collaborations with others.

The sample of forums was collected via a snowball sampling procedure. Specifically, two English language forums were identified through google.com using the search term "bot virus carder forum dump." After exploring the content of threads from these two sites, six other Russian language forums were identified via web links provided by forum users. In fact, most participants in forums involved in the sale and trade of malware communicate using the Russian language (see Thomas and Martin 2006). Thus, a sample of threads from each of these forums was examined by a native speaking Russian research assistant to ensure the content was focused on the sale and exchange of malware. Four additional Russian language forums were identified through links provided in these sites to create this sample of ten forums. Six of these forums focus exclusively on either open sales or requests for malicious software, hacking tools, cybercrime services, and stolen data. The remaining four forums provide a mix of sales, information sharing, and resources to facilitate hacking and malware creation. These forums were included in the sample to better understand the skills and abilities needed to create malware and engage in hacking.

Within these 10 forums, all of the available threads were downloaded and saved as web pages. There was a significant volume of information obtained, though we selected the first 50 threads from each forum to be translated from Russian to English. A certified professional translator was identified who translated the first 50 threads from eight of the 10 forums. Additionally, 25 threads from forum 06 and 21 threads from forum 05 were translated. Due to limited availability and duplicate translations in some of the forums, a native Russian graduate student was identified who translated additional content.[3] This student translated an additional 150 threads from forums 03 and 04, and an additional 138 threads from forum 05. Further content was translated from these three forums as they were very active and can provide greater detail on the activities and practices of actors within malware markets. Duplicate threads were translated to determine interrator reliability, which appeared high across the two translators.

A total of 909 threads were derived from this convenient, yet purposive sample of ten forums. The threads were composed of 4,049 posts, which provided a copious amount of data to analyze (see Table 2 for forum information). Moreover, the forums had a range of user

[3] The graduate translator provided translations from seven forums: six threads from forum 02; 150 from forums 03 and 04; 138 from forum 05, 25 from forum 06, one from forum 07, and one from forum 09.

populations, from only 35 to 315 users. These threads span a four year period, from 2003 to 2007, though the majority of threads were from 2007. This is concurrent with the timeframe of the bot analyses, thereby providing a more robust exploration of bots and their use among hackers relative to other malware and hacking tools.

Table 2: Descriptive Data on Forums Used

Forum	Total Number of Strings	Total Number of Posts	User Population	Timeframe Covered
01	50	183	88	6.00 months
02	50	164	50	20.00 months
03	200	1203	315	10.75 months
04	200	812	273	12.50 months
05	159	369	153	6.75 months
06	50	251	82	36.25 months
07	50	379	116	29.50 months
08	50	291	95	36.00 months
09	50	172	35	10.50 months
10	50	225	95	1.50 months
Total	909	4049	1302	

The translated threads were then printed and analyzed by hand to consider both the prevalence and cost of products and services bought and sold in these forums. A content analysis was conducted to identify products, resources, and materials either sold or sought out in these markets. Ad content was coded based on the detail provided. A post was coded as a sale if an individual stated that they were "selling," "offering," or otherwise providing a service. Requests for products were coded based on the language used, such as "need a," "buying," or "seeking." Each item either requested or sold was coded individually, such that an advertisement selling both a piece of malware and a spam database were coded as a single spam database and malware. Thus, the number of advertisements is larger than the overall number of threads where they appeared.

Services were coded into categories based on the content of the ad. Specifically, any ad that provided a service, such as the delivery of spam, web hosting, and hacking was coded as "cybercrime services." Ads related to malicious software, including bots, trojans, and iframe tools were coded as "malware." Individuals buying or selling credit card account information, records from keystroke logs on compromised machines, and other resources were placed into the category "stolen data." The tag "ICQ numbers" were used for ads by individuals who sold or requested ICQ numbers for their personal use. Any advertisement that appeared to be for legitimate products such as computer hardware or software, video game resources, legitimate security or programming services, and other products were placed under the tag "Other Services." Finally, there were a range of tools that were made available to forum users for free. Any thread or post related to a free program was placed under the tag "free tools."

The subcultural values and norms that structure the market and relationships between actors were assessed using grounded theory methodology (Corbin and Strauss 1990) and the concept of "normative orders" (Herbert 1998: 347). Normative orders are a "set of generalized rules and common practices oriented around a common value" (Herbert, 1998: 347). An order "provide[s] guidelines and justifications" for behavior, demonstrating how subcultural membership impacts actions (Herbert, 1998: 347). This gives a dynamic view of culture, recognizing that individual behavior can stem from individual decisions as well as through adherence to subcultural values. Normative orders also provide for the identification of informal rules considered important by members of the subculture because of the values they uphold. Furthermore, this frame allows the researcher to recognize conflicts in the subculture based on the presence of contradicting orders (Herbert 1998).

Herbert (1998) provides little guidance on how to actually measure normative orders, but identifies them through qualitative examination and consideration of the attitudes, beliefs, and perceptions individuals hold about their behaviors as demonstrated through verbal and non-verbal communication. Holt (2007) utilized posts from web forums and interviews with hackers to perform a similar hand-coded ethnographic exploration of the normative orders of the hacker community using grounded theory analyses. This study proceeds in the same fashion as Herbert (1998) and Holt (2007), by using grounded theory methodology to identify normative orders through hand coded analyses (Corbin and Strauss 1990).

Grounded theory analyses utilize a three-stage inductive methodology that is particularly useful as it permits the researcher to develop a thorough, well-integrated examination of any social phenomena (Corbin and Strauss 1990). Any concepts found within the data must be identified multiple times through comparisons to identify any similarities (Corbin and Strauss 1990). Specifically, grounded theory analyses begin with open coding where all data is placed into specific events or incidents, then labeled and grouped into categories and sub-categories using a specific identifying tag (Corbin and Strauss 1990). For example, terms such as trustworthy, reputable, or cheat were labels used to identify different seller within these forums.

The second phase of axial coding involves testing the relationships between categories, subcategories, and the data itself to further develop the identified concepts (Corbin and Strauss 1990). Each tag was re-read and recoded to identify unique elements or subcategories in the tags. For example, the repeated appearances of terms like cheat or reputable across the forums were examined further and the negative or positive context of these terms examined to discern their value in the context of purchases and exchanges. Also, certain passages were removed or placed under new headings during this phase because they were not relevant to their initial category.

Then the final selective coding phase began to determine how any categories or subcategories from previous stages could be linked to a "core category" of the phenomenon under study (Corbin and Strauss 1990: 14). All axial coded tags from each forum were analyzed to understand the relevance of subcategories evident across the forums, and establish the key orders of the subculture. For instance, the terms identified in previous coding demonstrated the value of trust in the markets as a way to reduce the likelihood of receiving bad goods or losing money which structured forum users' attitudes and actions. Thus, grounded theory methodology engenders the inductive identification of norms and values in this qualitative data.

III. Results

BOT ANALYSES

In examining the bots, there were several unique system-level affects that the malware had on the Windows image in the honeynet. When loaded on to the Windows image 10 of the 13 malware (77%) directly affected system processes by adding, deleting, and/or changing files. Specifically, these programs added or changed files, largely adding the malware executable to the system (see Table 3 for detail). There were 10 unique executables identified, and one variant of a program in this sample of malware (see Appendix 1 for detailed descriptions of each bot). Specifically, these programs include agldoc32.com and the variant agldoc32.com-up.txt, angmang.exe, csrs.exe, dsrss.exe, Ehncze.exe, lssas.exe, mswindll32.exe, spooIsv.exe, tray.exe, and wuaumqrl.exe. In addition, four of the bots loaded executables into the prefetch directory of the system. The prefetch directory is a component of Windows XP systems' memory manager designed to increase the speed of the windows boot process and application launch times (Steel 2006). Placing an executable in the prefetch directory may enable rapid and seamless installation and execution of malware upon system booting.

Table 3: System Processes Affected By Each Bot

Bot	Files Added	Files Changed	DLLs Added	DLLs Removed	Services Added	Services Changed
1	1	0	12	1	0	0
2	6	21	21	0	0	0
3	0	0	0	0	0	0
4	1	0	0	0	2	0
5	4	0	0	0	3	4
6	1	0	7	1	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	1	0	6	0	0	0
10	3	0	10	0	0	0
11	2	0	11	0	0	0
12	2	0	6	0	0	0
13	2	0	8	0	0	0

Eight of these programs removed or added new dlls, or Dynamic Link Libraries, to the system. A dll is a library that contains code and data that can be used by multiple programs at once as a way to use memory more efficiently (Steel 2006). Additionally, dlls allow programs to be loaded more quickly, as they can be broken down into components recognized and accessed only when used (Steel 2006). The fact that these malware added dlls suggests that they may be operating more efficiently than other programs.

Finally, only two of the malware analyzed affected system services. One bot added two new interrelated services: the first was a remote access connection manager that allowed an outside user to connect to the system, while the second was a telephony service that controlled all dial-up internet connectivity, and some cable internet access. These additions indicated that this bot was designed to manage zombie node Internet connectivity and possibly use zombie nodes as proxies. The other bot stopped four system services, including the software firewall, security center, and remote registry. In this way the bot was trying to make the machine more vulnerable to other attacks. This bot also added the same telephony and remote access manager programs. Thus, these two pieces of malware had a significant impact on the Windows image.

Four of the malware (31%) were also obfuscated by packers. A packing program compresses the size of a file so that it is initially smaller, though it can be unpacked once opened to resume to the normal size (Steel 2006). Two of the four packers used were identified as PECompact 2.x and ASProtect 2.1x SKE respectively. Both of these programs were legitimately created and sold on the open market and are not related to malware. The fact that the other two programs could not be identified suggests they may have involved some packing tools available in the hacker community (see also Dagon et al. 2007; Rajab et al. 2006).

All of the malware analyzed attempted to connect to a command and control server, though only nine were able to successfully log in to the channel. Of the bots that connected, they demonstrated the credentials used by the zombie node to connect to the channel. In fact, four of the channels used a password, which consisted of relatively simple phrases, including "spy," "FAST," "Dpass," and "p00n3d." These simple passwords provide a degree of protection for the channel and may aid the bot master in keeping other from accessing the bot (Kassardis et al. 2007; Rajab et al. 2006).

Two of the bots analyzed also attempted to download additional malware from independent websites. These attempts included the programs *spy.exe* from *nerashti.com* and *bb2.exe* from the website *californaisaabs.com*. The download from californiasaabs.com is interesting, in that this appeared to be a legitimate business website. As a consequence, the site may have been part of a larger compromise against the web server hosting this site to place the malicious code on that page. This may have been orchestrated by the botmaster for this program as a means to conceal updates for the bots to improve their functionality (see also Rajab et al. 2006).

While analyzing network traffic, 17 domain names were extracted from the bots and validated through network registration information for each domain through whois records. Fifteen of these names corresponded to the location of the Command and Control IRC servers, though some addresses did not successfully resolve. This may be an indication of short lived Command and Control channels as noted in previous research on botnets (e.g. Kassardis et al. 2007). The threats appeared to come from a handful of countries based on data obtained from whois records in Figure 1. The overwhelming majority, however, were hosted in the United States, suggesting that there is a need to better secure networks from becoming part of a command and control node. The domain names identified also provided point of contact information for the registered domain names, though there was no way to verify the actual user who registered each domain. The contact information provided may, however, be the information for the owner of a compromised server, or falsified information from a criminal.

Figure 1: Location of C&C Site

[redacted]

While nine bots connected to a command and control server only five received commands from the actual server. The tasks given by these five bots were varied, and may have been used in actual attacks. For example, one of the bots attempted to set up a NetBIOS session, which would allow for seamless communications between multiple systems (see Steel 2006). A second bot received requests to port scan other machines connected to the subnet. A third received requests to participate in a DDoS attempt against a specific IP address. The fourth installed a copy of the executable operating the bot on another machine within the subnet, thereby spreading the infection. The final bot connected with a remote computer and attempted to open a variety of connections on five separate ports. These connections enabled the computer to gain access and communicate with the other system through NetBIOS protocols. Thus, the bots in this sample appeared to receive a number of requests in line with some other studies of this malware in the wild (e.g. Rajab et al. 2006). The findings also suggest that bots have unique utilities for cybercriminals and exist in systems around the world.

QUALITATIVE ANALYSES

In order to understand the dynamics of malware markets and forums, it is critical to first consider how advertisements were created and the process of buying and selling malware and services. The following section details the structure of the market, using quotes from the data where appropriate.

Structure of Forum Markets

The forums identified in this study comprised an interconnected marketplace that is composed of unique threads that act as an advertising space. Specifically, individuals created threads posting their products or services to the rest of the forum. Alternatively, posters could describe in detail what they were interested in buying or acquiring on the open market. Both buyers and sellers provided as thorough a description of their products or tools as possible, including contact information, pricing information, and payment methods. Actors within these markets communicated primarily through the instant messaging protocol ICQ or e-mail, as they can be encrypted to protect both participants during the sales process. Some also used the private message, or pm, feature built into to each forum. Private messages ensure quick contact and act as an internal messaging system for each site, though they may not be as secure.

Prices were stated in either U.S. dollars or Russian rubles, along with the desired method of payment through some web-based monetary system. Forum users regularly paid for their goods and services using WebMoney [WM] or Yandex as noted in the following post from the ICQ seller Creator:

> 1. Money first, numbers later
> 2. I work only from Yandex Money and WebMoney.
>
> Course:
> 1 unit [ICQ Number] =26 wmr [Web Money Rubles] =$1 [U.S. Dollar]
> 1unit=26 Yandex rubles

Prices listed using the abbreviation wmz indicated that the seller would accept Web Money payments in U.S., or z, currency. This was demonstrated in a post by Statement who offered databases for spam and identity theft:

> I'm selling databases of postal clients for 700thous users 20WMZ, for 15 thousand users 7 WMZ (mail address_login_password). Spam database for 1 mil users for 15 WMZ, 700thou users 10WMZ. . . Payment by webmoney

The use of electronic payment systems may be due to the fact that they allow relatively immediate payments and require no face-to-face interactions between the participants. This provides a modicum of privacy and anonymity for the participants, but creates the possibility that they may not receive the goods for which they provided payment. As a consequence, four of the forums identified in this sample offered or discussed payment services through guarantors. A guarantor is a specialized payment mechanism that can be used to deal with individuals who may or may not be trustworthy. Given that the majority of the products and services offered in these markets are illegal or can be used to break the law, participants have little legal recourse if they are slighted at some point in their exchange. Access to a guarantor service is an important way to ensure transactions are successful and complete. Guarantor services were best described by an individual named Chackrat, who offered his services:

> About what a guarantor is:
>
> A guarantor is an intermediary in transaction. When you use a guarantor services it is impossible to get ripped off.
>
> Work scheme:
>
> The seller and the buyer get in touch with one of the representatives of the guarantor service by icq and they come to agreement on the **EXACT** terms of the transaction. When agreement has been reached, the buyer gives the guarantor the amount of the

> transaction (or as it was shown in the contract) +0.8%(commission by WebMoney.
>
> The Seller gives the goods to the buyer, after examining the quality of the goods, the buyer advises that the seller can give the money, and the guarantor gives the money. Commission is not charged by the guarantor.
>
> In order to avoid any mishaps:
>
> The ICQ of the guarantors are **ONLY THOSE** shown above, and there are no others.
>
> If you have any doubts, ask the guarantor to send you a PM [personal message] on the forum.

This post demonstrates the value of guarantors to minimize the potential risk of loss that an individual may incur. The presence of such a system may be an indicator of greater organization and sophistication within these markets relative to the others in this sample. It may also simply reflect variation in the overall nature of each forum. This was demonstrated in an exchange in the forum 10, where an individual requested a custom made trojan and specified that payment work through a guarantor:

> **Granted**: I'm buying a trojan (switch of html pages). 15k.
>
> I want to buy a ready to use tool, or to custom order one from a person with EXPERIENCE. . .
>
> Contact Icq: [number removed]
>
> If there is not enough experience, then don't waste my time and yours, just pass on by.
>
> Fraud artists and those looking for something for nothing can pass on by, I'm buying CODE after testing, the transaction is possible using a guarantee.
>
> Starting price 15k.

> **Zaphos:** The guarantor is on [a separate forum] - this is the forum administrator, a trusted person, to whom you will send the virus. The Guarantor tests the virus according to the scheme provided by the customer. After confirmation, the customer sends the money. Thereafter the guarantor pays the developer, and sends the goods to the customers. 3-5% of the transaction is usually charged for this.
>
> Only as I understand it, there is not guarantor here [in forum 10].
>
> **Granted:** We can figure something out with a guarantor, if you really have such a product - we'll definitely reach an agreement.

This exchange suggests that guarantors have a place within these markets, though they are not present in every forum. Instead, the majority of forums in this sample appear generally open, enabling individuals to advertise their products directly to others with little regulation or constraint. Thus, malware buyers can select who they purchase goods and services from and in specific quantities. From this perspective, the markets identified in this sample share some common traits with open air drug markets (Jacobs 1999, 2000) or direct hawking markets for stolen goods (Cromwell, Olson, and Avary 1991, 1993; Schneider 2005; Stevenson, Forsythe, and Weatherburn 2001; Sutton 1998; Wright and Decker 1994).

Though there were no actual public transactions of goods for money observed in the forums, posts from buyers and sellers gave some indication of how this process operated. An interested party contacts the individual who is either seeking or selling something via ICQ or e-mail. The parties negotiate what they need or require, and then payment is provided. It is important to note that several sellers specified that payments must be made in advance of any service or product being rendered. The entire sales process was demonstrated in a post from sanction who offered to encrypt trojans and malicious software:

> You know me [contact me] in ICQ and obviously explain what I need to do. . . After that, as soon as I complete your order, you transfer money into my WebMoney purse. After that, you receive the product. . . To familiars (at least exchange couple of words in ICQ) I will give the product first. For all the rest, we work based on the scheme: money first, and then chairs after.

This post emphasizes the importance sellers place on receiving payment for their resources, which introduces the potential for buyers to lose money should a good or service not be delivered. The unregulated nature of the market also provides no real leverage for a buyer should they be ripped off. As a result, the sales process appears to favor sellers rather than buyers. This relationship is also evident in open air drug markets, where individuals may be robbed or receive poor products and have few regulatory agencies to turn to for assistance (Jacobs 1996, 2000; Jacobs, Topalli, and Wright 2000). Thus, there may be some significant relationships between real world criminal markets and virtual crime markets. The goods that are offered are significantly different, and will be explored in detail in the next section.

PRODUCTS, RESOURCES, AND INFORMATION

In examining the forums, it was apparent that individuals posted goods and services that could used for legitimate or illegal purposes. In fact, 630 of the 722 ads either selling or buying a service involved a tool, service, or data that could be used to engage in cybercrime or some other illegal activity (see Table 4). Additionally, the majority of these posts were sales related (73.1%), rather than purchase related (22.8%). The remaining 91 (13%) requests were related to a variety of other legitimate or gray market jobs and services. For example, the primary category was composed of computer security job postings, programming services, and website and forum development requests (30.7%). Individuals also sold or attempted to purchase video game characters and items, as well as custom avatars for forums and websites (18.7%). SIM chips and cellular cards were also sold (16.5%), along with email accounts in Google, Yandex, Mail.ru, and Rambler.ru (13.2%), and computer hardware and software (13.2%). Finally, individuals sold access to file sharing accounts in sites such as RapidShare (5.4%) and other services (2.2%). Given that 87.3 percent of the requests in these sites were related to tools and services to facilitate cybercrime, this analysis will focus in depth on these items, using quotes from the data where appropriate.

Table 4: Resources Offered in Hacker Forums

Resources	Number of Posts	% of Total	Buy Posts	% of Total	Sell Post	% of Total
Cybercrime Services	219	30	39	17.8	180	82.2
ICQ Numbers	73	10	9	12.3	64	87.7
Malware and Related Services	246	34	103	41.9	143	58.1
Other	92	13	22	23.9	70	76.1
Stolen Personal Information	92	13	21	22.8	71	77.2
Total	722	100	194	26.9	528	73.1

MALWARE AND RELATED SERVICES

The forums identified in this study enabled individuals to access to a variety of malicious software and resources to facilitate the distribution of malware globally. Malware sales comprise the largest share of products sold in these markets (34%) with 246 posts requesting or selling resources. This section will explore each of the malware related products offered or sold in detail (see Table 5 for breakdown).[4]

[4] It must be noted that two individuals sought out individuals who could identify zero day vulnerabilities in systems so that they could be exploited for an attack. A third individual was selling information about a bug within the

Table 5: Malware and Related Services Offered in Hacker Forums

Resources	Number of Posts	% of Total	Buy Posts	% of Total	Sell Post	% of Total
Bots	16	6.5	8	50.0	8	50.0
Bugs	3	1.2	3	100.0	0	0
Cryptors, Joiners, And Polymorphic Engines	47	19.1	13	27.6	34	72.4
FTP Resources	27	11.0	15	55.6	12	44.4
Iframes and Traffic Sales	75	30.5	26	34.7	49	65.3
Tools	21	28.0	7	33.3	14	66.6
Traffic	54	72.0	19	35.2	35	64.8
Trojans	78	31.7	38	48.7	40	51.3
Total	246	100.0	103	41.9	143	58.1

Trojans

The most common form of malware available in these markets was trojan horse programs. There were 78 ads related to trojans, comprising 31.7% of all malware for sale. The cost of these programs varied significantly, from $2 dollars all the way up to $5,000 depending on the resource (see Table 6). A variety of trojans were available, including a tool called Pinch. This piece of malware is an extremely effective keylogger designed to steal information over 30 programs. The utility of Pinch was described by the seller downwind who offered custom builds of this tool:

> Services-
> [x] Pinch 2.99 (a version of the build below that indicated is OK, i.e. a selection upon request is accepted)
> [x] Parser (the program itself + video to be configured)

market. These posts, however, comprise only 1.2% of all malware related posts, and are not discussed in detail in the larger text.

[x] A Gate (custom-built, whoever is satisfied with the SMTP method, i.e. by e-mail)
[x] Crypt with the **Virtual Machine Protector** (concealment from antiviruses moreover each customer will have an individual signature, which means that only the owner will be responsible of the the burnability [detectability] of the trojan, since only he can burn out his trojan.)
[x] Bypass of Agnitum Outpost Firewall 4
[x] By-pass of Kaspersky Internet Security
[x] Self-deletion of the trojan after launch
[x] Addition of an icon to the trojan
[x] Gluing with any\favorite file\s within 10 mb
[x] Self-written Pinch user guide
[x] Masking off the trojan during the process as svhost.exe (if desired, any process name is possible_
[x] Changing the trojan extensions to *.**bat** , *.**exe** , *.**com** , *.**pif** , *.**scr**
[x] Auto-loading of the trojan in the system from a "hidden" place in the register which is not visible through msconfig
[x] Addition of information on the file
[x] Showing an error message after the trojan has been launched
[x] **Configuration of all components for overall performance**.

It has on board:
- A password grabber and password decrypter
- cmd shell (on board 8879, i.e. bindshell)
- Ftp
- Proxy
- Socks5

Decrypts passwords from the following programs-
- **ICQ 99B-2002a**
- **ICQ 2003/Lite/5/Rambler**
- **TRILLIAN**
- **&RQ, RnQ, The Rat**
- **QIP □/8030 and earlier versions)**
- **GAIM**
- **MSN & Live Messenger**
- **The Bat!**
- **MS Office Outlook**
- **Mail.Ru Agent**
- **Becky**
- **Eudora**
- **Mozilla Thunderbird**
- **Gmail Notifier**
- **Opera 9.2x**
- **Protected Storage(IE, Outlook Express)**
- **Mozilla Browser**
- **Mozilla Firefox**

- **RAS**
- **E-DIALER**
- **VDialer**
- **FAR**
- **Windows/Total Commander**
- **CuteFTP**
- **WS FTP**
- **FileZilla**
- **Flash FXP**
- **Smart FTP**
- **Coffee Cup FTP**
- **RapGet**
- **USDownloader**
- **RDP (Windows Remote Desktop)**

Table 6: Pricing Information for Malicious Software

Product	Minimum Price	Maximum Price	Average Price	Count With Price	Count With No Price
Bots	30.00	2000.00	322.27	9	7
Bugs	40.00	40.00	40.00	1	2
Cryptors, Joiners, And Polymorphic Engines	0.20	49.00	13.03	27	20
FTP Resources	20.00	1000.00	271.66	6	21
Iframes and Traffic Sales					
Tools	2.00	450.00	79.25	12	9
Traffic	1.00	500.00	110.84	34	20
Trojans	2.00	5000.00	742.97	28	50

This post illustrates that Pinch was designed to steal data from multiple programs and can be configured to obviate anti-virus software. Similarly, the seller xoform in forum 03 offered builds of Pinch stating:

> I am selling pinch builders. 50 wmz for a builder. To each there is a separate signature. The take comes from these programs:
>
> - ICQ/IRC Clients (ICQ 2002a/2003/Lite/Rambler /5, TRILLIAN, &RQ/RnQ, QIP 8010,8020,8030)
>   - GAIM(Pidgin)
>   - MSN & Live Messenger
>   - e-Mail Clients (The Bat!, MS Outlook, Mail.Ru Agent, Gmail Notifier, Eudora, Becky)
>   - Browsers (clients Opera до 9.2x, Mozilla Thunderbird (all versions), IE (all versions), Mozilla
>   - Dial-Up(Windows RAS, E-Dialer, Vdialer)
>   - FTP Clients & Downloader (Windows/Total Commander, FAR, CuteFTP, WS FTP, FileZilla, Flash FXP, Smart FTP, Coffee Cup FTP, RapGet, USDownloader)
>
>   Also there are added possibilities:
>
> -Bypass through a proactive Kaspersky Internet Security 6.0
> -In the builder there is a built-in cryptor. ICQ: [removed]. The work plan is: Pay the money and within 24-hour period I will give you the builder.

Beyond Pinch, individuals sold access to a variety of trojans designed to steal money from WebMoney accounts. For example, the seller Novacaine in forum 03 posted an advertisement for multiple builds of a WebMoney trojan. These malware could be used to steal electronic funds from a victim, as demonstrated in this description of one build:

> WM Trojan T266 Vers.2
> Extracts all the methods from the WebMoney Keeper Classic
> -Has been tested on versions 3.0.0.0-3.1.0.1
> -Extract of all methods from all Z, R, E, U purses; does not extract money from purses with less then [SIC] 0.20 (regulation is for you)
> -Installation of transfer detection, purses, and control through web admin
> -Invisibility to to anti-virus, individualization for each build
> -Drops off such firewalls like Outpost 3-4, Anti-hacker 1-1,8
> -Blockage of webmoney.ru, wmtransfer.com, victims will not be able to access the site
> -Size is 15KB
> -Autoloading
> -Installation of your icon
> -Web statistic of uploads
> -Control in the web admin, 1. We delete from the autoloading and exit 2. block the keeper
> -Checking the quantity of the file to verify the download of purses from that file
> -Donwload of purses through Internet Explorer, bypass of firewalls.
> -After the extraction of all methods, follows the blockage of the keeper; in future when someone turns to the keeper it will download from the processor
> -Checking the repeat lunch

Other sellers were not as detailed in their posts, instead simply describing their services for data theft or system compromises. For example, an individual named doubt in forum 04 advertised:

> Hello to everyone. I will sell a trojan, of a private writing, interrupts the WIN of the victim, with the capabilities of changing the files through the network and knock [contact] to the admin, informing the IP [address of the] victim. Weighs 14KB, unpacked. Contents: Build, Builder, 2 pHp scrypt [SIC]. Does not burn [get detected] by Kasper, NOD32, Dr. Web, Avast, BitDefender. Price is 5 wmz.

In examining the forums, it was evident that individuals also sought out custom trojans and malware from coders. This was demonstrated in a post by the user pavel in forum 10, who wrote:

> A coder is needed on [Forum 10]. 1. a coder is needed at the zero level, for writing a worm. 2. coder-reverser, for finding vulnerabilities in well-known systems and programs.
> if you have creative talents - that's a plus.
> experience in writing any soft is a plus.
> if you have some projects to show, that's a plus.
> high pay.

Such posts were found across the forums, suggesting that the market for existing trojans may not meet all individual sellers' needs. In fact, requests for trojans comprised 49.4% of all posts, while 50.6% involved direct sales. Thus, there is some balance between supply and demand for trojan horse programs.

Iframe Exploit Packs and Traffic Sales

In addition to encryption tools, a unique service was identified across the forums to enable the distribution of malware through web browsers. Iframes are used in legitimate website design as a means of pushing multiple html files in a single page of content for users seamlessly and without interaction (see Provos et al. 2008). This technology can be subverted by malicious actors in order to push down malware to infect end users. Thus, iframe exploits and packs were sold that, when placed on a server or a website, infect individuals who visit the web pages hosted there. This type of attack exponentially increases the infection vector for malicious software, and the risk of identity theft, data loss, and computer misuse. Within the forums in this sample, iframe resources comprised 30.5 percent of all malware resources offered (see Table 5). There were 14 individuals selling access to iframe scripts and infection packs, such as skelton in forum 01 who advertized the genom iframer kit:

> **genom iframer 2.23**
> Script for iframe. This is not a clumsy package of scripts, but one script which weights [weighs] just 12 kb.
> Moreover this small script doesn't only not yield to inject code, but outdoes the products which exists now. It will be most convenient for dynamic use. I wrote it myself.
> It's written on php.
>
> Capabilities:
> 0-work with txt databases.
> 1-entrance protection with the help of md5.
> 2-editing of additions and deletion of accounts through a web interface.
> 3-the possibility of loading .txt databases.
> 5-insertion of arbitrary code in site pages -- regulated by the level of penetration in the server sub-directory (i.e. you indicate the depth and the script goes through all the directories in the file search until the level indicated [6 absent]
> 7-auto-detection of directories
> 8-the ability to automatically purify bases from trash -- i.e. only ftp accounts remain
> 9- 4 different types of encrypting for your code -- moreover the crypt can be done sequentially -- i.e. first by the first method, then by the second, third etc.
> 10-a flexible system for working with file names - you can show the names in a lists -- to select ready-made names -- and the most convenient (in my opinion) description of file names using php regexp

> 11 - built-in protection against the turn-on option magic_quotes
> 12-built-in protection against inability to change set_time_limit for executing the script -- i.e. even if a small limit is put on executing the script it will still work
> 13-built-in deletion of other's inserts done using ftp_tools_pack, orphans and many others -- encrypted inserts are also deleted
> 14 - automatic sorting and purging of accounts from repetitions (executed upon click on only ftp)
> 15 - checking of ftp for valid both from the file and from the list
> 16- breaking through by accs [accounts] page rank both from a file and from a list
> Price 20 wmz

A similar post was found in forum 02 by an individual named Jules who offered a competing iframe script:

> **RooT [iFRAME]*R - script for installing iframe**
>
> The script is used for adding iframe code files to the index (index/main/default.htm/html/php/asp).
>
> In order to launch the script it is enough to have root user rights,
> or any other who has access to writing in the files/catalogs we need.
>
> ***Script capabilities:***
> ***** *Addition of iframe code files to index/main/default*
>
> ***** *Deletion of iframe code added earlier to index/main/default files*
>
> ***** *Changing already inserted iframe code to new code*
>
> After its launch, the script creates the base of needed (index/main/default) files for subsequent processing.
> As the script is working, there is a display of how it is being performed with a line-by-line output of a report on files changed.
> After processing has ended, the script gives statistics on the number of files which were changed.
>
> *One of the main advantages is the fact that one does NOT need to know logins and passwords on the FTP in order to insert the iframe.*
> *You can insert any of your code into the file, you only need to have write rights to the catalogs of the sites hosted on the server.*
>
> **Script price - 25$**

Given the power of these tools to infect a variety of computers, it is important to note that seven individuals actively sought out iframe malware. For example, an individual named xtacle in forum 10 posted a request for a skilled coder to build a custom loading program to facilitate mass web-based infections:

> a programmer is needed with experience working in the area of finished results for long term work in a term to create a codec solution.
> What we have:
> Our own adult traffic [via a website], the possibility of attracting traff [web traffic] from the outside and knowledge of what to do with it.
> The following is required from you:
> full software support of the project.
> at the start a loader will be needed (naturally with decent quality, polymorphic with firewall by-pass etc.)
> we will try to put a load on it with light traffic, and as soon as we see that you loader meets our requirements,
> we'll start installing everything we need:
> the replacement of search engine results, adware (you should also have at least minimum results in such soft),
> anti-spyware (if you have your toolz for infecting then we'll see what they are any maybe we'll arm ourselves with them),
> then we will try other options for conversion (WITHOUT CARDING).
> I can't say anything in particular now about the % [fee], we'll have to discuss that individually since it will depend on what you can really offer us,
> PS we will give out the % in money from the profit, and not a % of the traffic, since for is only important what will be established from our traffic and
> we should control this.
> PPS For this reason we need a partner, because we need quality support and continuous modification of the soft for increasing the "exhaust" [financial effectiveness].
> PSSS All our original costs for the server etc. are on us, we need only soft from you
> and in the closing, if you are really interested in long-term cooperation (the money may not be there immediately, you must understand),
> you are results-oriented and do everything on time and with enthusiasm, then you are 100% what we need.

As a whole, there were a number of iframe tools being sold, and an active demand for these resources. Additionally, the price for these products ranged from $2 to $450 (see Table 6). This suggests that customers may have some variation in the quality of resources available on the open market.

These markets also enabled individuals with established, active iframe scripts on servers to sell access to "traffic streams." Selling traffic enables an individual to make a profit by uploading some else's malware to the server so that it could be used to infect individuals when they visited web pages hosted there. There were a number of iframe traffic sellers, as their ads comprised 64.8 percent of the market for traffic, while 35.2 percent sought to buy access to traffic (see Table 5). For example, st3v3n from forum 03 described his service to both upload malware on servers and trade their services for other traffic:

> Available services:
> 1. Upload for all countries that are included on the list (from $25)
> 2. Upload of country MIX, chosen by you
> 3. Upload for a specific country (RU-$30, us-$90, ETC.)
> 4. Following the status in realtime
> 5. Free test up to 50 uploads
> 6. Friendly service (sweet and smart girl is always glad to assist you)
> 7. Moneyback guaranteed
> 8. Individual approach, tons of auctioning and discounts
>
> The service is under a regular quality check, in order to find any mistakes in work, and to guarantee the quality of the system. With such an approach, we can guarantee 99.9% validity, of course with a stable working contract.
>
> Information for Traff loaders: If you have a traff, we can offer to you our partnership program. We pay for successful installations $80 for USA-1K, other countries $25. Everything is done honestly. Average envelope MIX is $4 for 1K of traff. Payoff is sudden, right after getting the profit from your traff or by deal.

This post suggests an individual who pays for an upload service may very well be able to infect a wide number of users across the globe. Most providers advertised their fees based on 1,000 infections, and the average cost of this service was $110.84 (see Table 6). Individuals who paid for this service may receive significant return on their investment. In fact, traffic service providers used two different pricing structures to upload malware. The first was based on the geographic location of the traffic, as described in a post by scattershot:

> We present to your attention a quality service of downloading. The volume is 15-20K per day. The main traffic is RU, US, GB (UK), DE, FR, IN. Statistic for each downloading, individual choice of nations, possibility to load different files on different traffic.
> Prices: US/UK - 100$ per 1К
> RU - 25$ per 1К
> mix 1 - 20$ per 1К
> mix 2 - 50$ per 1К
> We are interested in serious people that are ready to do long term business.

Others, however, offered pricing based on the amount of downloaded traffic as in the following post from scrottle: "Sale of mix traffic. At the given moment, per day from 8K to 20-25K of traffic. Price is $4.00 for 1K traffic. Majority is US, Russia, and Ukraine. Knock to my ICQ."

Regardless of price, the preponderance of traffic sales advertisements suggests that iframe programs have become a common and critical vector in the distribution of malware. The prevalence of this form of malware led to a post in two of the forums describing a service designed to automate the trade and distribution of traffic:

> Dear forumers [forum users], I would like to call your attention to the FIRST AUTOMATED TRAFFIC TRADING EXCHANGE. . . here you can both buy traffic by criteria which interest you and sell it - at a price which is attractive for you.
>
> The task of our resource is to create comfortable conditions both for sellers and for buyers, to make the accounting easier for traffic, money, and guarantees for buyers of traffic feed, and timely payment for sellers. The flexible system for placing an order allows for satisfying the most exquisite requirements . . .
>
> A simply and understandable system for selling traffic at the exchange
>
> Detailed statistics, including not only content by country and also such parameters as the speed of the traffic stream, percentage composition of browser versions et al.
>
> You can sell and buy traffic of any type with us! Such as iframe, redirect, popup.

> Moreover when selling, you can name the price that you consider your traffic to be worth!
>
> The Support-service allows you not to forget about the existence of people!
>
> If something is unclear to you, or if you have questions, our SUPPORTS will always help you (ICQ #[numbers removed])

The emergence of an automated trading program coupled with the volume of traffic sellers suggests that iframe malware has become a common and important resource within the hacker community. Additionally, the ease with which this form of malware allows for mass infections with minimal effort suggests the need for greater exposition to understand its attack capability (see Provos et al. 2008).

Cryptors, Joiners, and Polymorphic Engines

The third most prevalent form of malware sold in these forums were programs designed to either conceal or encrypt malicious software such as a trojan or bot so it can be sent and activated without being detected by antivirus programs. These tools were referred to as cryptors, and comprised 19.1 percent of the total programs offered in the malware market (see Table 5). There were 26 different individuals selling access to these programs, such as george in forum 02 offered his services, stating:

> I'm selling a polymorphous cryptor - POLARIS[crypt].
> The cryptor crypts both exe [executable] and dll calls and can also encrypt packed files and those glued [joined or bound] with any file.
> After crypting the file can't be burned [detected] by an antivirus.
> And naturally during each encryption there is a new signa[ture].
> You can also open processes and add sections.
> And the well-executed design is nice to look at.
> Price of the cryptor: 2o WMZ!

In addition to encryption, some sellers offered programs that would bind an executable program with other files to create a single executable package. The utility of such a program lies in the fact that this packaged file can obviate antivirus software and appear as a movie, picture, or other file a potential victim will be likely to open. The utility of joiner programs was demonstrated by the seller atoc in forum 05 in his ad for the tool Thunder Joiner:

> Thunder Joiner-the given product is a joiner of files (any, from EXE files to Pictures with documents) into single executing EXE file. Qualities of this given Joiner:
> -The Joined File contains in itself the specified by you files in a coded format and has the anti-emulating function against huristic [SIC] anti-viruses. That is why, during the scan of the "Joined File," the harmful code is not found. But do not forget that after the lunch of the joined file, it releases the containing files onto a hard disk and then your Cryptor, not the Joiner, worries about hiding the harmful codes there. You can use any cryptor based on your preference, for example PAV.Cryptor [website removed].
> -Joined File is a regular EXE [executable] and does not contain data Overlay, via this method you can crypt it or join again with anything, you will not have problems.
> -Stub size is approximately 10-15KB. After joining, you can use any EXE packaging to reduce the size of the joined file, for example UPX and narrow it down with its help, joined file.
>
> -Autolaunch from the registrar: During the lunch of "joined file," the file will copy itself into the system folder (%systemroot%\sytem32) and will write into the registrar for autolaunch.
>
> -Launch of only one copy of the "joined file": option is predicted just in case if the user will try to lunch few copies of the "joined file." If the launched copy has not yet worked, then the new one will not lunch. It is recommended to always turn on the given option, since it conducts a parallel unpacking.
>
> -Self-deletion of the joined file: after the joined file works, it will delete itself.
>
> -As a bonus, the package with Thunder Joiner includes a collection from 42 of the most popular icons.
>
> -15 WMZ and agreeing with rules

A small number of sellers also offered combined crypting and joining services, such as Firefly from forum 05 who advertised his crypting service, stating: "Hello, I am offering you to crypt your trojan for $5.00; with the cost binding and icon is included. . . After crypting, trojan can only be burned [detected] with 3 anti-virus systems, but soon there will be signature update." Additionally, an advertisement was posted in forum 03 by valek who offered the program Fri Joiner:

> Fri Joiner Polymorph, this is a programming tool that secretly installs programs with specifically designed parameter commands onto systems of other users. The joiner itself is a Builder/Configurator (with options on the main screen), which depending on chosen options and setups, builds the body of the downloader. The presence of the polymorph generator with spam instructions can be contributed to the uniqueness of the program, who's [SIC] main command is the creation of individual signature files, during each compilation (binding).
>
> Main Screens: (Functional Characteristics of the builder version 2.2.0)
> -binding unlimited quantity of files with different content and formats
> -the attachment to the joining files is minimal (during building equals 1KB)
> -coding of the joining files with individual keys
> -The bodies of the loader are build dynamically in the process of the compilation
> -placement of the loader bodies that are binded and the information about their unpacking into one section of the file (makes it difficult to detect by anti-viruses)
> -Very fast speed of unpacking of files during the launch, regardless of their size
> -Methamorph building of files' decrypting functions, proceeding of commands is random
> -Option of uploading "Outpost Firewall Pro 4"
> -Option of uploading "Windows Security Center"
> -Chosing [SIC] the heading and text of the extracted message
> -Set up of the window for an extracted message (Info, Error, Ok)
> -Choice of the interface language (Russian or English)
> -Polymorph joiner, which does not have analogs and respected competition in the web.
> Prices:
> -The cost of the individual given Fri Joiner Polymorph v2.2.0 is 30wmz
> -The cost of renewal [updates], depending on the characteristic of the renewal is 1.50wmz

The detailed functionality of a program such as Fri Joiner demonstrates that encryption and binding tools are a critical resource in these markets. Additionally, the average cost of cryptors was $13.03, indicating these products are extremely inexpensive overall (see Table 6 for more detail). The availability of these tools across the market, may explain why only 15 individuals also sought out custom encryption methods for trojans and other malware. This was exemplified in a post from adrine in forum 10:

> IMPORTANT! I need you to write and support a polymorph!
> I need you to write and support a polymorph for a trojan (.exe and .dll)
> hit me up. . .$2,000+ URGENT!

Similarly, exploit9 stated: "I will buy a cryptor on a polymorph or metamorph drive, do not have additional functions. With all offers knock to me on ICQ." These individuals may have required certain tools outside of what was readily available on the market. Regardless, these exchanges demonstrate that quality encryption software is an important component in the creation and distribution of malware.

FTP Resources

In addition to malicious software, hackers offered access to illegally obtained File Transfer Protocol, or FTP servers that have been compromised in some fashion. FTP servers hold sensitive information including web page content, databases, email accounts and other resources (Steel 2006). Thus the sale and distribution of FTP server resources demonstrate a significant threat to computer security and individual privacy. FTP resources comprised 11 percent of the malware market, and the price for these items depended in part on the resource being offered with an average cost of $271.66 per item (see Table 6). The scope of a compromise that can occur as a consequence of accessing FTP resources was demonstrated in a post in forum 01 who stated:

> **I'm Selling an Ftp**
> The following sites are located on one ftp:
> 7353.ru
> admin.mr.sterno.ru
> ari.sterno.ru
> bartenev.com
> bartenev.ru
> best-ipoteka.ru
> boxa.ru
> evian-water.ru
> fb-group.ru
> fly-and-drive.ru

fond-legion.ru
gh0st.sterno.ru
golovanov.net
granini.ru
guard-333.sterno.ru
investclub.ru
investclub.sterno.ru
leenza.sterno.ru
mosregion.sterno.ru
opt.pepsi.ru
prostoipoteka.ru
realtymarket.sterno.ru
sly.sterno.ru
smartwoman.ru
stat.sterno.ru
sterno.ru
tartu.ru
technobelt.ru
teclub.ru
tropicana-go.ru
tropicana-juice.ru
tropicana-open.ru
tropicana-premium.ru
vasyap.sterno.ru
whitesun.ru
wiki.sterno.ru

Pr [Google Page Rank results in search engine requests] 0-5.
Price150wmz.

Similar posts were made by other sellers, such as frash in forum 03 who wrote: "a great number of ftp, individually or in large numbers. There are new and used, I have some edu and gov, mainly Europe and Australia. Knock on ICQ." Additionally, an individual named dR0n3 posted: "I am selling an ftp base-12,000 [accounts]. The base consists of ftp from Europe and USA. The base does not hold ftp of the USSR countries and the sites do not host on free hosts. All the ftps are valid during the sell. The price is 300wmz, Christmas sales." An individual using the handle artemis also offered a software program designed to aid in managing compromised FTP accounts:

FTP Checker [SeRoTKa] + [Code auto pour] v4.6.8
Description:
+Multi-thread scanning and pouring of files to ftp (configuration from 1 to 100 threads which are independent of each other)
+Filtration of repeating FTP accs
+Remote anonymous FTP
+Checks FTP for VALIDITY
+Deletes temporary files
+Able to write the code shown into a page
+Search for files within the FTP for pouring code, given by the user in an external file
+Search for directories for FTP, given by the user in an external file
+The possibility of searching for the given files IN ALL directories on the FTP
+The ability to configure the depth of the search (from 1 to 5 attachments)
+It is able to load/save FTP lists according to a mask (login:password@server.ru) or (ftp://login:password@server.ru)
(also able to load a mask (([21][ftp] host: 127.0.33.1 login: ?????? password: xxxxxx) - the mask of the program Hydra)
+Is able to save valid FTPs during the process of scanning!
+Auto-save of FTP list every 3 minutes!
+Additions to the mask for saving the list (ftp://login:password@server.ru)
+It's able to determine PageRank,AlexRank,YandexTCI
+Is able to sort FTPs by countries or PageRank, Yandex TCI, AlexRank (possible to separately save each PR/country, TCI and Alex in a file)
+the ability to save all settings in an ini file
+Detailed statistics of program work!
(Record statistics, PR Statistics, Valid/invalid FTP statistics, code replacement statistics)
+Ability to change the name of the FTP client
+Ability to search domains on the FTP and write them to a file
+Ability to search cgi-bin directories on the FTP and to write them to the file
+Ability to use the cache for the directory
Advantages over php checkers/iframers:
1. Very fast.
2. Can be launched in a Windows environment.
3. Flexible configuration.
4. In the CHECKER mode, without determining the PR the FTP eats little traffic!
5. Inexpensive compared to competing programs!
6. Able to work on a SOCKS4 connection!
7. High quality recognition of foreign iframes!
8. Able to copy the file given to a web directory!

Price of the program: **100$**
Price of source code: **not for sale**

These posts all demonstrate that hackers have the ability to access and utilize FTP resources for a variety of malicious activity. It is important to note that there was some equilibrium between the supply and demand for FTP resources and tools in the forums. Twelve individuals requested FTP accounts in 15 separate threads (55.6%), while only 12 individuals posted resources for sale (44.6%). Individuals who requested FTP resources were, however, very specific in what information they sought. For example, yM3 in forum 05 noted that he wanted to "buy .gov, for an expensive price. I am interested in Shells, FTP with recording rights, and admin in web directories. Preferably FTP. . . It is an excellent way to earn money, better then breaking regular sites for pennies. I will be waiting for your offers." Similar posts were found across the forums, as in this post from h3rcul3s: "I'm regularly buying ftp accesses with rights to record to the root (index) of all domain zones from PR [Google's Page Rank Status] =>5, except for ru (except for PR>5)!" Thus, these posts demonstrate the value of access to FTP resources for computer attackers.

Bot Malware

The final type of malware offered in the markets were bots, which constitute 6.5 percent of all malware bought and sold (see Table 5). Seven individuals offered either unique executables of bot programs or to lease out their existing infrastructure. For example, pogen5 offered "hack software, cheap" in a post in forum 02 which included two bot programs. His ad briefly described this malware, writing: "DDOS BOT Xerion 2006 v 1.3.b07 goes for $80 with the guidelines of the deal, the author sells it for approximately $1000. DDOS BOT Plutonium 2006 v 1.3.3.7 goes for $85 with the guidelines of the deal, the author sells it for approximately $1000." Additionally, a seller in forum 01 advertised a bot program designed to use zombie nodes as proxies that could be used for Internet access:

> **FF Http Bot v1.0 - Proxy bot**
> First experiment with an http bot For now I'm selling it at a very low price for a bot.
>
> **What it can do:**

> * HTTP proxy installation.
> * Flexible administrative console.
> * The possibility to create a service based on the admin console
> -* Client/admin system the client only looks at the proxy, the admin console administers all the proxies, admin uzers.
> * The percentage of good proxies out of 100 loads is ~50 (good connect, hangs online for a long time, accessible connection)
> * Convenient bot statistics
> * Script ping every 5 minutes
> * Writes itself for autoload (the proxy won't die after re-loading)
> * Bypasses Windows Firewall
> * Size 17kb - unpacked
>
> **What to expect in the next version:**
> * GeoIP database look at statistics by countries
> * Selection by countries
> * Uptime of each proxy
> * Bypass of firewalls
> * Improved addition to autoload
>
> For $40 you will get you own build bot, admin consol for it + I will configure all the scripts for you.
>
> The price will grow at it is updated. Those who buy now will get updates for free.
>
> In order to launch all of this, you need to have hosting + mysql.
>
> Knock on icq to buy

Two individuals also offered to lease out their botnets, as in this post from sal3nt who indicates how his network can be used for various forms of cybercrime:

> **Lease of bot networks!**, $100 a month (volume 6.9k online from 300 [nodes])
>
> **I'm leasing the admin console of a bot network!**
>
> **-** there are ~9,000 bots in the network (200-1,500 online regularly)
>
> **-** Countries: **RU,US,TR,UE,KI,TH,RO,CZ,IN,SK,UA**(upon request countries can be added!)
>
> **-** OS: **winXP/NT**

functionality:

[+] list of bot socks

type:

ip:port time (when it appeared the last time) Country|City

[+] loading of files on the bot machines (trojans/grabbers...)

[+] executing shell commands using bots

[+] Generates lists (**ip:port**) online socks in a **txt** file

ps admin console quite simple, convenient and functional, even a school kid can figure it out.

Today 1,000 more (mix) bots were added with good speed indicators + every 3,4 days 2k fresh machines are added (the person who works with the reports receives a unique service with unique and constantly new machines)

Super price**100wmz** a month!

all questions to **icq:** [number removed]

Spammers are in shock over such an offer (:

ps: we also make networks for individual **requests/orders**

These posts demonstrate that there are a sizeable number of botnets operating online. The number of requests for botnet programs was, however, equal to the advertisements for bot programs. This convergence suggests that there may be some balance in both the supply and demand of botnet resources. Additionally, the average costs of bot services were higher than that of iframe resources at $322.27 (see Table 6). The price is, however, inflated by a number of posts made by individuals seeking custom bots, particularly in forum 10. For example, n1k0n posted an ad in this forum seeking:

> Socks bot developer needed, ring0 technology. I need someone who is able to write a socks bot in asm or C++ with loader function which bypasses proactive AV protection using ring 0 or ring 3 technology, multi-thread...

Another individual named ph0t0n wrote: “I'm buying a Back-connect Socks Bot-? with an HTTP Gate (Admin console) Transaction only through a guarantor or positive recommendations.” Though bots comprised a small percentage of all resources available, they were clearly operating in competition with other malware. Additionally, the small volume of posts related to bots, and the balance between buying and selling requests noted may be a consequence of the range of botnet-driven services available.

CYBERCRIME SERVICES

The second largest category of products sold in these forums comprised services that enabled individuals to engage in a variety of cybercrimes, including Distributed Denial of Service (DDoS) attacks, spam, attacks, and hosting content on-line. Cybercrime services composed 30 percent of all products and services sought in these markets (see Table 4 for detail). This section will explore each of the resources offered in detail.

Spam Services

The primary service offered in these forums related to the distribution of spam, or unwanted messages to email accounts, ICQ, and mobile phones. These resources comprised 32.4% of this market, with 32.4% of ads related to services to support or distribute spam messages (see Table 7). Eight sellers offered to distribute email spam around the world, with pricing dependent on the number of messages sent and the country that will be spammed. A thread started in forum 03 exemplified this service, stating:

> Good day dear visitors of the forum. . . I would like to offer to you a service of quality email sending. At this moment I am offering the sending service not only for the same base, but also a selection to different countries.
> Price for a million of delivered mails is starting at $100, and drop real fast, practically to $10, for regular clients. Selection of countries is free.

Table 7: Cybercrime Services Offered in Hacker Forums

Resources	Number of Posts	% of Total	Buy Posts	% of Total	Sell Post	% of Total
DDoS	29	13.0	0	0.0	29	100.0
Hacking Services	30	14.0	16	53.3	14	47.7
Compromise	11	36.7	6	54.5	5	45.5
Email/passwords	19	63.3	10	52.6	9	47.4
Proxies and VPN	25	11.4	4	16.0	21	84.0
Proxy	20	80.0	4	20.0	16	80.0
VPN	5	20.0	0	0.0	5	100.0
Spam Services	71	32.4	14	19.7	57	80.3
Databases	33	46.5	7	21.2	26	78.8
Services	23	32.4	3	13.0	20	87.0
Tools	15	21.1	4	26.7	11	73.3
Webhosting and Services	64	29.2	6	9.4	58	90.6
Domains	24	37.5	2	8.3	22	91.7
Hosting	30	46.9	3	10.0	27	90.0
Registration	10	15.6	1	10.0	9	90.0
Total	219	100.0	39	17.8	180	82.2

Additionally, five individuals offered to send out spam to ICQ numbers. The spam messages sent could be advertisements, or simply a flood of blank messages to knock an account off-line similar to a DDoS attack. For instance, an individual in forum 01 would spam or flood ICQ numbers. His post demonstrates the discounts available based on the volume of spam ordered:

> **Spam Flood, Cheap service**
> **SPAM on ICQ**
> 1 500 messages ------ **????????? ??? ??????? ???????????? ??????**
> 2 000 messages ------ **9 wmr**
> 5 000 messages ------ **24 wmr**
> 10 000 messages ----- **30 wmr**
> 15 000 messages ----- **36 wmr**
> 25 000 messages ----- **54 wmr**
> 50 000 messages ----- **114 wmr**
> 100 000 messages ---- **180 wmr**
> 200 000 messages ---- **330 wmr**
> 500 000 messages ---- **600 wmr**
> 1 000 000 messages -- **1050 wmr**
> **Spam criteria:**
> **1)High speed distribution of messages.**
> **2)A screen as proof**
>
> **ICQ flood services.**
> Prices per item:
> 100 messages ------ **3 WMR**
> 500 messages ------ **15 WMR**
> 1000 messages ----- **27 WMR**
> 2000 messages ----- **50 WMR**
> 5000 messages ----- **100 WMR**
> 10000 messages ---- **190 WMR**
> 20000 messages ---- **300 WMR**
> 50000 messages ---- **750 WMR**
> 100000 messages --- **1350 WMR**
> **How [c]an one pay?**
> **You can pay with WebMoney**
> **30 wmr (WMR)-Rubles**
> **30 Yandex rubles**

Six sellers also offered to spam or flood mobile phones with SMS messages. The cost of these services was also based on the number of messages sent. As a whole, the average cost of spam distribution services was $50.91, suggesting this is a relatively inexpensive service (see Table 8).

Table 8: Pricing Information For Cybercrime Services*

Product	Minimum Price	Maximum Price	Average Price	Count With Price	Count With No Price
DDoS**	0.41	25.00	14.26	22	7
Proxy	0.50	200.00	42.53	9	11
Spam Services					
Databases	0.50	100.00	45.43	10	23
Services	0.50	700.00	50.91	12	11
Tools	2.00	180.00	59.11	9	6
Webhosting and Services					
Hosting	0.85	300.00	48.89	14	16
Registration	9.00	150.00	50.17	6	4

*Due to significant missing data, hacking services, domain sales, and VPN service pricing are not included here

** Due to variation in pricing, DDoS estimates are based on the stated hourly rate or an average hourly rate based on prices for 24 hour attacks.

Individuals also sold or sought out email databases that could be used to create distribution lists for spam delivery. Databases sales and requests comprised 46.5 percent of the overall spam threads. Twenty-four individuals across five of the sites sold databases for spam, such as a seller from forum 02 who noted: “I'm selling a database of soapmills [e-mails] with passwords on mail.ru, list.ru, inbox.ru, yandex.ru, rambler.ru.” The cost of spam databases also varied based on the number of emails and the country location for each address. For instance, a seller from forum 05 advertised: “There's a spam database for France being sold, in the base there are 1.5 lams [million], fresh database, I'm asking 40 Wmz for the database / Whoever needs it knock on [icq number].”

Two individuals combined both database and distribution services, as noted in this post from forum 03 stating:

> I would like to offer for your attention a service for mass mailings.
> Acceptable prices, good quality, high speed. I both to my bases for the USA and Europe or to countries which interest you, but I can also sent you letter using your own databases, which will be immediately deleted after the mailing - this is your property.
>
> Prices:
> **120$**- for 1 million inboxes! according to the GI bases.
> **150$** - for 1 million in boxes! by countries: US,AU,NZ,UK,IT,DE etc.
>
> Spam for jobs (USA):
>
> 100k - **200$** for spammed databases (1.8 mln)
> 100k - **300$** for new databases. (300k)
> Daily database update.
>
> Dating spam (USA):
>
> 100k - **200$** for spammed databases (1.8 mln)
> 100k - **300$** for new databases. (200k)
> update once a week.
>
> Note:
> - I don't spam Children Porno.
> - Mailing of certain themes to the databases costs more.
> - I don't take responsibility for your mail and the sites which sometimes arrive during the spam process. Use bulk hosting.
> - Fraud is allowed.
> - The price mentioned above doesn't change for mailing to your databases.
> - I am not responsible for the response rate.
> - Prepayment 100%
> - I don't do tests, all the minimum volumes are listed in the pricelist.
> - The price for attached files is +50$ up to 50kb although the soft handles much more.
> - I don't spam in the RU zone.
> - I do not provide consultation.

Prospam in forum 03 also sold distribution and database services, at a slightly reduced price and noted that his service hinged on a large botnet:

> Spam Professionally. We send out spam around the whole world, fast and with quality.
> The bases are constan[t]ly updated, validity and percentage of inbox is high.
> 1million is $100

> from 10million it is $90
> from 25 million it is $80
> from 50 million it is $70
> With questions and offers, please turn to us. . .
> P.S. the BOT net is new quick sending 15-30 million messages. Validity of the bases and percentage is very good. There is another person that handles the bases.

There were seven threads related to either buying or exchanging specific databases for spam. For example, koopa started a thread in forum 03 stating: "I am interested in fresh email bases for entire Russia and mail.ru. Please direct your offers to [icq number]." Similar requests were found in forums 01, 04, and 05. These threads demonstrate that there is a significant supply of databases to facilitate the distribution of spam within these markets relative to the demand.

Finally, there were 18 threads (21.1%) pertaining to spam tools, including scripts and mailing programs to enable the distribution of spam. The average price for spam tools was $59.11, suggesting these resources are less expensive than other malicious software sold on the market (see Table 8 for detail). For example, sendking created a thread in forum 03 to advertise a spam tool stating: "I am selling a private direct mailer for $100. If anyone needs it write in my ICQ." Some also offered spam scripts, as in this post from forum 04 as he described his service:

> New script for email spam. Cost is 500 rubles, plus free renewals. Test check was done through [an external website], passed successfully. Here is the configuration:

```
$host = 'smtp.mail.ru';
$port = 25;
$login = 'login';
$password = 'password';
$name = 'name';
$from = 'mail@mail.ru';
$subject = 'subject';
$max_threads = 20; // "Multithreading"
$wait = 1; // sleep(seconds)
$proxy = 1; // 0 - nosocks, 1 - socks4, 2 - socks5(auth)
$html = true; // true - html, false - plain
$mess =
'
```

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Untitled Document</title>
<style type="text/css">
<!--
body {
  background-color: #000000;
}
.style1 {color: #0000FF}
-->
</style></head>

<body>
<span class="style1"><a href="http://localhost">TESTHTML</a></span>
</body>
</html>
';
?>
```

Taken as a whole, these posts indicate that the creation and distribution of spam mail has become a service economy driven by hackers and botnets. Additionally, spam can be cheaply created and sent to potential victims around the globe. As a result, these markets enable individuals to easily engage in a common form of cybercrime with minimal knowledge of computer systems and networks.

Domains, Registration, and Web Hosting

The forums also offered services to support a variety of malicious web content and attacks. Hackers need resources to host malicious content, such as malware or cracked software, as well as send out spam and engage in other attacks, so groups offered their services for web hosting. Web hosting and domain resources comprised 29.2% of the threads related to cybercrime services in these markets. There were 30 threads related to web hosting made by 22 different usernames in five forums (see Table 7). Additionally, there were only three requests (10%) made for web hosting services, suggesting there is a strong supply of providers available. Descriptions of the hosting services varied depending on the level of support provided and gave prospective buyers insight into the quality of service they will receive. This was evident in a post from the seller duc3c3 who advertised in multiple forums:

> Our shared-hosting service is equipped with and the instruments you need for your work. If you don't have some module, then with a request to support - we'll supply it for you (only regarding virtual hosting). RAID technology is installed on all of our hosting servers, which excludes the possibility of your data being lost. Furthermore, every day your back-ups go to a SEPARATE independent server, which completely excludes the possibility that they might be lost.
>
> Abuso-resistant dedicated servers for any purposes with high bandwidth access channels in Moscow, Hong Kong, the USA, Malaysia and also legal servers for various project at affordable prices.
>
> Our own IP network in Hong Kong !!
>
> (The installation of an OS at the request of the customer (Fedora Core, CentOS, FreeBSD, Debian).
>
> Control panel:
> -DirectAdmin
> -cPanel
>
> Remote reboot panel ! Everything you need for your successful business.
>
> *We do not take responsibility for any losses which occur due to our service being unavailable. The amount of the lawsuit may not exceed the amount for providing our services. We take responsibility only for our service and not for anyone else's.
>
> **Dedicated servers are sold in an UNMANAGED condition (you yourself maintain and configure your server for your needs).
>
> ***MoneyBack for a dedicated servers is possible only if the unavailability of this server occurs by our fault (inasmuch as we pay the full cost of the server in the Data-Center). Replacement of the server is also possible.

This post demonstrates the high degree of support offered by hosting service providers. Additionally, the discussion of legal and “abuso-resistant servers” highlights a key issue in web hosting. Individuals offering web hosting understood that individuals in these sites may misuse the resources that they offer. As a result, sellers would indicate what content they viewed as unacceptable at some point in their advertisement. For example, the seller gh0st1n in forum 04 noted what his servers could not handle:

> IS CATEGORICALLY PROHIBITED TO USE OUR RESOURCES FOR THE FOLLOWING:
> -Child porn
> -Zoophilia
> -Sites which promotes violence
> -Projects aimed at breaking into government organizations and executive branch bodies
> We try to do every thing so that your work with our servers
> proceeds most comfortably.

The restrictions concerning child porn and bestiality listed by this seller commonly appeared in other hosting advertisements. This may be a reflection of the prevalence of laws against these forms of pornography around the world (Putnam and Elliot 2001) and significant law enforcement investigations against child pornography in the United States (Taylor et al. 2006). Hosting this content may pose too much of a risk for a seller, and is considered unacceptable. Other forms of cybercrime were, however, welcomed as in this post: “I'd like to offer for your attention a hosting service for resources with "non-standard" content: Logs, sploits, trojans, warez, adult, drop-projects, botnets, SPAM and others.” The variety of malware highlighted in this post demonstrates the need for and intersection of malware and hosting. Thus, web hosting plays an important role in facilitating cybercrime and are a key service in these markets.

Hosting service advertisements usually dictated prices based on the amount of storage space required and offered a tiered pricing structure. This was exemplified in an advertisement by cub3 in forum 04:

> Anti-abuse hosting service from [cub3].
> I am offering the anti-abuse hosting-hosting for projects of non-standard content.
> About the service:
> -100% pay upfront, regardless if is done through guarantee of any famous forum.
> -Individual approach to each client.
> -Discounts to regular clients.
> -We are working 14 hours a day, Sunday is a day off.

> -Distribution of drop projects through negations personally with the service owner -We have the right to deny service without giving reasons.
> Prices per month:
> New Year Discounts:
> **100mb = 20$ per month**
> **200mb = 30$ per month**
> **300mb = 40$ per month**
> **500mb = 50$ per month**
> **1gb = 100$** per month
> Prices can increase depending on the server download.

The range of prices evident in this post is reflected in the average cost of hosting services, which was $48.89. In fact, the lowest advertised price for hosting was 50 cents, suggesting this service can be obtained for a very low price depending on one's needs (see Table 8).

There were also seven individuals who sold web domains in multiple forums, comprising 37.5 percent of these services (see Table 7). In fact, sellers would often offer the same domain in multiple sites. These resources could be used for legal or illegal activity, though some sellers specified the utility of their products. For example, individuals in forums 01, 02, and 03 regularly sold web domains with names such as club2110.ru, Moskva.ru, and erohit.ru. An individual in forum 03, however, sold bank-related domains that appear to be useful for phishing. His post stated: **"**May be someone will be interested? Knock on ICQ. . . or personal message. empresas.ebankinter.com, ib.bankcolonial.com, my.dsbbank.sr, banking.postbank.de, idbibank.co.in, fidelity.com, dk.etrade.com, nettrader.ru." Only two individuals sought out specific domains, such as ski11z who created a thread in forum 03 seeking computer security themed sites that have a good search rating in Google, or a "good" domain name. Thus, there appears to be a ready supply of web domains made available to hackers in these forums.

There were also nine individuals who offered domain name registration services, as noted by hostmaster in forum 02:

> Domain registration
>
> **RU - 14$**
>
> **.COM .NET .NAME .BIZ - 7.5$**
>
> For more detail here. Instant registration
>
> Domain reselling
>
> Since we register a large number of domains, our company receives significant discounts from accredited registrars.
>
> And for just this reason our prices for reselling domains will pleasantly make you happy [sic].
>
> ATTENTION SALE!
>
> Before the May holidays and in the period up through 10 May inclusively!
>
> **RU - 14$**
>
> **.COM .NET .NAME .BIZ - 6.5$**
>
> Payment, registration and administration of domains accessible in real time (online) through the administration panel by domain reselling [sic].
>
> If you have your own hosting-company or site creation studio, if you periodically need to register domains in various zones, we can help you save ore earn on reselling domain names.
>
> All domains are registered only through accredited registrars (without intermediaries), which gives guarantees and clients' full rights to the registered domains.

Unlike hostmaster, a seller in forum 01 using the handle nada was quite specific in describing how his products could be used to engage in cybercrime, stating “http://juhost.ru - domain registration from $4, hosting from $2 for 200mb, all types of sites (warez [pirated soft], adult).

All questions can be clarified online with the operator." These discussions indicate that a solid infrastructure exists for hackers to host and develop malicious web content. Such services simplify the process of engaging in cybercrime by providing the necessary resources for a small fee in these forums.

Hacking Services

The forums examined in this study also offered access to individuals who would perform attacks against different targets. There were 30 posts advertising hacking services for those who did not have the requisite skill or ability to accomplish a task. Hacking services composed 14% of posts related to services, and appeared to fall into one of two categories (see Table 7). The first was account related, including obtaining passwords for email accounts or acquiring accounts from websites and forums in a surreptitious fashion. Eleven ads were identified in this sample of threads, with a relative balance between sellers (45.5%) and individuals seeking services (54.5%). For example, an individual in forum 01 created a thread asking for assistance in gaining the password for an email account:

> Odnoklassniki.ru- receipt of password and email. It interests me whether it is possible to receive the password and email of a person who is registered at odnoklassniki. And what the price of the question is. . . .Another option is possible, to find out the email of a person on odnoklassniki and open the mailbox. I guarantee payment.

Five individuals advertised a similar sort of service, as noted in this post from forum 05: "Hacking into the mail for order. Hacking 100%; full anonymity. No pre-pay. Pay by facts. Any support for hacking into the mail. . . hacking into electronic mail (email), without any collateral or pre-pay. Contacts: ICQ [number removed]." These advertisements illustrate that there is a small market to assist in gaining access to email and other electronic accounts.

The second type of request identified involved compromising or attacking a target in some fashion. There were 19 requests for compromise assistance with a similar distribution of buyers (52.6%) to sellers (47.4%). Specifically, 10 individuals requested assistance in obtaining access to different systems. For example, 1atera1 posted a message in forum 05 stating: "I need help with hacking two FTP servers. Who can realistically hack, write into personal message. We can agree about the price, guarantee is welcome." Similarly, a user in forum 03 sought assistance for a project:

> I needed bases from these sites, at least some of them. The list is bellow.
> freightquote.com
> 1800members.com
> freightclick.com
> freightcenter.com
> freightmanager.com
> uship.com
> If someone can help, with your price knock for additional information here, ICQ. . . I have a favor to ask from all the ripp [SIC] offs and cheaters, do not knock. Offers such as money first or guarantee. Stuff like money through guarantor, the favor is do not write me.

Nine users also advertised hacking services to order. For instance, an individual advertized his service in forum 03 in simple terms: "I'll do custom break-ins of highPR [Page Rank] blogs / sites / forums. . . The price of the custom break-in will be discussed individually with the customer. I don't deal in downloads, bundles, trojans and traffic. I accept only WebMoney." Similarly, an individual advertized a hacker team's services, stating: "Password recovery: Email: $20-$40 ICQ: Negotiable ZIP: $10 RAR: $20 MS Word: $10. Testing Web-Servers for escapability: $30 Writing software for order: negotiable. . . .With questions of all services write to [email address removed]." These posts indicate the value of hacking services, and the demand for individuals who have the ability to attack various systems. Thus, the markets enable individuals to engage in forms of cybercrime that may exceed their technical capabilities.

Distributed Denial of Service (DDoS) Attack Services

An additional service identified in these forums involved individuals offering access to distributed denial of service, or DDoS services. These services comprised 13 percent of the overall posts related to cybercrime services in these forums including 29 ads across four of the forums (see Table 7 for detail). DDoS providers' resources enabled buyers to keep a website from being accessed by other individuals over the Internet. Typically, DDoS attacks operate by flooding a web server with requests, and not completing the information exchange necessary to complete the request (Brenner 2008; Wall 2007). As a result, the server is not able to complete any other requests until the existing connection requests are resolved, and individuals are not able to access the webpage for the duration of the attack. Sellers regularly noted the reasons why an individual would need access to such a service, and would explain their product in detail. This was exemplified in a post from forum 03:

> ⚠**Quality DDoS-Service !!!not expensive!**
> I am happy to offer our new DDoS-Service to you.
> I will strike down the site of a competitor or someone who has insulted you without difficulty....
> Prices and terms are one of the best on the DDoS market:
> I provide a 10 minute test of the DDoS
> 1 hour- 15 wmz
> 12 hours -45 wmz
> 24 hours - 90 wmz
> 48 hours - 180 wmz
> Difficult projects are negotiable. (from 150 wmz per 24 hours)
> DDoS organized using bots!

These comments indicate that botnets provide the infrastructure for DDoS service providers. In fact, some sellers detailed the scope of the botnets supporting their services, such as a service provider from forum 03 who noted that "A large army of bots is always online, everything is quick and rapid . . . Complete anonymity." Another vendor noted that their infrastructure was supported by "Large quantity of BOTS on-line, quantity grows everyday. BOTs are located in different time belts [zones], which allows the DDoS to work 24 hours a day." These ads suggest that botnets have significant penetration and global scope.

There were no requests for access to botnets for DDoS attacks in any of the sites, suggesting these products have saturated the market and are readily accessible to interested parties. The average cost for DDoS services was $14.26 per hour, indicating that this service is also relatively inexpensive (see Table 8 for further detail). Thus, botherders recognize the value of their existing infrastructure, and utilize it to make additional money.

Proxy and VPN services

The markets examined in this study also offered an important service for hackers: access to proxy services and Virtual Private Networks (VPN). Though these resources composed on 11.4 percent of the overall service category, proxies can be used to conceal an individuals' IP address and location (see Table 7). The use of a proxy reduces the likelihood of detection while engaging in attacks or malicious activity on-line (see Furnell 2002; James 2005; Wall 2007). Specifically, proxies allow an individual to route packet traffic from their computer through IP addresses on a proxy server, thereby concealing the individuals' location (see Wall 2007). There were 20 threads related to proxy services found in these forums, and 16 (90%) of these threads were sales related, suggesting there is a good supply of proxy resources available (see Table 7). Sellers would note if the proxies they offered were SOCKS based, as this protocol operates differently from an HTTP proxy. For example, the seller mount31 advertised a SOCKS service in forum 03:

> Store of socks.
> These are:
> -Elite, 100% anonymous socks
> -Large quantity of online socks. Renewal is in realtime
> -Choice of cities and countries

> We give out fresh damps of proxys [SIC] from bases (Renewed every 5 minutes in the base). Because of that 99.9% of socks in the base are working. You can see the socks in your account of countries and cities.
> Over 1,000 socks online at all times. The quantity of socks grows with every day, the base is always filling up. Added is the automatic pay with the help of the WebMoney system, as well as autoregistration. Now, it is not required to knock in ICQ and wait for an answer if you need a sock real soon. You sim[p]ly register and pay in your account for the chosen packet, or fill the balance of your account for any sum, and use the socks. When buying any tariff plan from us, you also receive an indicated quantity of socks into your account with an autorenewal and exchange for the "dead" proxys every 10 minutes. This means that after buying from us a tariff plane Pioneer for example, you receive onto your account 5 working socks and if within 10 minutes one of them happens to be a non-working one, it will be exchanged for a fresh one. Because of that you always have an access to fresh socks in your account. The price of a single socks based on your request of Country/City-$0.50. Tariff plans and packets are:
> Pioneer ....5.........20$
> Advanced........10.......30$
> Clasic................30.......70$
> ElitE....................50.......120$
> V.I.P...................100.....200$

The pricing tiers and structure observed in this post were noted in other advertisements, supporting the average cost of proxy services at $42.52 (see Table 8). The volume and global distribution of proxies described in this post suggests it is likely that proxy services operated through zombie nodes of a botnet or other malicious software infection. In fact, a seller from forum 05 described his proxy service and explained the way his proxies were collected:

> We are selling proxy.
> We are offering to your attention our proxy-service for sale of anonymous and elite proxy. Proxies are partially taken from the public, partially from private. Ports are different. Proxies ideally match the CEO spam and etc.
> Why do we use from public?
> Just because they live either way longer, then the private trojan types (majority in itself). List update occurs every 5-10 minutes, which happens to be optimal. Validity is acceptably big. Usually not less then [SIC] 50-60%, which is very good, and will reflect upon the speed of your spam, since the spam will be needed for less time, in order to find working proxy in the list. Methods of receiving the list can be discussed separately. Prices are pleasant. We give a test prior to purchase, so that there are no complains about cheating and etc.

This post demonstrates that proxy service providers operate over an infrastructure of malicious software and provide support for spam and other forms of cybercrime.

Similarly, four individuals (10%) offered access to Virtual Private Network (VPN) services which operate differently from SOCKS proxies (see Table 7). VPNs can be secured and encrypted as a way to conceal user information and provide privacy in unsecured networks. Often, individuals must log in to a VPN, and then all of their traffic is directed out through nodes on the service network. This structure conceals an individual's actual location and machine information from others. One of VPN provider, slam, described their service in detail, stating:

> Our company. . . is pleased to provide you with quality, reliable, and secure pptpVPN and openVPN access.
>
> I would like to note that our service is unique in that you can buy or extent the payment of your VPN any time of the day or night since our service is automated. You manage your account yourself, without the participation of the support team.
>
> At the current time we have servers in Germany, the Netherlands, Estonia, Malaysia and the USA, and there will be servers in other countries as our service grows.
>
> Payment may be made a day, a week, a month, 2 months, 3 months, 6 months or a year in advance. The greater the time period, the bigger the discounts. . .
>
> You can find more detailed information on the site [external link]

This post demonstrates the value of VPNs, as they operate around the world and provide a degree of security and anonymity that is invaluable for hackers. Thus, proxy and VPN services play an important role in facilitating cybercrime by reducing the risk of detection by law enforcement and other security entities.

STOLEN PERSONAL INFORMATION

The third most prevalent category of resources sold in these forums included fraudulently obtained financial accounts from banks, online accounts, and access to personal information.

These goods and services represent 13 percent of the market, and are elaborated in the following section (see Table 9 for breakdown).[5]

Table 9: Stolen Personal Information Offered in Hacker Forums

Resources	Number of Posts	% of Total	Buy Posts	% of Total	Sell Post	% of Total
Credit Cards	17	18.5	4	23.5	13	76.5
Drops	7	7.6	2	28.6	5	71.4
Malware Log Files	9	9.8	1	11.1	8	89.9
On-line Accounts	39	42.3	11	28.2	28	71.8
Passport Services	17	18.5	2	11.8	15	88.2
Software	3	3.3	1	33.3	2	66.6
Total	92	100.0	21	22.8	71	77.2

On-line Accounts

The most prevalent item sold in these forums included access to a variety of on-line accounts that could be used to engage in fraud or theft (see Table 9). For example, a seller in forum 05 created a thread offering access to accounts on Russian auction and commerce sites, stating:

> I am selling accounts. I am selling accounts on molotok (molotok.ru) [an auction site], balance 702 rubles and ozon accounts (ozon.ru) [a retail site] with 212 rubles on the account. I will give away for 15%. Also, if someone needs it, I can give accounts stream for 10%, with different balances. 338 rubles, 359 rubles, 494 rubles, 1338 rubles. Knock in ICQ.

[5] Due to the small number of requests, software is not discussed in this section. These requests comprised individuals seeking access to credit card creation or validation software, as well as one person providing access to this resource.

Similar posts were found across four of the forums, as in this post from 5313ct0r in forum 01 who offered to sell skype accounts: “skype sale: I'm selling account for 50% of the amount in the account. Minimum 10$ - price 5 WMZ [Web Money USD] ICQ [number removed]” Additionally, a user in forum 04 posted the following advertisement:

> I will sell verified accounts of PayPal or I will open and will verify to any name. Only USA. You receive log in and password to the account, access to the email, to which account is registered, bank account numbers, which was used for verification. Knock in ICQ. . . (even if I am online. I will answer when I get back.)

On-line casino accounts were also available for sale in the forums. For example, timer posted the following message in the 03 forum: “I will sell fidelity, bcs.ru, dk.etrade.com, cyberbingo.com, online.person.com, gamebookers.com, partypoker.com, betcity.ru. Minimum balance is 10K.”

These examples demonstrate that many on-line accounts are not safe from compromise by active hackers. These types of accounts comprised 42.3 percent of all posts related to stolen data. In addition, there were 28 threads selling account information (71.8%), relative to 11 request-related threads (28.2%), suggesting there is some ready supply of information already available. On-line accounts were also significantly more expensive than the other resources sold, with an average cost of $156.79 (see Table 10). Thus, consumers should take care to safeguard any and all resources where they may have stored sensitive financial information.

Table 10: Pricing Information for Stolen Data

Product	Minimum Price	Maximum Price	Average Price	Counts With Price	Counts With No Price
Credit Cards	2.00	55.00	10.66	8	9
Drops	7.00	141.79	40.75	3	4
Malware Log Files	1.75	220.00	55.00	8	1
On-line Accounts	1.50	2000.00	156.79	13	26
Passport Services	1.00	150.00	20.27	8	9
Software	20.00	250.00	63.55	2	1

Credit Cards and CVVs

Participants in the market also sold credit cards and bank accounts obtained through different methods. This information was sometimes referred to as a dump, and was sold at different prices depending on the customer data associated with each account. Nine sellers offered credit card data, and advertised their products noting the country or region of origin and the information associated with the account (see Table 9). Dumps may include Track One and Track Two data contained on the magnetic stripe of each card. Track One stores the cardholder's name as well as account number and other discretionary data (Newman and Clarke 2003). Track Two data is the most commonly used track, and contains the account information as well as other discretionary data (Newman and Clarke 2003). Sellers would sometimes specify which tracks were included in their data, as demonstrated in this advertisement from forum 06:

> VISA/MC CLASSIC/STANDART
> < 100 - 15$/dump
> > 100 - 10$/dump
>
> VISA/MC GOLD/BUSINESS/SIGNATURE/PLATINUM
> < 50 - 25$/dump
> > 50 - 20$/dump

> AMEX/DISCOVER
> < 100 - 10$/dump
> > 100 - 7$/dump
>
> -------------------
>
> icq: [number removed]
> e-mail: [address removed]
>
> -------------------
>
> Dumps without pin [Personal Identification number], they have the first and second original track.
> I don't provide any consultation, exchange is not valid 24 hours.
> The database is frequently updated.
> Method of payment: WU, WMZ

Four individuals also offered credit card accounts with CVVs, or the Card Verification Value, which is a three or four digit number imprinted on the card and in the magnetic strip (Newman and Clarke 2003). The CVV number is designed to ensure that a card is present with the card holder as a means to reduce theft and fraud. These numbers are now commonly maintained in on-line databases during transactions making this information easier to obtain by thieves (Franklin et al. 2007; Newman and Clarke 2003). A seller in forum 03 offered such information, stating: "I am selling CC with CVV2. USA-1.50wmz, UK-2.00wmz. Each one is checked for 90% validity. Invalid cards will be exchanged in 24 hour period." Some sellers were less specific about the information associated with the account. Instead, they listed the cost of their cards, as demonstrated in a post from a seller in forum 04:

> Good time of the day. Service for selling cards, any selection.
> 1 Credit Card, master card or Visa=$1.50;
> American Express is $3.00, EU (Euro Cards)-$3.00.
> Price can change depending on the selection.
> Discounts to regular customers.
> I do not give the card for verification, if you want to check it, buy 1 card.

The sale of stolen financial information enables individuals to engage in identity theft and fraud, and represents a small, but important threat within these markets. Credit cards could be obtained for an average cost of $10.66 which is low relative to other goods (see Table 10). There were fewer requests for these resources than sales posts suggesting there is some market presence for these resources. It is important to note that a smaller percentage of credit and bank account information was sold in these forums relative to markets operating on IRC (see Franklin et al. 2007; Thomas and Martin 2005). This may reflect variation in the location of a market and the products that are offered, though further exploration is needed.

Passport Services and Identity Documents

A number of individuals also sold or sought access to passport scans and identity documents as a means to facilitate identity crimes. These services constituted 18.5 percent of posts related to stolen data (see Table 9), and were posted by 17 different individuals across four of the forums. The detail provided in advertisements by passport sellers suggested that they had access to a great deal of sensitive information about individuals around the world. For example, a seller from forum 04 gave very specific detail about the information he sold, stating:

> I offer a service for selling and altering scans of passports, credit cards and other documents. There are around 60 countries, more than 3,000 scan's available, around 1,500 scans of credit cards, more than 100 different banks, various versions of sets of +billing, credit card, stateman [statement], rights, INN [Tax Identification Number] and others. Prices from 1$ to 5$ for a scan of CIS countries, from 7$ to 15$ for others. Alteration mostly for 15$ (+-5$). . .
> You can get information on the entire range of goods and services at [ICQ number removed]. . .
> Alterations within 1-3 hours if online, up to 12 hours if offline.

Individuals who purchase such information can use it to create new accounts, engage in fraud, and perform a wide range of illegal activities. This was noted by the seller v0dk@ from forum 03 who described the utility of his service:

> I draw scans of documents for different countries. There is a big base-4GB. There is a capability to do following documents:
> 1.Cards (visa, mc, maestro/cirus, amex, discover, rus bank)
> 2.Pasports/id (euro, usa, uk, russia, other)
> 3.Driving license (euro, usa, russia, other)
> 4.Statement (card, bank, account)

5.Bills (utility, phone, electric, other)
6. Zags (Proof of marriage, birth certificate, proof of divorce, death certificate, and others.)
7. Diplomas (Colleges, Schools, community colleges)
8. Photo Montage (for divorce of your husbands)
9. Screenshots
10. Checks
11. Verification of different enforcement structures/military branches (FSB for example- Federal Service of Safety.)

The supply of identity documents and information was significantly higher (88.2%) than the number of requests for such data (11.1%). Additionally, the average cost of passport service providers was $20.27, suggesting these resources were relatively inexpensive (see Table 10). As a result, these forums provide access to a surplus of resources to engage in serious forms of fraud and theft from victims around the world.

Malware Log Files

The preponderance of malware sold in these forums engendered access to stolen information via access to traffic logs and materials obtained through keyloggers, iframe infections, and other compromises (see Table 9). These log files may contain sensitive information such as usernames and passwords for email and bank accounts. The value of log files were noted by an individual named Jackal who suggested: "In logs you can possibly find useful information, passwords to log ins, ICQs, ftps, and etc. Anyways, you can for example, find password/log in from yandex, on which there may be 1,000,000 rubles or just different symbols you can sell." To that end, an individual named young999 from forum 03 described his service, noting: "Pinch logs; Updated counts. We have a large quantity, 1,000 for $15. Mix traffic, mainly Russia." Individuals often specified that their log files were typically obtained from the trojan Pinch, which was available from a number of sellers in these markets. The average cost of these products was $55 dollars, suggesting there may be a high return on investment for those who purchase log files should they find useful information in the data (see Table 10).

Drop Services

The availability of financial and personal information in the forums was tied to a unique service offered in these forums: drop services. There were seven threads related to drops services, which allow individuals to access and drain funds from credit or debit accounts. These resources facilitate the process of using stolen data, making it easy for an individual to acquire goods or money from the accounts they purchase. Vendors take a percentage of the total amount of money transferred, as noted in the following advertisement:

> I'm happy to offer users of this forum an encashment service for Great Britain!
>
> We always have **unduped** and duped drops **of all banks and payments** of Great Britain. We also accept transfers from Europe by international wire.
>
> we pay 25-30% of the amount of the transfer (for regular clients it is possible to increase the %). Payment is made by E-gold, WebMoney, and also by Western Union (other methods can be discussed separately by icq). The drops are almost all unduped, they work quickly, accurately and without excess questions.
> We accept sums from 3k, for payments from 1k. Pours [transfers] and interest on a smaller sum can be discussed with me separately by icq.
> Should the drop cheat (cannot be excluded, you can understand why) **compensation is possible**, % and terms can be discussed separately with me by icq.
>
> The[re] are also occasionally duped drops in the USA. The availability of drops in the usa, the % and terms via my icq.
>
> **Exclusively for the clients of our service:**
> -We provides drops for PayPal the terms and % are to be discussed separately with me by ICQ.
>
> - Now we cassh Epassporte! terms and % are to be discussed separately with me by ICQ.
>
> - We provide drops for the majority of well-known payment systems. terms and % are to be discussed separately with me by ICQ.

> - For people with a large number of logs and accs in the UK, we take your accs for cashing. terms and % are to be discussed separately with my by ICQ.
>
> - should it be necessary we will provide calling. Voice: male, language: English.

Drops also utilized the purchase and resale of electronics as a way to launder money from stolen financial accounts. Using a stolen credit card, an individual could buy electronics or other goods that have a high resale value and have them sent to an address. Subsequently, these items are picked up by a confidant and then resold and the money passed on to the individual who initially acquired the card. Such a program was offered in forum 06 as described in this post:

> I would like to offer for your attention a drop service in the USA for electronics.
>
> - A large choice of drops with choice of states and cities.
>
> -Your 30% of the cost of the goods according to pricegrabber.
>
> -Payment takes place 1-3 days after delivery in advance. . .
>
> We take goods such as: notebooks, digital cameras, mp3, computer components, dj equipment, mobile phones, gps, automobile sound systems.

Two individuals posted requests to identify drops services, as in this post from cahha in forum 03: “Urgent, people are needed for receiving envelopes (documents from a bank, European union (EU). Also, if you have drops for documents in other countries besides US and ex-USSR countries, also knock into ICQ. All conditions of the offer are in ICQ.” These examples demonstrate that a small service industry has developed to enable individuals to drain funds obtained through electronic accounts. Additionally, all manner of financial resources and personal data could be obtained in these forums.

ICQ NUMBERS

The final category of products available in these forums was ICQ numbers. It is not clear why individuals sold these resources, as ICQ numbers can be obtained freely through the service provider ICQ.com. Sales of ICQ numbers, however, composed 10% of all sales related threads. There were 52 unique sellers were found in 64 threads across five forums (see Table 4 for detail). Thus, there was a clear supply of ICQ numbers in these markets. One possible explanation for the sale of an otherwise free resource may be related to the mix of numbers in a given ICQ number and its overall length. Numbers that are composed of two to three digits are easier to remember, and numbers that are short in length can be an indication that an individual has been on-line for a long time. Additionally, a number can represent certain information about an individual, as explained in a post by an ICQ seller from forum 02:

> When buying an **Icq**number, many clients want their **Uin** [Unique Identification Number] to coincide with their cell phone number, home phone number or for example their birth date. There is one complication, that ordering a specific number is a very very expensive service, and there are few who can afford to give 35-95 c.u. [condition units, usually equivalent to USD] for a little number like that.
> Now the possibility has appeared to select a 7-digit number with numbers that you like from a large database which contains several tens of thousands of numbers. The percentage of those who are able to find a specific 7-digit that interests you is quite large.
>
> For example, you mobile number: **+79074576833**, it is possible to select 7 digits which will correspond to the 7 last numbers of your mobile "**4576833**". Or under the same birth date, for example if you were born on 31 August 1975 - **31.08.75** In this case, the number will be of the following type **?310875** or **310875?** - i.e. you birth date + some sort of number either at the beginning or at the end.
>
> The cost of this service is significantly less than 35-95 c.u. and starts from 300 rubles.

The length and digit combinations of an ICQ number affect its price, as noted in this excerpt from an advertisement by a seller in forum 04:

> Hello. In the world of ICQ I am known as an error. . . I have few beautiful ICQ numbers left, which I want to sell.

5-digit... Price is in WMZ
x4444 - 2500.00
x777x - 2000.00
100xx - 1200.00
abcba - 800.00

6-Digit... Price is in WMZ
222xxx - 2000.00
88888x - 1500.00
x11111 - 1500.00
55555x - 1200.00
x55555 - 1200.00
99999x - 1000.00
8xx888 - 800.00
x44444 - 800.00
8x8x8x - 700.00
5x0000 - 600.00
7x0000 - 600.00

7 digit... Price is in WMZ
xxxxxxx - 6000.00
x000000 - 2500.00
999999x - 600.00

Despite the preponderance of ICQ sellers across the forums, several users questioned the value of these products. For example, q-ver from forum 03 asked "why is this even needed?" Additionally, the average cost of an ICQ number was $4.44 per number, suggesting these products have very low value. Thus, the frequency of ICQ number sales may represent an unusual and tangential service in the forums identified in this study.

FREE DOWNLOADS

Though many products were bought and sold across the forums in this sample, individuals also gave access to malicious software and other resources free of charge. A wide range of hacker tools were available for download in four of the forums, including 163 different pieces of malware, hacking tools, and other programs (see Table 11 for detail). The majority of tools provided were some type of trojan, rootkit, or backdoor program (42.3%) including Nuclear

Grabber, Pinch, and Agent DQ. These programs have a significant reputation for data theft, phishing, and malicious activity (see James 2005) and were provided in some form free of charge. Iframe tools (16.6%) and bot programs (9.8%) were also available in some supply. For example, a thread in forum 09 was devoted to the distribution of a number of bot programs, including a single downloadable package titled 0wn3d:

> **0wn3d botnet pack**
>
> Include:
> Rxbot command list
> Botnet Guide - Rezo and wewt
> AV_Devil2
> Celsiusi
> eXPressor
> R00tkits - Feliks
> icon sets - chasenet.org
> Themida 1.8.5.5 - f1r3f1y
> UD_methods archive - Ssgroup
> Bat_To-Exe_converter
> Binder Pack - Feliks
> ResHacker - For changing icons and version info
> Unreal 3.2 (modded + secure) -unknown
>
> **Sources:**
> Rxbot 7.6 (stable)
> Dbot 3.1 (modded)
> Rx-asn-2-re-worked v3 (very stable, one of my favorites)
> Ryan1918 botsources - ryan1918.c|o|m (many sources)
> SkuZ-Netapi-VNC-IM (good spreader)
>
> I want to thonk [thank] [names removed] for such an amazing pack.
> Download
> PS we'll make a mirror so that there will be no problems.
>
> pass: r00t

A similar example was found in forum 07, where an individual named Sartr3 wrote: "hi! You'll probably laugh that a novice wants to create a botnet, but I still want to try!" In response, the user jigsaw stated: "There's nothing to laugh about there. And regarding the sources (I'm sorry for being so banal), there are many that are public. . . If you don't find it then write- I'll dig around." The user then posted the executable for the malware program Gigabot in a compressed .rar file for others to download from the site. The tools available in these sites were accessed through links to massive file sharing sites like RapidShare, slil, webfile, or hacker forums and websites. These programs may either be password protected, or in the case of forum 03, accessed with registration to the forum and a certain number of posts.

Table 11: Free Tools Available in Russian Forums

Resource	Posts	Percentage of Total
Bots	16	9.8
Cryptors and Joiners	6	3.7
DDOS and Defacement Tools	8	4.9
iFrame Tools	27	16.6
Other Tools	13	8.0
PHP Tools	6	3.7
Spam and Email Hacking Tools	10	6.1
Trojans, Viruses, and Rootkits	69	42.3
Unknown*	8	4.9
Total	163	100.0

* A small number of downloadable materials were blocked from view, thus their payload was unknown.

The availability of free tools in forums 07 and 09 had a significant impact on the overall cost of products sold in the forums in this sample. Tools sold in the open market eventually lost their value as a commodity, and became available for free. Some individuals, however, downloaded these free materials and then sold them for a profit. A seller who engaged in such behavior was perceived as a cheat attempting to steal funds from other participants in the market. This was noted in a thread from forum 03 titled "Death to speculators!!!," that attempted to limit the resale of known malware by posting these tools publicly. For example, an individual named birdguy posted a well known bot program for free download and noted its initial value in the open market:

> I think that many have see[n] the bot from Dr. Pixel for sale – DCKS DDoS bot. The price at the time it was sold was 1,400 dollars (wmz), now this is accessible to everyone for free.
> Files:
> Admin_panel.rar – adminlet for controlling the botnet 9the author didn't tell the password) ;))
> Dkcs_ddos_bot_src.rar – the bot itself, its code is in c++
> SC_generateor.rar – program for translating the binary file into byte array (used in the bot)
> >>> Download

The imperative to create this thread was described in the initial post by zood, who felt it was necessary to keep individuals from engaging in speculation:

> **The topic has been created for various types of public and half-public material that was noted as having been used by speculators ("barygs," "re-sell-processors," exchanjers [exchangers] and other). Everything that you download from here you use at your own risk! Flooding and begging are forbidden - this is what PM [personal message] and other communications are for. If you don't decide to launch something from this topic, or if you don't know how to use it - you're better off not downloading from here and don't even try. The discussion of one or another software is also forbidden. Create a topic for discussion with special sections is strictly forbidden in this topic . . .**
>
> **Sources KyrgyzTrojan v5.0**
> The source for a broadly functional system.
>
> **Source Microjoiner 1.7**
> Source code of the widely known file gluer. In purchasing a source, you can modify the code to your own needs. For example, hide it from anti-viruses.
> download
>
> **Sources for SYN-flood, UDP-flood and ICMP-flood**
> Set of source codes (C++) for SYN, UDP and ICMP flood with IP substitution. They will be very handy when developing modules and programs using these functions.

download

Socks5
Source of Socks5 in C++
Since it is well known that they are being sold, the link to the Satanic Socks Server

Smerch v0.4
updated ddos script for testing web server reliability. Module support has been activated in this version. One can use the control panel to conduct operations with shells, list management, selective shell usage and validation. It allows one to run any php code (DDoS, spam etc) on remote shells.
download

PHP-Ddos script (Private)
an excellent modernized script for testing web server reliability. Supports many commands. Connects through the IRC channel (Multithreading and nic [nickname] substitution to any one you choose has been added to the script)

Individuals who posted to this thread strongly supported its development, as an individual could otherwise find these tools through various search engines. For example, boz wrote: “You can google all this just fine, but good that you posted it in one place,” and zood said “Yes. Google rules. If anyone has anything else, that’s already public, but they steal it, then post it. Death to speculators.” Additionally, an individual named c3ntigrad3 wrote “This soft has been going around on people’s hands for a long time, so better people download it for free that [than] buy it from speculators.” As a result, a number of individuals posted a variety of bot and trojan programs within this thread. This was demonstrated in the following posts:

Park: Sprut ddos
download
only the antivirus objects to it strongly...

Mail.ru Agent Spamer spamer
download
only in one of the posts I'm speculating with it myself..so I get a + in my repu[tation] ...I turned myself in 😁

5878480: IcePack [web-based exploit kit]

link

> \+
> mirror
> [external link]
>
> Shred: DKCS DDoS bot
> as the author himself has said, it coasted 1,400 dollars (wmz). I'm public since the 13th
>
> Ivas: I'm putting up **Agent DQ:**
> Description: A very convenient formgrabber with a working tan [transaction authentication number?].There is a script in the set that goes along with it
> Download
> Mirror
> Another mirror
>
> As I promised to a few speculators, I'm putting up NuclearGrabber5 [a very powerful trojan program designed for phishing], with cagen on my site.
> The project was closed long ago, and there are more and more speculators
> Download Nuclear Grabber

A similar post was noted in forum 04, where an individual posted the following message:

> Hello to normal people. I want to say to those who do not know, that there are hackers that are sitting on this site. Cheaters, around 85% of such people approximately. So that you do not fall prey to such people, follow the directions:
>
> 1. Look at normal sites about the programs that you are interested in (most of the programs that are located in public sites and widely used).
> 2. All trojans and popular programs can be downloaded from the source of the cheaters: [external link provided]. Here you will find everything that cheaters offer to you. (Pinch 3.01, zeus_v1.0.3.7, Mail.ru-registrator, INF [Socks] BOT, Skype flooder] or also from here [external link provided]
>
> All the trojans are workable but can be burned by anti-viruses. There are also normal people which allowed themselves to buy private cryptors, cooler then from Gloffa. Pinchers, Joiners, Basically get yourself a normal trojan, request so that it gets crypted and attach it to a needed file. And everything upfront. . .
> This post is not an advertisement at all, I am trying to isolate cheaters. Good luck with hacking.

Based on the attitudes espoused in the examples above, the proliferation of tools across the hacker underground made it difficult for some sellers to offer products that were well known and freely available. For example, and individual named downwind attempted to sell a version of the trojan Pinch in the open marketplace. His ad drew derisive comments from some of the forum users, as in this exchange:

> **moonstone:** Downwind Pinch 3.01 has already been posted public, and you are still pushing [like a drug dealer] 2.99
>
> **Downwind:** There as still such stupid shitheads like you, I'm not pushing pinch, I'm not pushing a builder, I'm not pushing builds, I configure a package, a fully operable package.
>
> And the fact that you're stupid and show your knowledge about supposed pinch 3.01-is this is only a pinch configurator built upon the build 2.99 from damrai, and the fact that for instance in the configurator there are pictures does not make it pinch version 3.01.
>
> In the future I'd ask you not to flood the topic by such stupid people as moonstone
>
> **Dew:** nya, everyone earns like they want)))))
> interesting, have you already made a lot of money? you'd have to be a complete horse-head not to be able to configure pinch =))

Similarly, an individual in forum 09 offered a polymorphic crypting tool that could be used for a variety of different encryption methods. In response to this ad, the moderator posted a message stating: “The pinchers are driving me crazy. You’re banned, push your megatulz on another forum, reindeer [jackass]. ☺” Thus, individuals were likely to deride those who sold tools that could otherwise be obtained free of charge.

Despite the presence of free resources, individuals were not necessarily able to utilize these tools and programs. A variety of factors affected the quality and utility of the malware posted in the forums. For example, free tools were hosted for a limited time on file sharing sites due to restrictions by the service providers. This was demonstrated in a post by swissgate when he posted a link to download a large pack of hacker tools, stating: “Move your balls and make a backup, they’ll close the shop soon.” In addition, a similar exchange between several users in forum 09, where swissgate emphasized the limited availability of free tools:

> **Ant:** Pour it over [make it available], please! Broken archive ((((((

swissgate: Ok I poured it (Link to download)

placement: Again the link died

swissgate: because no one downloaded it and the deadline expired

Files hosted on hacker sites and forums were also restricted due the sites being compromised. For example, zoot in forum 03 posted a variety of tools for download, and a user named Slant noted, "WebAttacker. . . is deleted I can't download it ☹" Zoot then posted a comment stating "You'll see it there [at the hosting site] the whole host is down. I'll pour it to my host. upd [update]: I poured it. I fixed the link." This exchange demonstrates that individuals had to act quickly to obtain free tools.

Free tools were also sometimes incomplete, making the program difficult to operate or completely useless. For example, an individual from forum 03 indicated that a trojan program posted for free was not the correct or complete version:

> people, most of the things posted here are fakes. Look at the description of Trojan A-311. If you've seen a real help for this trojan, then it'll be clear. Look at the builder of this troy . . . the author has been changed. Absolute pure fake! The sploits are all encrypted in bundles.

A similar exchange between users in forum 03 also indicated that free versions of tools may not be completely functional:

Trash: ZeuS 1.0.3.7 [a trojan posted for free download in the forum] lol [laugh out loud] just look at the help for it, its version 1.0.2.0. . .

Imploseioun: that zeus is non-functioning and glued. . .

Wherez the r[e]quest from, toss a normal iframer for scripts, or else the ftp_tools don't import the lists, bestrides which there's someone else's frame, a d1ez [a malware writer] frames bathy, I had a heap of pages that were simply ruined. . .

> **slant**: d1ez iframes perfectly. The one posted here [for free download]. . . may not be so good.

The user suething reinforced these issues, stating "the adpack [a piece of malicious software] that's [p]osted here is an ancient buggy version. . . you won't find anything good that's public, better to buy it from the author."

These comments demonstrate that free tools can be difficult to use due to problems with the code or content. Programs that were complete when posted could also pose a challenge for those who did not understand how to operate the software effectively. For example, an individual named Sari downloaded Agent DQ, and posted a message asking for help:

> Help me configure Agent DQ
> I poured [ftp transferred] it to hosting created a database wrote the username and database in the file r.php and l[a]unched the configurator, I wrote the path to the file as http://www.domen.com/www/r.php but when I press Test I get the warning: no strings received from script and the tables are not created in the database.

A similar post was found where an individual asked for help using a free version of Nuclear Grabber, stating:

> Unfortunately the builder is glued with the trojan Spy.Goldun.JY The trojan is contained in the file config.dat and when the builder is launched it installs in the system. According to the description this is the same formgrabber only it doesn't steal all passwords but only from egold. But if you make config.dat an empty file, then builder won't launch at all. . . Knowledgeable people, help pleaz unglue the horse from the builder?

Thus, individuals who were able to access the tools available in these sites may not have the skills needed to successfully use these programs.

A final and significant problem with free malware and hack tools is that they may be infected by malicious software of some type. Since others wanted access to these resources with no fee, infecting a downloadable program with malware is a sensible attack vector. This was noted by swissgate as he posted a backdoor tool with the following disclaimer:

> Attention! The administration of the site and the hosting service bears no responsibility for the contents of files which are located in the buffer! When downloading files, you should absolutely check them with an anti-virus program! You are using these files at your own risk!

In fact, an individual posted three older pieces of malware, and in response the forum administrators stated:

> **Swissgate:** they didn't teach you in school that it's not nice to plant an infection on people.
>
> **Psixo:** I'm baniciding [banishing or blocking] him, banaciding ☺

Similar comments were noted in forum 03, where free tools were made available for download. Specifically, a trojan was found in a downloadable botnet program, and individuals who attempted to run the program would potentially become infected. This was explained in the following exchange:

> **Blah:** The trojan substitutes WM pocketbooks, registers itself upon launch of C:\WINDOWS\TWUNK32.exe in the registry
>
> **Shell:** I apologize in that case, I'll have to check myself.
>
> **indeve:** Yes, there's a trojan there (file r57 reg.exe). All you need to do is delete it from the archive and that's it. In the future- please check files before posting them. And in general test similar soft needs to be done the same way, with a virtual machine.

These comments demonstrate that the lifecycle of tools in the cybercrime market affects the larger hacker community. Once a resource is widely available, it loses value as a commodity and becomes freely accessible. Accessing these free tools is not necessarily easy as they may be infected or incomplete. Though these programs were not always complete, the ability to obtain them free of charge means that these forums engender the spread of effective and established malware and hacking tools. Additionally, the availability of these tools may account for the number of encryption tools sold in the market. If one can find a free bot or keylogger, then spending three to five dollars on a cryptor is a small investment relative to the larger damage that can be caused through active infections. Finally, the sale of free tools can affect the level of trust and respect sellers receive. All of these factors emphasize the value and unique role that free tools play in cybercrime markets.

INFORMATION SHARING

In addition to the tools and services identified, forums 06, 07, and 08 also provided information on the process of information sharing in the Russian hacker community to facilitate the creation of malware and computer attacks. The content of threads in these forums indicated that individuals can acquire direct assistance to engage in cybercrime. Forum 09 provided direct information on and access to malware that could be used in an attack. In addition, 38 threads in forum 07 and 13 of the threads in forum 08 involved questions related to the development and coding of viruses and trojans, how to recover from an infection, steal information, use cryptors, and pointed questions on hacking. Such information provided a primer on attack methodologies and techniques to avoid detection. For example, a user named Minote in forum 07 asked "what are stealth-algorithyms? I heard they allow viruses to hide themselves. Could you give any more details?" In response the user Ragtop stated:

> In the majority of cases one is talking about the hiding of keys in the registery [registry], files on the hard disk and processes. On the whole the algorithms are based on a capture of the api-functions. .. . and in this way you achieve stealth. You can learn more about the capture from the article on [Forum 10].

The external link provided by Ranger was given as a means of providing information to the interested party. Individuals regularly provided external links to other forums or google, as these sites give a significant amount of information in a more concise and simple way than to explain each answer (see Holt 2007). For example, an individual asked about loading viruses into Windows when it boots, and byte responded stating: "In the August issue of Hacker there is an article by Chris on implementing in auto-load, and more precisely on various methods and keys. . . Find this journal and read it." Such comments suggest hackers helped others learn, but demand individuals acquire substantial information on their own rather than through direct mentoring.

Forum 06 also provided detail on methods of using stolen data and accessing money from fraudulently obtained accounts. In fact 41 of the 50 threads in this site involved direct information provided by users, such as three multi-page detailed threads on how to engage in fraud on eBay as a means to use stolen credit cards or get drops to access funds. Users also asked pointed questions about methods to engage in fraud. For example, the user skoal asked "Can you tell me where I can check how much a credit card has?" Several individuals responded to this question, as in the following examples:

> **House**: In order to find out the balance on a credit card:
>
> 1. You need to find out what bank does it belong to by using the BIN (Bank ID#)
> 2. Enter the needed account through the bank site.
> 3. Look at the balance.
>
> Credit card has to have an online access.
>
> **Plot:** Visa has a phone number, where by calling it you can discover the balance. At least used to be the way, again, you can call the bank and find out the balance.

A similar exchange was observed between two users on how to use drop services:

> **Shellg:** What creds [credentials] and what info is needed for purchasing stuff in the usa in the name of a drop? Thanks in advance.

> **K:** In order to verify drops, you need a simple carton [card] CC [credit card] + CVC [Credit Verification Code], simple stuff is carded up to $500 in order to be sure of the reliability of the drop.
>
> Then for large purchases you need an enroll, here besides the additional information there is online access to the cardholder's account, where you can look at the balance and change the home address to the address sofa [of] the recipient, i.e. info for the drop.

Additional questions were posed by users in this forum concerning how to use stolen credit cards, utilize drops, and cashout cards. For example, runoff asked how to transfer funds across electronic accounts: "what percent is considered to be normal? I give them acct drop for pouring [transferring], they pour and offer me a percentage of the sum. Would 50/50 be normal? What is considered to be the standard?" These questions demonstrate that individuals can gain some insight into the process of utilizing stolen data.

Regardless of the forum, if an individual asked a question, they had to be very specific in order to obtain a useful and direct response from participants. This was exemplified by an exchange in forum 07:

> **Mathet:** So the troj[an] has come, I don't know what the f=) is it cryped or what =) I kinda don't wanna launch something and the antivir doesn't detect it. . . .how can I learn what kind of troj this is without launching it =)
>
> **Golan:** where'd it come from? Did you download it yourself? Or did they toss it to you?

In a related post, deets asked: "executable jpg How can one realize this thingy? So that a certain code executed when this picture is opened, for example, an .exe file?" In response, the user facet posted a message stating:

> The question is rather imprecise, please clarify. . .

> If you are interested in how to launch picture.exe and put this picture on the screen, then the most obvious is a joiner. But if we need to make an executable file with the extension jpg, then as far as I know, there is no way to do this directly. . .

Additionally, an exchange in forum 06 demonstrated the importance of clear and concise questions:

> **Grokk:** How can you configure USA windows [operating system] . . . for carding [data theft and use]? I looked for it but didn't find it. Everywhere you see superficial information on configuration and it doesn't say anything. What progs [programs] might be needed. If someone knows, write?
>
> **koeheless:** It depends on what you mean with the word "Configuration." OS are not configured, one just changes the time on the computer for the country/state/city. Nothing else. If you describe what you need in more detail, you'll accordingly get a more detailed answer.

These examples demonstrate that users will actively question a participant if they do not find there to be sufficient information to answer the question. Otherwise, forum users seeking information must give some thought and structure to their questions in order to obtain a correct answer (see also Holt 2007).

Individuals also had to demonstrate a certain level of competency in order to obtain very detailed information from some users (see also Holt 2007). If an individual appeared to misunderstand the topic they were interested in, forum users would be dismissive or deride the individual. This was demonstrated in the following exchange from the 07 forum:

> **crunch:** I have the following question. Does anyone program in Paskal in our day? If yes then tell me how to create a trojan or virus, toss me some source codes.

> **kakaow:** crunch, not Paskal, Pascal. ☺ First let's determine what you understand under the work trojan or virus? And what you want the proga [program] to do?
>
> **crunch:** In general I'd like to learn to great viruses in Pascal. And I know what a trojan or virus is: a trojan is a proga that steals passwords or info, and a viruses delete sumpin'.
>
> **kakaow:** So that's better, lets start with viruses, that'll be simpler. In your view, what files does one have to delete in order to knock the OS out of operation? i.e. critical files.
>
> **crunch:** It would seem to me something from the system files from Windows or Windows/sistem32 [sic]. And is possible to program the virus, so that for example it eliminates the whole Windows folder or Program Files?
>
> **kakaow:** I didn't understand, what does <u>it seems</u> mean? You need to figure this out and understand what needs to be deleted. I could tell you, but which one of us is planning to write a virus? ☺ So come on, gain insight

This exchange emphasizes the importance of understanding how the software and tools and individual is working with actually function. Without such an understanding, the individual is bound to fail (see Holt 2007). A similar exchange was found in forum 06 where an individual asked for help identifying a program that could automatically generate a CVV for a credit card. In response, several individuals replied to correct this individual, such as dol3n who wrote "what is this non-sense? Throw those ideas out of your head. Generators were working in the beginning of the 90s, now it is too late." Additionally, drastic replied, stating "Well, depending what type of a generator. Generator for CVVs or 3-digits, or plastics? Although in the first scenario, and the second one, you will not receive the CVV." These examples demonstrate individuals who ask questions must demonstrate some knowledge or they may be chastised.

In some cases, individuals provided direct assistance in creating malware or reviewing code to aid an individual's request. For example, sparxx in forum 08 stated that he needed a program to filter proxy server lists to determine active proxies and the port on which they ran. The user poiz then posted a message stating:

> a script with a few lines will solve this problem, for example if the format of the entry is such:
>
> alive_proxy:_192.168.99.1:3128,_protocol_socks5
>
> where the symbol "_" - signifies a space.
>
> Code:

```
#!/usr/bin/perl

while(<>) {
chomp;
my $iport=(stat(split(/\s+/,$_)))[2];
chop($iport);
print "$iport\n";
}
```

> The use of ,
> perl script.pl file.txt
>
> where file.txt - is the file with proxies;

Sparxx was not certain, however, what this code meant or how it worked. As a result, poiz wrote a message stating: "this is more difficult...if you don't know what to do with it....I could roll it into an .exe for you...I'll toss the link here later." Subsequently he provided a complete executable that would run this script for him.

A similar process was identified in forum 07 in a thread where the user iedo1 asked about developing a trojan in Delphi programming language that would create an FTP server on the victim machine. He was unable to get his trojan to activate due to Windows firewall protections and asked how to properly code the malware to get around this software. In response, the user ragged stated "the built-in firewall is elementary" and provided a detailed piece of code that could be appended to the trojan to go through the firewall. These examples suggest that skilled users can gain direct support from others for the creation of malware, though they must also be willing to learn on their own (see also Holt 2007: Jordan and Taylor 1998; Taylor 1999). Additionally, questions must be carefully constructed so as to receive a satisfactory answer. Thus, the flow of information in these forums is regulated in part by individual behavior and knowledge.

NORMATIVE ORDERS OF THE CYBERCRIME MARKET

Examining the exchanges between actors within the open market found in this sample of forums provided significant insight into the relationships and actions of buyers and sellers. The content reflected a larger series of social forces that shape the market environment and the relationships between actors. There were three normative orders identified that play a key role in structuring social interactions between buyers and sellers: price, customer service, and trust. These three normative orders were not, however, evenly distributed across the sample. Four of the seven forums where goods were sold had a greater level of interplay between participants, suggesting they may be more active and function differently than the other forums. As a consequence, certain norms may be more significant or affect individual behavior more heavily in one forum than another.

Price

The cost of goods and services played an important role in the relationships and exchanges between buyers and sellers. As noted above, the prevalence of free tools in the hacker community led forum users to root out and undermine individuals who attempted to sell malware that could be acquired without a fee. Individuals who offered a service were subject to scrutiny by buyers when a price for a product was perceived to be priced too high or low. This was evident in an exchange in forum 10, where an individual named demcho requested a custom written proxy-socks bot and would pay the coder $1,000 for the program. Several individuals responded to this request, indicating differences in the perceived cost of the bot:

> **alep:** [quoting demcho] "you have probably written similar things for yourself"
> true. for_myself_, 2k - is a laughable price.
>
> **museo:** 2k - that just for the bot
> +2k*5 for bypass of fires and full invisibility
>
> **Conter:** [Quoting museo] "2k - that just for the bot
> +2k*5 for bypass of fires and full invisibility"
> =(darn. Aye some kind of sucker. i'm writing three similar projects now, none of them exceed a thousand... =/

Similar discussions were found across the forums, as in the case of a seller in forum 05 who sold a trojan for $10, designed to steal ICQ numbers and passwords and send this information on to a specific email account. The advertisement led to significant debate over the potential value of this project, and if it would work as advertised. The administrator of the forum, velentin, made a post to clarify this issue, stating:

> This trojan is fairly well-known, which extract passwords starting from electronic mail, up to passwords that are saved in system utilities. Obviously from ICQ as well. And if you are interested in full information, then use search. What I want to say, is that yours is not functional, for that kind of money. For $10 you can get a sploit for 2 days for $5 (I can rent it out), buy traffick [SIC] for 2K and load the same pinch. There will be nearly 500 accounts.

His comment emphasizes that for a similar cost, better resources are available. Similar comments were found in other forums. For example, an individual in forum 02 offered "hundreds of thousands of nine-digit [ICQ] numbers available for flooding and spam: 10,000 numbers for 25$" The forum moderator satnn quickly posted to this thread, stating:

"Constructive criticism: 1 thousand 9 digiters costs 1$ you can buy 10 thousand for 8-9$" Finally, an individual named goat offered a crypting service and a forum user downwind questioned the price he charged, leading to a revealing exchange concerning prices and product quality:

> **downwind:** The price is high, others do the crypt for $1-$2. Those who do a supper dupper job get $5. More then 10 is a cheat.
>
> **zood:** The difference between the crypt by hand the cryptor is obvious. The price is approved.
>
> **Jail:** I agree with downwind, price is too much for crypting. It doesn't matter to me if it is done with hands or legs, major thing is do it does not burn.
>
> **Placent:** The price is totally approved. Goat has crypted for me, everything is perfect.

These examples demonstrate that there are expected price ranges for products and services. Experienced participants understand this, and actively questioned those whose prices varied from the norm.

Savvy sellers recognized that pricing can affect their market share, and offered discounts and deals to buyers. Bulk discounts were a common way to sell products in large quantities. For example, enfold sold log traffic, stating: "The more you order, the smaller the price." Such comments were found across traffic seller advertisements. Individuals selling ICQ numbers also offered large lots of numbers at reduced prices to increase their sales. This was exemplified in a post from the seller dratt from forum 03, noting:

> WHOLESALE PURCHASES!
>
> 50 xyzab [numbers with at least five different digits] (those for 0.9 [cents]) – 35 wmz
>
> 100 xyzab (Those for 0.9) – 60 wmz

271 available

50 xyza [numbers with at least four different digits] (those for 1.1 [$1.10] – 40 wmz

100 xyza (those for 1.1) – 70 wmz

191 available

Others offered percentage discounts based on high dollar or large volume purchases. For instance, an ICQ seller offered a discount stating: "When ordering services for more than 300 rub[les] - discount 5 %." Similarly, mastodon from forum 03 offered reductions on the cost of his spam service: "Price is $100 for million sent mails. Every third million is free. To regular clients discounts are 20%. Spam for your base is 50% off." Individuals offering DDoS services also offered discounts, as in this post from cantar: "When ordering the DDoS service for 3-6 days, discount is 10%, with a DDoS service of more than 7 days, discount is 20%, and with a DDoS service for 3 sites, gives a free service for the 4th site."

The pricing and discount structures indicated in these posts suggest that the price of goods and services are variable, with those individuals making large purchases receiving the greatest benefit. In turn, an individual's return on investment in a cybercrime service may increase with volume purchasing. This may help to account for the volume of spam and malware infections seen in the wild. Thus, the cost of a good plays an important role in the relationships between buyers and sellers within these forums.

Customer Service

The second and interrelated normative order identified within these forums was customer service. Individuals interested in buying a product or service sought the most satisfactory experience and noted how sellers cater to their customers. This begins with the speed of contact between buyers and sellers. Some individuals would note "knock me in ICQ, I am there often," or "I am always online," suggesting they could be reached at any time. Those who did not quickly respond to messages from prospective buyers or were difficult to reach received negative comments from forum users. For example, pientza wanted to obtain services from a SOCKS proxy provider, stating: "I knocked [contacted on ICQ] you are not answering. I would like to try it. How many socks will be in the browsers?" Additionally, a malware seller named slicked in forum 03 was not responding to messages, leading to a conversation about his service:

> **Planetoid:** Does anyone know where slicked disappeared to, I haven't seen him a week on ICQ.
>
> **venom:** Maybe he had enough with his trojan
>
> **Zood:** No, he is a secret person. Noone even knows where he is from, sometimes he disappears and reappears again.

In addition to the speed of conversation, sellers who immediately provide goods to their customers received praise from their efforts. For example, an individual with the handle grendel purchased a build of the trojan Pinch from Downwind. He was happy with the product and noted the speed with which it was delivered, stating: "Thanks, I ordered it. Four minutes and it was ready. Respect." Another of his customers named virtuel posted a similar comment, stating: "You can work great with this guy. He does everything perfect and clear, and in a good amount of time. . . Respect to the guy." Thus, sellers who can offer quick distribution of product receive a good deal of respect within these sites.

The quality of the product or service a seller offered was also critical for their prospective buyers. Given the importance of price, customers considered what benefits they would receive for their investment. This was exemplified in a post from the malware installer cyptor, who noted "our price may look to you not so adequate, but the quality will cancel this out, do not forget, that the cheap one pays twice." If a tool was ineffective or data was insufficient, a buyer may post bad reviews or not recommend that provider. For instance, an individual named tripod purchased Pinch logs from a seller and was asked: "Was there anything legitimate?" He responded noting "Not really, it was modest. But I have not seen better stuff from anybody."

The importance of quality was particularly evident in posts from DDoS vendors. These providers regularly noted that they would give customers a free 10 minute test to measure the efficacy of their attacks against a particular target. This was demonstrated in an advertisement by letrin in forum 05:

> DDOS Service, with quality and reliable. I think that majority know this DDOS, but I will remind it to you again, if you have competition, who interrupt your work and if someone has hurt your feelings, you can play on the site of this person, best solution is smokin.
> Why our Service?
> Affordable prices
> 1 hour-$20
> 1Day-from $100
> All this is discussed individually with everyone. There are possibilities for cheaper prices, depending on the projects.
> We give 10 minutes for a test. Always online, large BOT army, all is fast and organized

Some vendors also offered money back guarantees, as in this example from forum 3: "If the site your order to attack comes alive earlier than the time chosen by you, then you will get money back." Such a measure demonstrated a willingness to negotiate with prospective customers that could increase their overall business and reputation.

Some vendors also offered free gifts as a means to generate new customers or to keep current customers satisfied. For example, an individual named vivendi sold credit cards in forum 03, and one customer noted the level of service provided: "I took one card already for doing spam, domains, porn, the person is super, in the form of a discount he gave me a free card." This comment demonstrates that free gifts can satisfy a customer, and may also draw in additional clients. Similarly, retrograde offered a socks service in forum 03 and gave a free gift to customers due to downtime over the New Year holiday, stating:

> For all clients of our service, during this time of the New Year, we are compensating the two days of inactivity during this holiday period, for those whose accounts expire on the 31st. . . . Besides that, in this time, there will be available a few PIN numbers which will be given out as presents.

Such comments demonstrated that service providers recognize the need to maintain their customer base and will take significant steps to do so.

Another important indicator of customer service was the degree of support individuals offered for their products. Services, tools, and resources that required a higher degree of knowledge or specification often came with some form of customer support. Anti-abuse web hosting providers offered a good deal of support for their customers, as in the case of a provider who described how clients could speak live to his sizeable support staff:

> We have implemented real-time client support for the ICQ protocol. You can submit your question and also receive full consultation from our specialists, if your question relates directly to our service. The ICQ support service works for your convenience round-the-clock in 2 shifts: day and night. Below you fill find information for quick contact.
>
> ICQ #1. . . owner of the service. The solution of very important, as well as organizational questions. Complaints and suggestions regarding the work of the service, receipt of payment for services).
>
> ICQ #2. . . Support. . . decides the same questions, purchase of accounts, general consultation on the service. COORDINATION of the work of support and administrators);

ICQ #3. . . - support, system_administrator, night shift. Solutions on difficult technical issues);

ICQ #4. . . (Support. . . -Night, support, system_administrator, night shift. Solutions on difficult technical issues);

ICQ #5. . . (Support. . . -support, day shift);[/B]

ICQ #6 . . . -support, day shift, Solutions on difficult technical issues)

A loading service provider in forum 03 also described his customer support service:

> What are the principles of work?
> You knock [contact in icq] to the support, present the question of your interest, and take the exe and begin the co-working with us.
> Payment?
> Two times a month (once every two weeks.)
> With big sellers the payment term can be discussed individually.
> Support?
> [ICQ Number]24 hours
> [ICQ Number] -technical questions.
> From support you can find out who we work with and feedback as well.

These posts demonstrate that access to support and regular software updates are a critical service component that may help to develop and maintain a regular base of clients. These posts also demonstrate that principles of customer service found in the legitimate business world appear to shape the interpersonal dynamics of buyers and sellers in this cybercrime market.

Trust

The third order identified in these forums was related to customer service: trust. The participants in these forums sought out commodities that they valued, and had to pay for these goods without actually interacting with others in person. Participants may not receive the goods they paid for or received bogus products with no value. In addition, most data and services sold were either illegally acquired or a violation of law, so the buyers could not pursue civil or criminal claims against a less than reputable seller. As a result, it was critical that participants know who they may be able to trust and the steps they can take to reduce the likelihood of losing money.

The significance of cheating and mistrust led to the development of three key methods to reduce the likelihood of loss. The first was through the use of checks or tests by the forum administration as a means to validate the quality of a product sold in the forum. For instance, one of the moderators of forum 05 described the checking process, stating:

> Administration has the right to ask any seller to present his/her product for check. You present the product in the form that it is being sold, so that it can be checked for a test. No videos, audio, sreens. Forum safety relies on many factors, but the main one is saving the users from possible cheaters.

Four of the forums in this sample utilized checking systems, though the seller was required to initiate the process of checking or testing. For example, an individual in forum 01 offered an iframe tool and at the end of his advertisement stated: "I'd be happy to get checked out, guarantor and all the rest. . . .^_~" Similar comments were found in the other three forums, suggesting that reputable sellers would engage in the testing process. The value of check services was evident in this exchange from forum 05:

> **recticule:** Flood through telephone calls (Of all cities and operators). Good time of the day. I want to present to you a flooding service through telephone calls for mobiles (any operators) and also home phones (of any cities).
>
> Required from you: Victim's number and code, if the numbers are from another country. Knock, service is more accessible then anytime before. If I am off-line, write and tell me how much of the service you need, I will answer. I can pass the check/verification on [Forum 05]
>
> **Hatt3r:** Go to check, ICQ
>
> **Hatt3r:** Verification has been completed, it works.

By going through the checking process, recticule demonstrated to others that his service worked. Similarly, an individual in forum 03 was selling credit card numbers, and had his services checked. A review was then posted by slat434 which read: “Passed the check. At the time of the check, the person possessed quality product. Also, in order to escape and avoid any confrontational situations while buying, selling products on the forum, the guarantee service is working.” As a whole, these posts demonstrate that checking services in the forum provide prospective clients with an assessment of the individual’s level of trust based on their product or service.

In addition to internal checks within a single forum, some sellers advertized that their products had been checked in other forums, and provided web links to verify this information. For example, belial noted three separate websites at the end of his advertisement in forum 03 where his products had been reviewed. An interested party could venture out through those links to confirm that he was, in fact, trustworthy. Similar comments were noted in the other forums, as exemplified in this post from forum 01:

> Structure2021: Quality Spam Service
>
> I’d like to offer for your attention a quality SPAM service.
>
> Distribution of 1 million messages – 75$
>
> Minimum order quantity 100 000 lette[r]s
>
> I’ll gaterh [sic] any databases for you
>
> You can read recommendations and comments here
>
> [external link]
>
> It was tested here:
>
> [external link]

These exchanges indicate that individuals sell products across forums and use these cross-site advertisements as a means to garner more customers and higher levels of trust. In turn, buyers can look across other forums as a means of validation of a seller's reputation.

The second method employed in the forums as a means to instill trust was the use of a guarantor program. If an individual was uncertain about a prospective buyer, they were encouraged to make a payment through a guarantor system. Guarantors ensure that a payment will not be delivered until the product is received, and played an important role in establishing trust. Four of the forums in this sample used guarantor services. Their value was demonstrated in a post from valentin in forum 05:

> Guarantee and passing a check. If you do not trust the seller or simply want to secure yourself from cheaters, then you can use the services of the guarantee forum. Any administrator can take the role of the guarantee. There are only two administrators. . . I am esxplaining [SIC] to those in the tank, that if you want to pass the check or buy/sell/or present services through a guarantee, then the ICQ of the guarantors is above. Guarantee services are free.

The value of guarantors was demonstrated in a thread where an individual named megaphish posted an offer to exchange software, stating:

> Exchange with a private software. I will conduct exchanges with people who have equal software. I am not conducting any selling/buying, it is not good to cheat. Exchange is conducted one for one, meaning we agree with you through ICQ about what we need from each other, and conduct an exchange.
>
> There is a possibility to conduct an exchange through a guarantor of the forum (in the corresponding theme I have found that in this forum there are 2 guarantors and guarantee is free).
>
> If you have a reputations on the forum (on this one or any other one similar to this, in size and theme), then right away I will give you the software first, and then after that you will give me the link to the software. No cheaters allowed.
>
> If you think that just because there is an exchange of private information you can cheat, then you are deeply mistaken, even for such cheating you can be added to the shit list, I can do that, to turn on the video with the monitor parts, not difficult, and this is a better proof then logs.

Forum users doubted the value of the program being offered, and megaphish honesty. For example, vaseq posted: “Why wouldn’t you write what kind of a software you have? So that we would know if there is a sense to knock to you or not.” Similarly, scattershopt suggested: “Heh. Maybe you do not have it. Give it to the admin for the check [ICQ number provided]. If everything is okay, maybe I will exchange, because like that I can also write a lot of things.” These comments led the forum guarantor, sanction, to post the following message:

> If you are scared to be cheated, then there is always a guarantor, and the guarantor is free and megaphish knocked me in ICQ and we conducted a software exchange. Meaning, the following took place:
>
> Approximately an exchange of similar value with a software has also been conducted.
> Just waved a little bit, I gave him one, not a big release (trojan), and he gave me a software that I requested.
> You need to make all conclusions:
> Now, a little bit about the moral side of the question:
> How have you need able spot the cheaters, we are not against deleting the topics posted by cheaters, no one will know, that this person is a cheater, but so everyone will know that this person is a cheater and you know it too (we have created a separate section for the cheaters) and if you are against cheaters, then you do not even have to enter there into that section, and do not have to buy anything from those cheaters.
> I do not even know to what group should this person belong, you can not call him a cheater straight up, he is not selling anything. And making exchanges of private software in the open is not pleasant either, but all make such exchanges with their friends and familiars, simply through ICQ. So conclusion can only be made by you about how to deal with such topic.
> I do not have a large task, I was just asked to conduct a check, so I did it.

These exchanges demonstrate the importance of guarantors and checks as a way of validating and confirming an individuals’ level of trust and reliability within these forums. Without guarantor payment systems, individuals increase their risk of loss and theft.

The third way that individuals can gain or demonstrate trust within the forums was through customer feedback. Individuals who purchased a product or service could provide detailed comments about their experience with a seller for other users so that they may understand how that person operates. Posts that gave favorable reviews or positive comments demonstrated that an individual is trustworthy. For example, the seller track offered so-called "abuzo reliable hosting services" in forum 01. He received a number of positive comments from customers, as demonstrated in the following posts:

> **Drag0n:** I uze the host! I like it!
>
> **Angry:** I took a .info host+domain, registered all the people, ****** which I recommend
>
> **Psych:** I use this hosting+domain in the Info zone. Everything is quick and presise!
>
> **Ask3:** I bought the domain+hosting+good person=I recommend it!

Similar feedback was found in customer reviews for stagg from the 03 forum who sold credit cards:

> **bastard:** everything is good I took a CC. Right away he gave me a valid one, without problems and fast. Thank you.
>
> **escq:** I haven't work with this person for a very long time. So far I am satisfied with everything. He exchanges the invalid ones. I am hoping for the same type of service in the future.
>
> **kindle:** I have bought the CC, everything is good. I suggest it.
>
> **search:** The service is perfect, 95% valid, exchange of an invalid is done within 1-2 minutes. I have taken 4 times, everything is ok.

These favorable reviews clearly demonstrate that a seller or service provider could be trusted to provide quality products on time and without a great deal of difficulty. Such information helps to build a solid and trustworthy reputation for a seller, and may potentially increase their market share and customer base over time.

At the same time, individuals who provided bad services or were untrustworthy received negative feedback. When a customer lost money or did not receive products, they buyer could clearly elaborate when and how they were cheated. For example, an individual named locat in forum 10 sought an experienced programmer for "developing server projects" with "Preferably experience developing polymorphic software." He noted that "This ad is being published a second time since the previous person shamelessly gypped me out of $1,000, he seemed to have started to do something, took the money, and then dropped out of sight." He also made a second post describing the way that he was bilked out of money, stating:

> If anyone is interested - the person who gypped me. . . he agreed to develop, what's interesting to me is that he seemed to be a decent person and understands the subject matter, he seems to have some experience, he seems to have already shown something earlier, but then why later disappear, when I decide to give a person a bonus...

Related posts were found across the forums, as in the case of an individual named diesel who posted an ad for a log purchasing service. An individual named ne0 apparently purchased logs from diesel and was dissatisfied, stating: "I write facts, so that people are more careful. . . Whoever does not trust me, should check. Whoever trusts me will be grateful for saved time and money. . . TS [topic starter diesel] took the money for the order and disappeared." Thus, negative feedback demonstrates how a person treats their clients and provides a metric by which others can assess seller quality and practices.

Individuals who referred to someone as a cheat or provided negative feedback had an important impact on the social dynamics of a forum. The appearance of negative comments often led to significant debate and some degree of infighting among forum participants. If an individual who had regularly posted in the site was argued to have engaged in questionable behavior, others posted to support or refute these claims. This was demonstrated in a thread which started when an individual named smack posted an advertisement for high priced ICQ numbers. Others began to refer to him as a cheater, leading to a debate between users:

grasp: The site [external link] offers the similar numbers. What are you doing admin [forum administrators]

bettle: Cheater.

steel: You [smack] are an idiot.

Snapdecision: No, he is just a cheater.

Spetznas: Dude, when was the last time you went to see a psycho [a]nalyst? By the way, this is punishable. I have the favor for you to read the regulations codes and the history of ICQ creations. And will agree with the rest that you are an idiot.

kalish: Yeah. The prices are of course cosmic. Do you have anything cheaper? You must be (saying in a nice manner) no too bright of a person to stick such prices for a number, even if it is a 5-digit number.

streep: Guys, you are just in the wrong topic. Slap is a famous person in the ICQ world, and his store in my opinion is the best and most reliable, and if you can not afford such an elite number, then buy a simpler one and cheaper, or come to me, I am giving away the 7-digit numbers.

Rosign: The topic started has good prices for such numbers. Plus, he has numerous feedback, so there is no point to call him a cheater, you are making yourselves look like idiots.

R3dst@5 [a senior member]: What is going on, its like a zoo here, are you all morons. He has the most elite numbers, and you are raising hell. If you are too weak to buy a new elite number then don't write in the topic.

This exchange demonstrates that calling someone a cheater based simply on product pricing does not benefit the forum users. A similar exchange was found in forum 03 where an individual named nitrex sold a number of Web Money trojans and received some negative feedback from several individuals:

> **cytox:** Hm, I have seen code of such a trojan in an open access. I honestly do not know how with the updates, but the name is the same. I sory [sort] of do not believe into the workability. The greatest concern that rises are:
>
> -Strengthening of the autoloading-that is some bull, if the program destroys antivirus and firewalls and kills the windows and all to hell, then the autoload would be quick as is…
>
> -Blockage of the windows- no comment to that one. . .
>
> (Why has the price dropped in couple of weeks from 500WMZ to 50WMZ?) If it is truth that you can get such money with such a program, then it is priceless, if it is 50WMZ or even 500WMZ. I am not against the creator of the topic, and do not suspect anyone of anything, such had some questions arise. I think such questions can naturally arise from anyone who is a potential buyer.
>
> **Myopic:** Respect to the person, I sued [used] the trojan, but unfortunately haven't compensated mine. Complaints fly… but honestly, there are some defects, especially I do not like the fact of a constant shut down of the victim's computer. Should have just disconnected inet [internet] and that's all. But the product is good.
>
> **sectorstrap:** Here is what I can say about the given person. I wanted to buy the WM trojan from him.
>
> 1. The description of the functions did not match the real operationality. Software was not working and everything that he did, only 1 of 10 promised things worked.

2. This guy was luring clients. After the deal was conducted, he would turn the admin onto his host and would say that after he receives the money, he would build the software onto my host.
3. He sold me the joiner for 10wmz, which was in the public. $10 is not money, but it amazes me how this guy treats clients of his software.
4. After working through a guarantee I lost almost $150 (guarantor services, insertion, and extraction) so think 3 times before you buy anything from him. I haven't heard anything positive about this guy on the net.

Nitrex: Sectorstrap, go to hell. You shit for me on every forum. If you do not know, then be quiet. You think I am gonna give you a trojan on your host without money? I gave you a test on my host, its not my problem you did not want to buy it. You are lying. Whoever wants to buy it, will buy it. However does not want to buy, then bypass.

Since negative feedback and name calling foments debate, mistrust, and disorder among participants, forum moderators attempted to limit these discussions. This was exemplified by the forum moderator n30n who posted a message concerning how he would deal with individuals making negative comments:

For groundless complaints, swearing, flood and multi-accounting - BAN. I've had enough. Groundless complaints include:

- "He has one munth [SIC], that pers[on] registered himself and praised himself," - remember finally, that those who need one or another service don't even have to register on the forum, and accordingly it also isn't necessary flood here with up to hundreds of posts, that that they should later check him;

- "He's a fraud artist! I regged [registered] a box, and he didn't break in to it," - if you

> specially don't read this box, and in answer to the secrete question "What's your dog's name" the Chinese alphabet is written, then this is not surprising;
>
> - "I transferred money, and that pers doesn't appear any more," - this is your own fault. This means that you are a SUCKER. Never give pre-payment, transfer money with a protection code, but don't give it, just show that you have this money. Send test letters to broken-in mailboxes, accs etc. require screens. If you decide to use someone's services, then take an interest as to what other forums this person offers them on and where you can see references regarding his work.
>
> FLOOD IS PROHIBITED!
>
> Ask the seller via pm or icq regarding all details on providing one service or another and the quality of goods. Only messages which specifically related to work are allowed: "I bought it, everything's ok," "He's a fraud artist, evidence of some type or another, links to other forums, where this fraudster was noted." Everything else is considered to be flood.

These comments clearly demonstrate the disruptive impact that claims of cheating can produce in these forums, and the significance of trust in structuring the relationships between actors. Furthermore, this post illustrates the relationship between trust, price, and customer service and their affect on the social dynamics of the forums in this sample.

IV. Conclusions

A. Discussion of Findings

This study attempted to examine the creation, distribution, and function of malicious software using both a sample of bots examined through a honeynet, and a qualitative examination of 909 threads from 10 forums operating out of Russia and Eastern Europe that facilitate the sale and distribution of malicious software and cybercrime resources. The analysis of bots presented supports the finding that botnet command and control channels may have particularly short lifespans, as only five of the channels sent requests to the infected image (see Cooke and McPherson 2005; Karasaridis et al. 2007; Rajab et al. 2006). Of the nine bots that connected to a command and control channel, several required a password to access the channel (see Karasaridis et al. 2007; Rajab et al. 2006).

The ways that the bots in this sample were used support the notion that bots have significant utility for cybercrimes (see Dagon et al. 2006; Rajab et al. 2006), whether to infect other systems or surreptitiously collect information on systems in the same network as the zombie node. The majority of bots in this sample attempted to connect to IRC channels in the United States, though other countries were included, emphasizing the global distribution of botnet command and control structures (see Collins et al. 2007; Cooke et al. 2005; Dagon et al. 2006). Thus, these findings suggest that there is a need for careful monitoring of U.S. websites and servers for malicious traffic. Federal law enforcement may have greater success in shutting down or gathering information from servers in the U.S., rather than in foreign countries due to difficulties in extradition (see Brenner 2008). As a result, such measures may be one way to impact and reduce botnet traffic in the wild.

The findings of the qualitative portion of this study suggest that myriad tools and services are available and sold for profit in an open market environment that encourages and supports a variety of cybercrime. In fact, the resources and structure of the forums identified in this study are similar to research on markets operating in IRC (see also Franklin et al. 2007; Honeynet Research Alliance 2003; Thomas and Martin 2006). A key difference lies in the volume of malware and services available in these web forums relative to IRC channels. Individuals could procure spam, DDoS attack services, iframe exploit infections, web hosting, and proxy services for low costs from the forums in this sample (see also Franklin et al. 2007; Honeynet Research Alliance 2003; Thomas and Martin 2006). Several of these services were also dependent on botnets for functionality, demonstrating the importance of bots in facilitating cybercrime. Credit cards, bank account information, and sensitive personal information were sold in mass quantities at variable prices, though in much smaller lots by comparison to the IRC markets observed in other studies (see also Franklin et al. 2007; Honeynet Research Alliance 2003; Thomas and Martin 2006). Finally, free tools were readily available though not necessarily fully functional when downloaded.

As a whole, the products sold and normative orders of this market suggest that buyers need little technical knowledge in order to access or utilize these resources. These forums simplify and engender identity theft and computer-based financial crimes (see also Franklin et al. 2007; Honeynet Research Alliance 2003; Thomas and Martin 2006). In fact, the findings support the notion that "parts of the Net will soon develop into a new 'improved' underworld" where criminals can obtain all manner of resources and engage in crimes (Mann and Sutton 1998: 225). At the same time, these forums were largely unregulated, and participants engaged in transactions at their own risk (see also Franklin et al. 2007; Thomas and Martin 2006). The normative orders that structure relationships between buyers and sellers in these forums also emphasized the lack of formal controls over actor behavior. Price, customer service, and trust affect the likelihood that an individual may purchase goods from a seller, but do not eliminate the risk or likelihood of loss.

As a consequence, the cybercrime markets identified in this study share some similarities with real world stolen goods markets. Specifically, sellers received a small portion of the true value of the services and information that they offered, as with goods stolen in the real world (see Schneider 2005; Stevenson et al. 2001). For example, a credit card or electronic account may contain thousands of dollars, though the average price for these items on the open market were very low, comprising a small percentage of its overall worth. Similarly, an individual can spend a few dollars on a crypting program that will enable the spread of a piece of malicious software on thousands of machines. Thus, the value of resources in these forums appears to be derived more from the information connected to the account or the utility of a service, rather than its monetary value. As a consequence, malware, databases, and information appear to be commodities in the Russian hacker community that are impacted by market forces and competition. This enables individuals to engage in cybercrimes that have a significant economic impact at an extremely low cost.

Exploring these markets also illustrates the significant and changing threat that cybercrime victimization poses for individuals around the world. The advertisements provided by DDoS sellers and iframe traders suggest that victim computers exist globally and may unwittingly be used in the facilitation of spam and other crimes (see also Franklin et al. 2007; Honeynet Research Alliance 2003; Thomas and Martin 2006). The presence of stolen identity information indicates that financial fraud is a small, but related problem in the malware market as well. These results indicate that offenders can victimize large populations regardless of geographic boundaries and those affected may have no knowledge that their computers or information have been compromised. As a result, there is a need to develop strategies to reduce both the proliferation of botnets and the markets that facilitate cybercrime.

B. Implications for Policy and Practice

One of the most important policy implications of this study is the significant threat that botnets play in cybercrime. The bot analyses demonstrated that command and control servers were spread around the globe and the infections may not be easily identified by end users due to the variety of system changes caused by the bot. This study found that the bots were primarily used for scanning and attacking purposes. Additionally, the forum analyses indicated that bot masters realize the value of their infrastructure and offered services enabled by their botnets to engage in cybercrime for profit. Bots are, however, part of a wider spectrum of malware as noted in the threads from the forums examined in this study. As a result, any attempt to effectively reduce or impact the creation and use of botnets specifically, and cybercrime generally, will require a combination of both technological solutions and traditional policing practices.

The relationships between the cybercrime market and other real world criminal markets suggests that principals of situational crime prevention (Clarke 1983, 1995, 1997; Clarke and Eck 2007; Newman and Clarke 2003) and intelligence-led policing (McGarrell, Freilich, and Chermak 2007) may be useful in affecting cybercrime. For example, actively collecting and running malware in an emulated computing environment like a honeynet can enable law enforcement agencies to understand the nature, functionality, and structure of a botnet active in the wild. The information generated from this sort of analysis has tactical value, as individuals can obtain the location of a command and control server. If the server is hosted in the U.S., federal law enforcement agencies can notify the owner and request the server be shut down, or monitor the channel to gather further information. This sort of information gathering could prove invaluable to develop cases against bot masters, and potentially successful prosecutions given the number of channels hosted in the U.S. If a botnet is controlled from a foreign nation, this may decrease the likelihood of developing a successful prosecution (see Brenner 2008). At the same time, documenting the global scope of the botnet threat may stimulate relationships and discussion with other nations on the problem of cybercrime, and the need for increased law enforcement collaboration.

The forums identified in this study also provide a platform for botherders to lease their botnets for various services. Therefore, it is critical that these sites play a key role in law enforcement investigations. The participants and exchanges observed suggest that cybercrime markets are structured much like real world drug (Harocopos and Hough 2005; Jacobs 1999, 2000; Jacobs et al. 2000) and stolen goods markets (Cromwell et al. 1991, 1993; Schneider 2005; Stevenson et al. 2001; Wright and Decker 1994). In turn, the same policing strategies may be employed to investigate, disrupt, and reduce their presence on-line (see also Newman and Clarke 2003; Taylor et al. 2006). For example, it is clear that law enforcement agencies have developed undercover investigations to penetrate and purchase goods in web forums to develop criminal cases against these actors (Brenner 2008). The market forces and structures identified in this study can be used as a roadmap for federal law enforcement to infiltrate the market with reduced likelihood of detection. Undercover agents can create fictitious identities and use these covers to register in multiple forums. The findings from this study can be used by agents to more rapidly conform to the behaviors and processes of the market to identify key buyers and sellers. This will facilitate the collection of actionable intelligence, and the development of behavioral profiles for key buyers and sellers (see also McGarrell et al. 2007).

The data generated from these investigations can also be used to conduct stings to affect both buyers and sellers in these markets. Specifically, undercover agents can purchase a good or service from a seller and use this as a means to build a case against the individual and any of their known associates. Arrests of single individuals in street crimes, however, appear to have little impact on the operations of open air markets due to the freelance nature of sales and the range of available locations to sell products (see Harocopos and Hough 2005; Jacobs 1996). If these principals apply to the cybercrime market, then arresting agencies may be better served using potential charges as a means to encourage cooperation from the offender in order to create a larger case against multiple sellers in a single forum, or across multiple sites. This would make a greater impact on the supply side of the cybercrime market than may otherwise be observed with single arrests.

Targeting specific providers within cybercrime markets can also be used as a means to stem the use and spread of active botnets. For example, undercover investigations of DDoS service providers can be used to map the location of zombie nodes and the scope of a botnet. This study found DDoS service providers offered to attack services at low prices in forums across this sample. Federal law enforcement agencies could establish simple websites hosted on a public or protected network and hire a DDoS service provider to attack the site, and then analyze the attack traffic using log files obtained from the server. This data would provide information on the location of zombie nodes, and allow affected computer owners and Internet Service Providers to be notified of the infection and given tools to remediate the problem. Additionally, the DDoS service provider can be charged with violations of the Computer Fraud and Abuse Act and other related legal statutes depending on their country of origin (Brenner 2008). Such a measure would help to destabilize botnet infrastructures, thereby weakening their use in various forms of cybercrime. Repeated investigations may also deter individuals from offering these services due to the perceived risk of detection or arrest.

The use of "reverse stings" against buyers may also be effective to impact the demand side of the cybercrime market (see Newman and Clarke 2003). Undercover agents working in conjunction with financial institutions could sell falsified credit card numbers to interested parties in a forum. These numbers could be flagged by the financial institution as stolen, and monitored for any attempts to check or use the accounts. Alternatively, officers could attempt to sell a polymorphic engine or cryptor and identify and develop a case against an individual for attempting to engage in violations of various legal statutes. Any malware would have to be carefully configured to not operate properly so as to keep the buyers from using the program to engage in attacks. Such an action may, however, lead to bad reviews and force an undercover identity out of the market. This may stimulate arguments and help create infighting and mistrust in the market (see Franklin et al. 2007). Furthermore, the cases that could be developed may help to remove multiple buyers from the market and spread fear over purchasing goods in the open market. It must be noted that any reverse sting must be developed in conjunction with legal counsel to ensure that the potential for entrapment is low and effectively managed (Newman and Clarke 2003).

The strategies outlined above may prove useful in affecting key players within malware markets, but may displace participants into more carefully concealed and protected websites and on-line locations (see Franklin et al. 2007). This may unintentionally make the investigation of cybercrime more difficult and limit the likelihood of detection and successful prosecutions. Thus, there may be some practicality in attempting to disrupt these markets through surreptitious use of the social processes that undergird the forums (Franklin et al. 2007). In particular, trust between participants is critical to establish an individual's reputation, and maintain customers. When an individual is accused of cheating, the exchanges can become heated and lead to disruption and reduced social cohesion. Undercover agents operating under false identities in the forums could make comments about the quality of a product or a seller's actions. Posting bad reviews could affect a seller's reputation and, if repeated often, may lead to mistrust among participants and network disruption. This sort of "slander attack" strategy poses less direct risk of detection and legal challenges for law enforcement, though it may lead to a user account being closed and banned (see Franklin et al. 2007). Thus, considering the use of informal social processes may prove useful in affecting the organization and relationships that undergird the cybercrime market without the need for legal interventions.

All of these investigative techniques outlined above require a significant financial investment in federal law enforcement resources. It is imperative that increased financial resources be allocated to the Federal Bureau of Investigation, Secret Service, and other federal agencies to more effectively combat the problem of cybercrime. For example, the language barriers identified in the cybercrime markets indicate the need for language training and translation services to properly investigate websites and forum content. Additionally, funds are needed to engage in undercover purchases of malicious software and hacking services to build cases against cybercriminals. The computer and communications technologies necessary to properly investigate cybercrimes also require significant financial investment. Thus, greater resources must be allocated at the federal level to improve their capacity to investigate cybercrimes.

There is also a need for increased international collaboration in law enforcement agencies to improve the response to cybercrime. The use of the Russian language in all of these forums, coupled with the presence of job postings for positions in Russia and Eastern Europe, suggests that the participants in these forums are either living in Russia or are Russian speakers living abroad. In addition, several web hosting providers noted that their servers resided in Malaysia or other parts of Asia. The Command and Control servers identified in the bots analyzed in this study also appeared to reside in Hungary, France, Malaysia, and China. Therefore, it is necessary that the Department of Justice and other federal law enforcement agencies around the globe carefully consider and develop improved extradition treaties and cooperative frameworks to ensure improved relationships with agencies such as the Russian FSB (see Brenner 2008; Wall 2007).

Another important policy implication is the need for more stringent legal frameworks to prosecute the creators of malicious software and individuals who sell access to these tools. There are several laws in the United States pertaining to computer intrusions, identity theft, spam distribution, and intellectual property theft. The existing statutes do not, however, provide punitive sanctions for the sale of malicious software, or of identity information (see Brenner 2008; Wall 2007). Creating statutes that clearly elaborate these crimes can improve the ability of law enforcement and prosecutors to build cases targeting these actors. In turn, this may help to increase the risks of cybercrime for actors and improve the power of federal prosecutors to pursue cybercrime investigations.

Finally, the victims of malicious software infections and attacks play an important role in the prevention of cybercrime. Zombie machines, compromised servers, and web pages facilitate a variety of cybercrimes. System administrators, Internet Service Providers (ISPs), and home computer users must take care to act as place mangers to prevent or mitigate infections and protect their machines (see also Brenner 2008; Newman and Clarke 2003). This is challenging given the prominence of encryption tools and binders that allow malware to obviate antivirus programs and other protective software in place in large hosting companies. The volume of traffic that ISPs and corporate security professionals must deal with also complicates the identification of questionable or malicious traffic (see Brenner 2008; Newman and Clarke 2003). Thus, there is also a need to develop better sensor technology and resources to facilitate the identification of malware on servers and malicious traffic from nodes under the control of a service provider or corporation. In addition, increased relationships between service providers and law enforcement may facilitate higher levels of reporting infections and cooperation during investigations.

There is also a need for improved awareness among home computer users who do not necessarily have a strong grasp of basic computer security principals (see Brenner 2008; Wall 2007). A home computer may be more likely to be infected as end users do not adequately protect their systems from compromise (see PandaLabs 2007). One way to affect this problem may be through public awareness campaigns targeted to ensure that home users understand the potential vectors for malware infection and the importance of owning, updating, and regularly using protective software. These measures may help to destabilize botnets and the platforms that engender spam and identity theft by increasing an offender's risk of detection and reducing the likelihood of successful infections.

It is important to note the limitations of this study. The bots analyzed in this research were not necessarily as functional as other bots examined by researchers (see Bacher et al. 2005; Dagon et al. 2007; Rajab et al. 2006). This may be a function of the random sample of bots that were captured, or a result of short lived command and control structures. Other bots were examined, though the findings were not presented here as the data were lost due to a cataclysmic system error. Regardless, the weak findings presented here are a sharp contrast to some other research on botnets (see Bacher et al. 2005; Karasaridis et al. 2007; Rajab et al. 2006). As a consequence, this suggests that while some bots are extremely large and high functioning, others are less successful in the wild. Further research is needed to identify any changes in the behavior of bot programs in different environments outside of honeynet testbeds.

Additionally, the bot analyses presented here are constrained to one period of time during 2007. Given the rapid adoption and innovation of malware and tools across the hacker community (see Brenner 2008; Holt and Kilger 2008), these findings may not be generalizable to bots currently circulating on-line. Further research is needed to consider the function of bots in the wild at multiple points in time. Such longitudinal research can improve our understanding of malware, and identify solutions to mitigate this problem.

There are also several limitations within the qualitative analyses that must be discussed. First, publicly accessible forums were used, enabling any individual to access the forum content. The content of these forums may be different from the exchanges that take place in private forums that require registration in order to access the content. The resources sold in this sample of forums may also be different from the tools used by hackers in other countries, such as Germany, China, and Brazil. Thus, the findings of this study may not be generalizable to closed forums and communities across the world.

Additionally, this analysis utilized a small sample of the threads from each forum. The difficulties in translating large amounts of data from Russian to English limited the number of threads that could be analyzed. There may be further malicious content that was not identified or additional normative orders that were not uncovered between participants in this sample of threads. Further data translation and analysis is necessary in order to expand this sample beyond the subset of threads used in this analysis.

C. Implications for Further Research

Taken as a whole, there is a need for greater exploration of botnets and the forums that facilitate the sale and distribution of malicious software. Specifically, researchers must continue to capture and examine bots and other forms of malware to understand how the utility of these programs change over time and uncover trends in the location and function of malware. This research can facilitate the creation of improved signatures to detect malware through antivirus programs, as well as the development of other technological means to defeat botnets in the wild.

Future research is also needed using a sample of threads from closed forums that require registration in order to consider the malware and products that are available. The findings can provide important insights into the variation of products and prices sold across open and closed forums in the active hacker community. Such analyses may also shed light on any differences in the relationships between buyers and sellers in more trusted environments. Future studies should also sample hacker forums in other nations and languages to document any regional variation in the tools and techniques common across hacker communities. Longitudinal studies of the market could also expand our understanding of the speed that exploits are identified and weaponized by hackers. Economic analyses of the costs and return on investment of malware and cybercrime services could also expand our knowledge of the true cost of cybercrime for both victims and offenders.

Given the implications of this study for law enforcement policy and procedure, future research is needed to evaluate the success of intervention strategies used to affect cybercrime. There are myriad studies considering the impact of traditional and experimental policing strategies on a variety of street crimes, including prostitution (Scott and Dedel 2006), drug markets (Harocopos and Hughes 2005), and other forms of offending (Clarke 1997; Clarke and Eck 2007). Few studies have considered or evaluated best practices, displacement affects, and the overall impact of law enforcement cybercrime investigation techniques. Evaluations of cybercrime interventions are needed to provide guidance on the strategic and tactical value of policing methods to affect rates of cybercrime.

Criminological collaborations with other disciplines can also greatly improve our understanding of both the methods of cybercriminals and means of preventing these offenses. For example, linguistic analyses of forum content could be used to generate demographic information about the participants, and expand our knowledge of the background of the market actors. Computer science and information security perspectives should also be incorporated into criminological analyses in order to better identify the attack methods that facilitate malware infections and the spread of botnets. Such collaborative research can lead to the creation of technological and social solutions to reduce the likelihood of infection, and destabilize the market for malware and stolen information. In addition, criminological and information security collaborations may lead to software that can be used to surreptitiously monitor stolen data markets and increase our awareness of their prevalence on-line. Such research is critical to improve our knowledge of the role of the Internet as a conduit for crime, and the parallels between cybercrimes and real world offending.

V. References

Bacher, Paul, Thorsten Holz, Markus Kotter, and Georg Wicherski. 2005. *Tracking Botnets: Using honeynets to learn more about Bots.* The Honeynet Project and Research Alliance. Retrieved July 23, 2006 from http://www.honeynet.org/papers/bots/

Brenner, Susan W. 2008. *Cyberthreats: The Emerging Fault Lines of the Nation State.* New York: Oxford University Press.

Chien, Eric and Peter Szor. 2002. "Blended Attacks Exploits, Vulnerabilities and Buffer Overflow Techniques in Computer Viruses." *Virus Bulletin Conference.* Retrieved July 15, 2005 from http://enterprisessecurity.symantec.com/content/knowledgelibrary.cfm?EID=0

Choo, Kim-Kwang Raymond. 2007. "Zombies and botnets." *Trends and Issues in Crime and Criminal Justice.* Australian Institute of Criminology. Retrieved December, 28, 2007 from http://www.aic.gov.au/en/publications/current%20series/tandi/321-340/tandi333/view%20paper.aspx

Clarke, Ronald V. 1983. "Situational crime prevention: Its theoretical basis and practical scope." *Crime and Justice* 4: 225-256.

Clarke, Ronald V. 1995. "Situational crime prevention." Pp. 91-150. In *Crime and justice: A review of research*, edited by M. Tonry and D. Farrington. Chicago, IL: University of Chicago Press.

Clarke, Ronald V. 1997. *Situational crime prevention: Successful case studies* (2nd ed.). Guilderland, NY: Harrow and Heston.

Clarke, Ronald V., and Eck, John E. 2007. *Crime analysis for problem solvers in 60 small steps*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services. Retrieved April 20, 2007, from http://www.popcenter.org/Library/RecommendedReadings/60Steps.pdf

Collins, M. Patrick, Timothy J. Shimeall, Sidney Faber, Jeff Janies, Rhiannon Weaver, Markus De Shon, and Joseph Kadane. 2007. "Using uncleanliness to predict future botnet addresses." Proceedings of the 7th ACM SIGCOMM conference on Internet measurement. Pp. 93-104.

Computer Security Institute. 2009. "Computer Crime and Security Survey." Retrieved January 12, 2009, from (http://www.cybercrime.gov/FBI2009.pdf).

Cooke, Evan, Farnham Jahanian and Danny McPherson. 2005. "The zombie roundup: understanding, detecting, and disrupting botnets." *SRUTI '05 Workshop Proceedings*: 35-44. Berkeley CA: USENIX Association

Corbin, Juliet and Anselm Strauss. 1990. "Grounded Theory Research: Procedures, Canons, and Evaluative Criteria." *Qualitative Sociology* 13:3-21.

Cromwell, Paul F., James N. Olson, and D'Aunn W. Avary. 1991. "Breaking and Entering: An ethnographic analysis of burglary." *Studies in Crime, Law, and Justice*, 8. Newbury Park: Sage.

Cromwell, Paul F., James N. Olson, and D'Aunn W. Avary. 1993. "Who buys stolen property? A new look at criminal receiving." *Journal of Crime and Justice* 16:75-95.

Dagon, David, Cliff Zou, and Wenke Lee. 2006. "Modeling Botnet Propagation Using Time Zones." In *Proceedings of the 13th Network and Distributed System Security Symposium NDSS*.

Denning, D. E. 2001. "Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy." Pp. 239-288 in *Networks and Netwars: The Future of Terror, Crime, and Militancy,* edited by J. Arquilla and D. Ronfeldt. Santa Monica, CA: Rand.

Franklin, Jason, Vern Paxson, Adrian Perrig, and Stefan Savage. 2007. "An Inquiry into the nature and cause of the wealth of internet miscreants." Paper presented at CCS07, October 29-November 2, 2007 in Alexandria, VA.

Furnell, Steven. 2002. *Cybercrime: Vandalizing the Information Society*. Boston, MA: Addison-Wesley.

Goodin, Dan. 2008. "I was a teenage Bot Master." *The Register.* Retrieved October 20, 2008, from http://www.theregister.co.uk/2008/05/08/downfall_of_botnet_master_sobe_owns/

Gordon, Sarah. 2003. *Virus and Vulnerability Classification Schemes: Standards and Integration.* Symantec Security Response. Retrieved October 3, 2005 from http://enterprisesecurity.symantec.com/content/knowledgelibrary.cfm?EID=0

Gordon Sarah and Ma Qingxiong. 2003. *Convergence of Virus Writers and Hackers: Fact or Fantasy?* Cupertine, CA: Symantec.

Harocopos, Alex and Mike Hough. 2005. "Drug Dealing in Open-Air Markets." *Problem oriented guides for police: Response guide series (31).* Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Herbert, Steve. 1998. ''Police Subculture Reconsidered.'' Criminology 36: 343-369.

Holt, Thomas J. 2003. "Examining a Transnational Problem: An Analysis of Computer Crime Victimization in Eight Countries from 1999 to 2001." *International Journal of Comparative and Applied Criminal Justice* 27 (2): 199-220.

Holt, Thomas J. 2007. "Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures." *Deviant Behavior*, *28*, 171-198.

Holt, Thomas J. and Max Kilger. 2008. "Techcrafters and Makecrafters: A Comparison of Two Populations of Hackers." wistdcs,pp.67-78, *2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing.*

Holt, T.J., Soles, Joshua B., and Lyudmila Leslie. 2008. "Characterizing malware writers and computer attackers in their own words." Proceedings of the 2008 International Conference on Information Warfare and Security, Peter Kiewit Institute, University of Nebraska Omaha.

The Honeynet Project. 2001. *Know your enemy: Learning about security threats.* Boston, MA: Addison-Wesley.

Honeynet Research Alliance. 2003. Profile: Automated Credit Card Fraud. *Know Your EnemyPaper* series. Retrieved July 20, 2008, from http://www.honeynet.org/papers/profiles/cc_-fraud.pdf

Houle, Kevin and George Weaver. 2001. *Trends in denial of service attack technology.* CERT and CERT Coordination Center, Carnegie Mellon University.

Ianelli, Nicholas and Aaron Hackworth. 2005. *Botnets as a vehicle for online crime*. Pittsburgh PA: CERT Coordination Center

Jacobs, Bruce. 1996. "Crack dealers apprehension avoidance techniques: A case of restrictive deterrence." *Criminology* 34: 409-431.

Jacobs, Bruce. 1999. *Dealing Crack: The Social World of Streetcorner Selling.* Botson MA: Northeastern University Press.

Jacobs, Bruce. 2000. *Robbing drug dealers: Violence beyond the law*. New York: Aldine de Gruyter.

Jacobs, Bruce A., Volkan Topalli, and Richard Wright. 2000. "Managing Retaliation: Drug robbery and informal sanction threats." *Criminology* 38: 171-198.

Jewkes, Y. and K. Sharp. 2003. "Crime, deviance and the disembodied self: transcending the dangers of corporeality." Pp. 1-14 in *Dot.cons: Crime, deviance and identity on the Internet*, edited by Y. Jewkes. Portland, OR: Willan Publishing.

James, Lance. 2005. *Phishing Exposed.* Rockland: Syngress.

Jordan, Tim and Paul Taylor. 1998. "A Sociology of Hackers." *The Sociological Review* 46: 757-780.

Kapersky, Eugene V. 2003. *The Classification of Computer Viruses.* Metropolitan Network BBS Inc., Bern, Switzerland. Retrieved June 4, 2005 from http://www.avp.ch/avpve/classes/classes.stm

Karasaridis, Anestis, Brian Rexroad, and David Hoeflin. 2007. "Wide-scale Botnet Detection and Characterization." *USENEIX Workshop on Hot Topics in Understanding Botnets* (HotBots '07).

Keizer, Gregg. 2005. "Dutch botnet bigger than expected." *InformationWeek* October 21. Retrieved June 29, 2007 from http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=172303265

Longstaff, T. A., J. T. Ellis, S. V. Hernan, H. F. Lipson, R. D. McMillian, L. Hutz Pesante et al. 1997. "Security of the Internet." Pp. 231-255 in The Froehlich/Kent Encyclopedia of

Telecommunications (Vol. 15), edited by M. Dekker. Retrieved June 5, 2005 from http://www.cert.org/encyc_article/tocencyc.html.

Mann, David and Mike Sutton. 1998. "Netcrime: More Change in the Organization of Thieving." *British Journal of Criminology* 38: 201-29

Mathieson Sa. 2006. "Hot stocks to your inbox." *Infosecurity Today* 3(5): 10–13

McGarrell, Edmund F., Joshua D. Freilich, and Steve Chermak. 2007. "Intelligence-led Policing as a Framework for Responding to Terrorism." *Journal of Contemporary Criminal Justice* 23: 142-158.

Nazario, Jose. 2003. *Defense and detection strategies against Internet worms.* Artech House.

Newman, Grame and Ronald Clarke. 2003. *Superhighway robbery: Preventing e-commerce crime.* Cullompton: Willan Press.

PandaLabs. 2007. *Malware infections in protected systems.* Retrieved November 1, 2007, from http://research.pandasecurity.com/blogs/images/wp_pb_malware_infections_in_protected_systems.pdf

Provos, Niels, Panayiotis Mavrommatis, Moheeb Abu Rajab, and Fabian Monrose. 2008. "All your iFRAMEs point to us." *Proceedings of the 17th conference on Security Symposium*, p. 1-15.

Putnam, T.L., and D.D. Elliott. 2001. ''International responses to cyber crime.'' Pp.35-68 in A.D. Sofaer and S.E. Goodman (eds.), *The Transnational Dimension of Cyber Crime and Terrorism*. Stanford: Hoover Institution Press.

Rajab, Moheeb Abu, Jay Zarfoss, Fabian Monrose, and Andreas Terzis. 2006. "A Multifaceted Approach to Understanding the Botnet Phenonmenon." *IMC'06*: 41- 52.

Schneider, Jacqueline L. 2005. "Stolen-goods markets: Methods of Disposal." *British Journal of Criminology* 45: 129-140.

Scott, Micheal S., and Kelly Dedel. 2006. "Street prostitution." *Problem oriented policing guide series (2).* Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Sophos. 2007. *Did your PC try to bring down the internet last night? asks Sophos.* Retrieved February 7, 2008 from http://www.sophos.com/pressoffice/news/articles/2007/02/dnsbackbone.html

Steel, Chad. 2006. *Windows Forensics: The Field Guide to Corporate Computer Crime Investigations.* Somerset, NJ: Wiley.

Stevenson, Richard J., Lubica M. V. Forsythe, and Don Weatherburn, D. 2001. "The stolen goods market in New South Wales Australia: An analysis of disposal avenues and tactics." *British Journal of Criminology* 41: 101-118.

Sutton, Mike. 1998. "Handling Stolen Goods and Theft: A Market Reduction Approach." *Home Office Research Study 178.* London: Home Office Research and Statistics Directorate.

Symantec Corporation. 2003. *Symantec Internet Security Threat Report.* Retrieved October 3, 2005 from http://enterprisesecurity.symantec.com/content/knowledgelibrary.cfm?EID=0

Taylor, Paul A. 1999. *Hackers: Crime in the Digital Sublime.* New York: Routledge.

Taylor, Robert W., Tory J. Caeti, D. Kall Loper, Eric J. Fritsch, and John Liederbach. 2006. *Digital Crime and Digital Terrorism.* Upper Saddle River, NJ: Pearson Prentice Hall.

Thomas, Douglas. 2002. *Hacker Culture.* Minneapolis: University of Minnesota Press.

Thomas, Rob and Jerry Martin. 2006. "The underground economy: Priceless." *;login: The Usenix Magazine* 31(6): 7-17.

Wall, D.S. 2001. "Cybercrimes and the Internet." Pp. 1-17 in *Crime and the Internet,* edited by D. S. Wall. New York: Routledge.

Wall, David. 2007. *Cybercrime: The transformation of crime in the information age.* Cambridge: Polity Press.

Wright, Richard T, and Scott H. Decker. 1994. *Burglars on the Job: Streetlife and Residential Break Ins.* Boston: Northeastern University Press.

APPENDIX 1: FINDINGS OF BOT ANALYSES

Bot 1

MD5: e957108fbf8dff68195547316f98abee

Period: 04/30/2007 – 05/11/2007

AV Description

Symantec: W32.Spybot.Worm (Worm.SdBot-500224)

Bot System Interaction

Tried to connect to **zynus.myip.hu** and **danger.eternal-irc.net**

File Report

1 file wasadded
C:\WINDOWS\mswindll32.exe

DLL Report

1 DLL was removed: CLUSAPI.dll
12 DLLs were loaded

Services Report

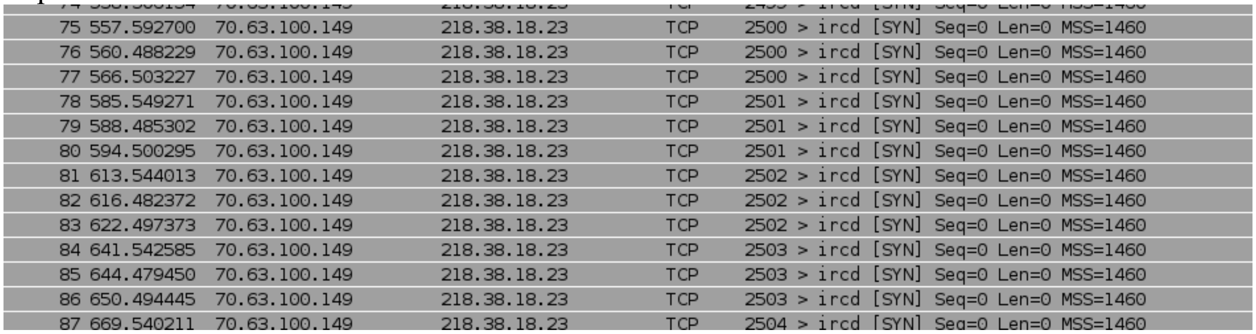
None Reported

Registry Report

None Reported

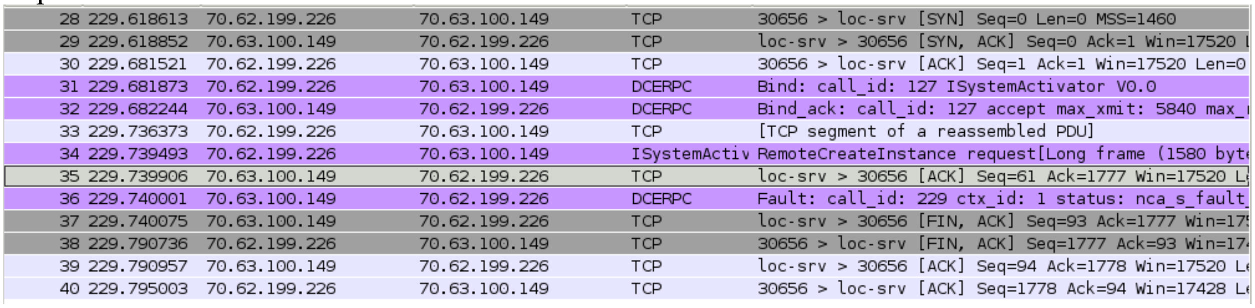
Observed Traffic

Consists mostly of ircd SYN requests to 1 IP: 218.38.18.23, the only DNS request



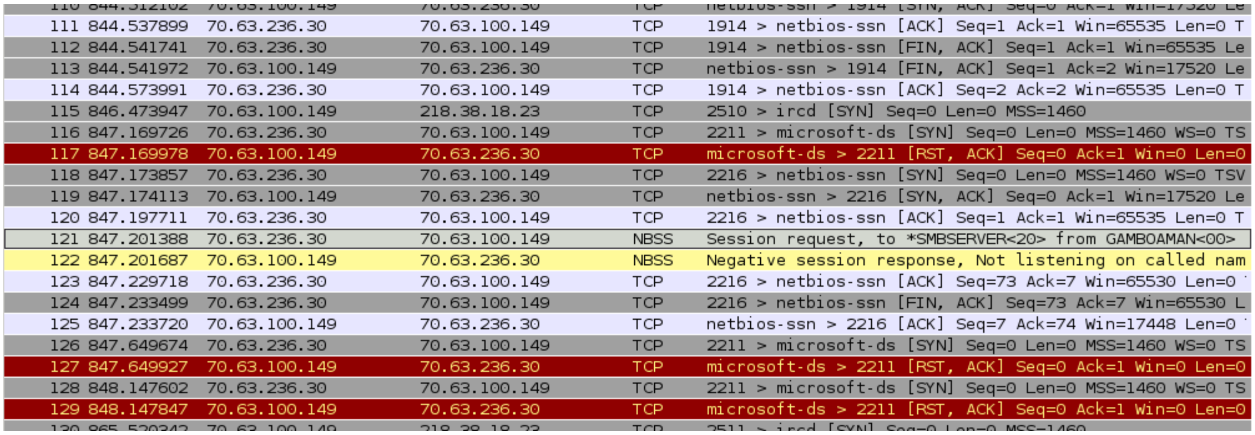
```
74 558.508154  70.63.100.149     218.38.18.23     TCP    2499 > ircd [SYN] Seq=0 Len=0 MSS=1460
75 557.592700  70.63.100.149     218.38.18.23     TCP    2500 > ircd [SYN] Seq=0 Len=0 MSS=1460
76 560.488229  70.63.100.149     218.38.18.23     TCP    2500 > ircd [SYN] Seq=0 Len=0 MSS=1460
77 566.503227  70.63.100.149     218.38.18.23     TCP    2500 > ircd [SYN] Seq=0 Len=0 MSS=1460
78 585.549271  70.63.100.149     218.38.18.23     TCP    2501 > ircd [SYN] Seq=0 Len=0 MSS=1460
79 588.485302  70.63.100.149     218.38.18.23     TCP    2501 > ircd [SYN] Seq=0 Len=0 MSS=1460
80 594.500295  70.63.100.149     218.38.18.23     TCP    2501 > ircd [SYN] Seq=0 Len=0 MSS=1460
81 613.544013  70.63.100.149     218.38.18.23     TCP    2502 > ircd [SYN] Seq=0 Len=0 MSS=1460
82 616.482372  70.63.100.149     218.38.18.23     TCP    2502 > ircd [SYN] Seq=0 Len=0 MSS=1460
83 622.497373  70.63.100.149     218.38.18.23     TCP    2502 > ircd [SYN] Seq=0 Len=0 MSS=1460
84 641.542585  70.63.100.149     218.38.18.23     TCP    2503 > ircd [SYN] Seq=0 Len=0 MSS=1460
85 644.479450  70.63.100.149     218.38.18.23     TCP    2503 > ircd [SYN] Seq=0 Len=0 MSS=1460
86 650.494445  70.63.100.149     218.38.18.23     TCP    2503 > ircd [SYN] Seq=0 Len=0 MSS=1460
87 669.540211  70.63.100.149     218.38.18.23     TCP    2504 > ircd [SYN] Seq=0 Len=0 MSS=1460
```

70.62.199.226 initiated DCOM create object instance request



```
28 229.618613  70.62.199.226   70.63.100.149   TCP          30656 > loc-srv [SYN] Seq=0 Len=0 MSS=1460
29 229.618852  70.63.100.149   70.62.199.226   TCP          loc-srv > 30656 [SYN, ACK] Seq=0 Ack=1 Win=17520 L
30 229.681521  70.62.199.226   70.63.100.149   TCP          30656 > loc-srv [ACK] Seq=1 Ack=1 Win=17520 Len=0
31 229.681873  70.62.199.226   70.63.100.149   DCERPC       Bind: call_id: 127 ISystemActivator V0.0
32 229.682244  70.63.100.149   70.62.199.226   DCERPC       Bind_ack: call_id: 127 accept max_xmit: 5840 max_
33 229.736373  70.62.199.226   70.63.100.149   TCP          [TCP segment of a reassembled PDU]
34 229.739493  70.62.199.226   70.63.100.149   ISystemActiv RemoteCreateInstance request[Long frame (1580 byte
35 229.739906  70.63.100.149   70.62.199.226   TCP          loc-srv > 30656 [ACK] Seq=61 Ack=1777 Win=17520 L
36 229.740001  70.63.100.149   70.62.199.226   DCERPC       Fault: call_id: 229 ctx_id: 1 status: nca_s_fault_
37 229.740075  70.63.100.149   70.62.199.226   TCP          loc-srv > 30656 [FIN, ACK] Seq=93 Ack=1777 Win=175
38 229.790736  70.62.199.226   70.63.100.149   TCP          30656 > loc-srv [FIN, ACK] Seq=1777 Ack=93 Win=174
39 229.790957  70.63.100.149   70.62.199.226   TCP          loc-srv > 30656 [ACK] Seq=94 Ack=1778 Win=17520 Le
40 229.795003  70.62.199.226   70.63.100.149   TCP          30656 > loc-srv [ACK] Seq=1778 Ack=94 Win=17428 Le
```

Repeated attempts to set up NetBIOS session from 70.63.236.30



```
110 844.512102  70.63.100.149   70.63.236.30    TCP   netbios-ssn > 1914 [SYN, ACK] Seq=0 Ack=1 Win=17520 Le
111 844.537899  70.63.236.30    70.63.100.149   TCP   1914 > netbios-ssn [ACK] Seq=1 Ack=1 Win=65535 Len=0 T
112 844.541741  70.63.236.30    70.63.100.149   TCP   1914 > netbios-ssn [FIN, ACK] Seq=1 Ack=1 Win=65535 Le
113 844.541972  70.63.100.149   70.63.236.30    TCP   netbios-ssn > 1914 [FIN, ACK] Seq=1 Ack=2 Win=17520 Le
114 844.573991  70.63.236.30    70.63.100.149   TCP   1914 > netbios-ssn [ACK] Seq=2 Ack=2 Win=65535 Len=0 T
115 846.473947  70.63.100.149   218.38.18.23    TCP   2510 > ircd [SYN] Seq=0 Len=0 MSS=1460
116 847.169726  70.63.236.30    70.63.100.149   TCP   2211 > microsoft-ds [SYN] Seq=0 Len=0 MSS=1460 WS=0 TS
117 847.169978  70.63.100.149   70.63.236.30    TCP   microsoft-ds > 2211 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
118 847.173857  70.63.236.30    70.63.100.149   TCP   2216 > netbios-ssn [SYN] Seq=0 Len=0 MSS=1460 WS=0 TSV
119 847.174113  70.63.100.149   70.63.236.30    TCP   netbios-ssn > 2216 [SYN, ACK] Seq=0 Ack=1 Win=17520 Le
120 847.197711  70.63.236.30    70.63.100.149   TCP   2216 > netbios-ssn [ACK] Seq=1 Ack=1 Win=65535 Len=0 T
121 847.201388  70.63.236.30    70.63.100.149   NBSS  Session request, to *SMBSERVER<20> from GAMBOAMAN<00>
122 847.201687  70.63.100.149   70.63.236.30    NBSS  Negative session response, Not listening on called nam
123 847.229718  70.63.236.30    70.63.100.149   TCP   2216 > netbios-ssn [ACK] Seq=73 Ack=7 Win=65530 Len=0
124 847.233499  70.63.236.30    70.63.100.149   TCP   2216 > netbios-ssn [FIN, ACK] Seq=73 Ack=7 Win=65530 L
125 847.233720  70.63.100.149   70.63.236.30    TCP   netbios-ssn > 2216 [ACK] Seq=7 Ack=74 Win=17448 Len=0
126 847.649674  70.63.236.30    70.63.100.149   TCP   2211 > microsoft-ds [SYN] Seq=0 Len=0 MSS=1460 WS=0 TS
127 847.649927  70.63.100.149   70.63.236.30    TCP   microsoft-ds > 2211 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
128 848.147602  70.63.236.30    70.63.100.149   TCP   2211 > microsoft-ds [SYN] Seq=0 Len=0 MSS=1460 WS=0 TS
129 848.147847  70.63.100.149   70.63.236.30    TCP   microsoft-ds > 2211 [RST, ACK] Seq=0 Ack=1 Win=0 Len=0
130 865.520342  70.63.100.149   218.38.18.23    TCP   2511 > ircd [SYN] Seq=0 Len=0 MSS=1460
```

Additional Information

DNS Queries: 218.38.18.23
Corresponding whois record:

Registered to:
bloodcrew (BLOODCREW4-HOLDER)
W4152 Wendy Ln
Fond du LaC, WI 54935, US
Domain Name: BLOODCREW.NET
Registered through: 1stDomain.net
Administrative Contact, Technical Contact, Zone Contact:
Ann Harshbarger (ANHA2109F) upol4you@yahoo.com
W4152 Wendy Ln
Fond du Lac, WI 54935, US
+920-923-1784
Billing Contact:
Valerie Sanchez (VASA2103F) upol4you@hotmail.com
Sanchez
Bronx, ny 10455, US
+920-923-1784
Domain created: 2005-10-20.

```
Domain last updated: 2006-07-12.
Domain expires: 2010-10-20.
Name servers for this domain:
NS2.PMSDNS.ORG   63.101.245.10   (HO113681F)
NS1.PMSDNS.ORG   217.160.246.244 (HO113680F)
```

Bot 2

MD5: cdf8c960721ccee3d27773a7e81488

Period: 05/12/2008 – 05/25/2008

AV Description

Symantec: W32.Spybot.Worm

Bot System Interaction

Tried to connect to **irc.nerashti.com**with the following channel name and key attribute: #nerashti# (channel) and spy (key)

File Report

21 Files were changed and
6 Files were added including the infection: C:\WINDOWS\system32\wuaumqr1.exe

DLL Report

21 DLLs were loaded

Services Report

None Reported: System crashed

Registry Report

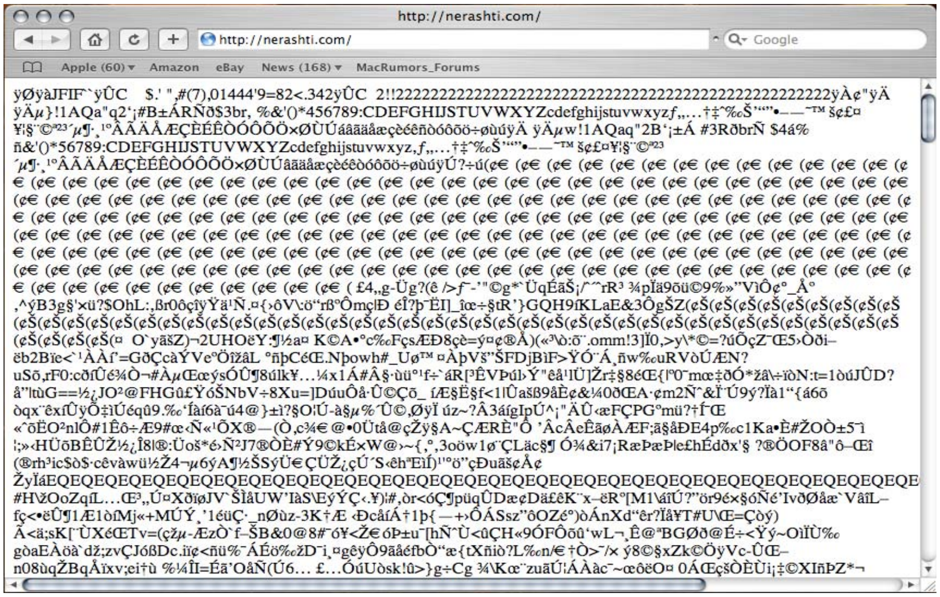
None Reported: System crashed

Observed Traffic

None: System crashed

Additional Information

Secondary Injectionwas discovered. The file name was spy.exe and its MD5 value was 9aff64aad4d3011e6aaa907b5004d578. The following snapshot shows the first page when we attempt to access the site: **nerashti.com**.



```
ÿØÿàJFIF``ÿÛC    $.' ",#(7),01444'9=82<.342ÿÛC  2!!22222222222222222222222222222222222222222222222222ÿÀ¢"ÿÄ
ÿÄµ}!1AQa"q2'¡#B±ÁRÑð$3br, %&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyzƒ„…†‡ˆ‰Š'""•–—˜™ š¢£¤
¥¦§¨©ª²³´µ¶·¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚáâãäåæçèéêñòóôõö÷øùúÿÄ ÿÄµw!1AQaq"2B'¡±Á #3RðbrÑ $4á%
ñ&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz‚ƒ„…†‡ˆ‰Š'""•–—˜™ š¢£¤¥¦§¨©ª²³
´µ¶·¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚâãäåæçèéêòóôõö÷øùúÿÚ?÷ú(¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢
€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€
(¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢
€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€
(¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢
€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€
(¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢
€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ (¢€ ( £4„g-Üg?(ê />ƒ¯-'"©g*`ÜqÉãŠ¡/ˆˆrR³ ¾pÏä9õü©9%»"VìÔ¢°_Å°
,^ýB3g§'×ü?$OhL:,ßr0ôçîÿŸä¹Ñ.¤{›ôV\:ö"rß°Ômç|Ð éÎ?þ¯ËI]_îœ÷§tR'}GQH9ïKLaE&3ÔgŠZ(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š
(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š(¢Š
(¢Š(¢Š(¢Š(¢Š(¤  O`yãšZ)¬2UHOëY:¶½a¤ K©A•°c‰FçsÆÐ8çè=ý¤¢®Å)(«³\ò:õ¨.omm!3]Ï0,>y\*©=?úÕçZ¯Œ5›Òði–
ëb2Bïe<`¹ÀÀí'=GðÇcàÝVeºÖîžâL °ñþCéŒ.Nþowh#_Uø™ ¤ÀþVš"ŠFDjBìF>ŸÓ¨Á¸ñw‰uRVòÚÆN?
uSõ,rF0:cðíÛé¾Ò¬#ÀµŒœýsÓÛ¶8úlk¥…¼x1Á#Â§·ùü°¹f÷`áR[³ÊVÞúl›Ý"êå¹lÜ]Žr‡§8éŒ{|º0¯mœ‡ðÓ*žâ\÷ïòN:t=1òúJÛD?
å"|tùG==½¿JO²@FHGû£ŸóŠNbV÷8Xu=]DúuÔå·Û©Çõ_ íÆ§Ë§f<1|ÛašB9åÈ¢&¼0ðŒA·¢m2Ñ^&Ï¨Ú9ý?Ïà1"{á6õ
òqx¨êxíÛÿÕ‡ìÚéqû9.‰'Íàí6à¯ú4@}±ì?§O¦Ú-à§µ%´Û©,ØÿÏ úz~?Â3áígIpÚ^¡"ÄÛ‹æFÇPGºmü?†Í¯Œ
«ˆõËO²nlÔ#1Êô÷Æ9#œ‹Ñ«¹ÕX®—(Ò,c¾€ @•0Ütå@çŽÿ§A~ÇÆRÈ"Ô 'ÂcÂeÊãøÀÆF;ã§åÐE4p‰c1Ka•È#ŽOÒ±5¯ì
¦;»‹HÜõBÊÛŽ½¿Î8|®:Üoš*é›Ñ²J7®ÒÈ#Ý9©kÉ×W@›~{,°,3oöw1ø¨ÇLäc§¶ Ó¾&i7¡RæÞæÞ|e£hÉdðx'§ ?®ÖOF8â"ô–Œî
(®rh³ic$ò$·cêvàwü½Ž4¬µ6ýA¶½ŠSýÜ€ÇÜŽ¿çÚ´S‹êhªEìÍ)¹°ö"çÐuãš¢Å¢
ŽyÏáEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQEQE
#H\žOoZqíL…Œ³„Ú¤XðïøJV`ŠÌåUW'IàS\EýÝÇ‹.¥)|#,òr<óÇ¶püqÛDæ¢Dä£êK¨x–ëR°[M1\áîÚ?"ör9é×§óÑé'IvðØåæ`VâîL–
fç<•ëÛ¶1Æ1òíMj«+MÚÝ¸'1éüÇ·_nØùz-3K†Æ ‹ÐcåíÁ†1þ{—+›ÔÁSsz"ôOZé°)òÁnXd"êr?Ïå¥T#U\Œ=Çòý)
Ã<ä;sK[¨ÙXéŒTv=(çžµ-ÆzÒ`f–ŠB&0@8#¯ó¥<Ž€óÞ±u¯[hÑ^Ù<ûÇH«9ÓFÔõû'wL¬¸Ê@ªBGØð@É÷<Ÿý~OìÏÙ‰
gòaEÀöà`dž;zvÇJóßDc.ïï¢<ñü%¯ÁÉö‰žD¯i¸¤gêÿÔ9ãåéfbÒ"æ{tXñiò?L‰n/€ †Ò>¯/× ý8©§xZk©ÖÿVc-ÛŒ–
n08ùqŽBqÅïxv;ei†ù %¼ÎI=Éã'OåÑ(Ú6… £…ÓúUòsk!û>}g÷Cg ¾\Kœ¨zuãÚ¦ÁÀàc¯~œôëO¤ 0ÁŒçšÒÈÙi¡‡©XIñÞZ*¬
```

DNS Queries: 66.218.79.147

Corresponding whois record:

OrgName: Yahoo!
OrgID: YAOO
Address: 701 First Ave
City: Sunnyvale
StateProv: CA
PostalCode: 94089
Country: US

Bot_3

MD5: 5313a0dbc6759a6e917930e5f3f7ad56

Period: 05/22/2007 – 05/29/2007

AV Description

Symantec: Worm.SdBot-500224

Bot System Interaction

Tried to connect to **zynus.myip.hu** and **danger.eternal-irc.net**

File Report

None Reported

DLL Report

None Reported

Services Report

None Reported

Registry Report

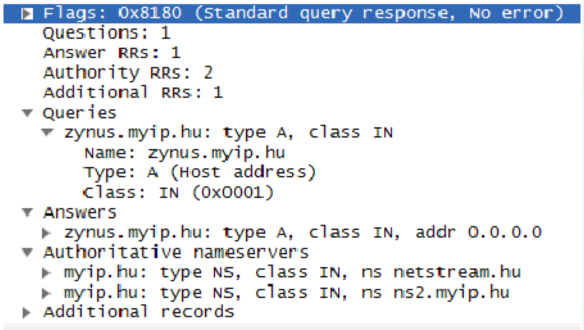
None Reported

Observed Traffic

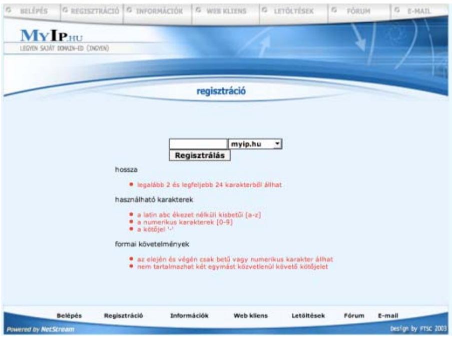
None Reported

Additional Information

myip.hu is a free domain name registration service in Hungary and Zynus.myip.hu resolves to 0.0.0.0 after being identified as malicious host.



```
▶ Flags: 0x8180 (Standard query response, No error)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 2
  Additional RRs: 1
▼ Queries
  ▼ zynus.myip.hu: type A, class IN
      Name: zynus.myip.hu
      Type: A (Host address)
      Class: IN (0x0001)
▼ Answers
  ▶ zynus.myip.hu: type A, class IN, addr 0.0.0.0
▼ Authoritative nameservers
  ▶ myip.hu: type NS, class IN, ns netstream.hu
  ▶ myip.hu: type NS, class IN, ns ns2.myip.hu
▶ Additional records
```



regisztráció

[ ] myip.hu ▾
Regisztrálás

hossza

- legalább 2 és legfeljebb 24 karakterből állhat

használható karakterek

- a latin abc ékezet nélküli kisbetűi [a-z]
- a numerikus karakterek [0-9]
- a kötőjel '-'

formai követelmények

- az elején és végén csak betű vagy numerikus karakter állhat
- nem tartalmazhat két egymást közvetlenül követő kötőjelet

DNS Queries: 62.112.194.220
Corresponding whois record:

```
domain:        myip.hu
org:           Private person
org:           org_name_hun: Marcz Gábor
hun-id:        0991233439
admin-c:       2000773978
tech-c:        2000252017
zone-c:        2000252017
nameserver:    ns.myip.hu
nameserver:    ns2.myip.hu
registered:    2002.12.03 01:00:15
changed:       2008.04.14 08:31:50
registrar:     1000600228

person:        Marcz Gábor
address:       Kossuth L. 122
address:       7727 Palotabozsok
address:       HU
phone:         +36 30 314 6575
fax-no:
hun-id:        2000773978

person:        Marcz Gábor
address:       Kossuth L. 122
address:       7727 Palotabozsok
address:       HU
phone:         +36 30 314 6575
fax-no:
e-mail:
hun-id:        2000252017

person:        Marcz Gábor
address:       Kossuth L. 122
address:       7727 Palotabozsok
address:       HU
```

```
phone:        +36 30 314 6575
fax-no:
hun-id:       2000252017

org:          org_name_eng: HW24 Bt.
org:          org_name_hun: HW24 Bt. (Registrar)
address:      Õsz u. 133. 3/10
address:      1045 Budapest
address:      HU
phone:        +36 1 3903130
fax-no:       +36 1 3903130
hun-id:       1000600228
```

Bot 4

MD5: dae674b8e6625268a21324a41debcb58

Period: 07/02/2007 – 07/05/2007

AV Description

Symantec: W32.Spybot.Worm

Bot System Interaction

Tried to connect to **mansql.bsd.st** with a higher port number 6667 and following IRC credentials: ##speed## (Chanel), FAST (Key) and tiesto&edsy (Botmasters).

File Report

4 files were added:

```
Ehncze.exe
CatRoot2/tmp.edb
RUNDLL32.EXE-160FACFA.pf
NETSTAT.EXE-2B2B4428.pf
```

DLL Report

None Reported

Services Report

2 new services were started:
Telephony Service was triggered and *Remote Access Connection Manager* was also initiated which is dependent on the Telephony service. Telephony service may control all dial-up activity and some cable/DSL activity.

Registry Report

None Reported

Observed Traffic

The following IRC traffic was observed:

```
NICK [XP]|7528552201651728
USER dcoimkjdtdorexuran 0 0 :[XP]|7528552201651728
```

```
…
:Army.34045.org 002 [XP]|7528552201651728 :Your host is Army.34045.org, running
version   Unr3414stic(ArmyNet0wnz)
:Army.34045.org 003 [XP]|7528552201651728 :This server was created Sat Dec  4
17:34:45 2004
…
USERHOST [XP]|7528552201651728
:[XP]|7528552201651728 MODE [XP]|7528552201651728 :+iwp
MODE [XP]|7528552201651728 -x+Bi
JOIN ##speed## FAST
:[XP]|7528552201651728 MODE [XP]|7528552201651728 :+B
:[XP]|7528552201651728!~dcoimkjdt@rrcs-70-63-100-149.midsouth.biz.rr.com JOIN
:##speed##
:Army.34045.org 332 [XP]|7528552201651728 ##speed## :.remove -r
:Army.34045.org 302 [XP]|7528552201651728
:[XP]|7528552201651728=+~dcoimkjdt@rrcs-70-63-100-149.midsouth.biz.rr.com
PRIVMSG ##speed## :[SCAN]: Random Port Scan started on 70.63.x.x:2967 with a
delay of 5 seconds for 800 minutes using 100 threads.
PRIVMSG ##speed## :[SCAN]: Random Port Scan started on 70.63.x.x:139 with a delay
of 5 seconds for 800 minutes using 100 threads.
…
PING :Army.34045.org
PONG :Army.34045.org
```

Additional Information

The identified *ehncze.exe* was started. It was used for port scanning and attempted to make a remote connection using the Telephony/RACM services.

DNS Queries: 209.63.212.17

Corresponding whois record:

```
OrgName:          Electric Lightwave Inc
OrgID:  ELIX
Address:        4400 NE 77th Ave
City:         Vancouver
StateProv:       WA
PostalCode:      98662
Country:        US
NetRange:        209.63.0.0 - 209.63.255.255
CIDR:         209.63.0.0/16
NetName:        NETBLK-ELI-NETBLK7
```

Bot 5

MD5: 9645b82cc3db9cf14419d9433203b983

Period: 07/09/2007 – 07/12/2007

AV Description

Symantec: Trojan.SdBot-6530

Bot System Interaction

Tried to connect to **w.rtsfgwq.org** with following IRC credentials: ##waj## (Channel) and p00n3d (Key)

File Report

4 files were added:
C:\WINDOWS\system32\dllcache\dsrss.exe
C:\WINDOWS\CatRoot2\tmp.edb
C:\WINDOWS\prefetch\RUNDLL32.EXE-2B55B9B2.pf
C:\WINDOWS\prefetch\DSRSS.EXE-39BA95C9.pf

DLL Report

None Reported

Services Report

4 services were stopped and 3 new services were started.

- Firewall/Internet Connection Sharing was stopped
- Security Center was stopped and the configuration was changed from *auto* to *disabled*
- Application Layer Gateway was stopped
- Remote Registry was stopped and the configuration was changed from *auto* to *disabled*
- Service *dsrss* was started, which was added as a prefetch file
- Telephony service was started and Remote Access Connection Manager was started

Observed Traffic

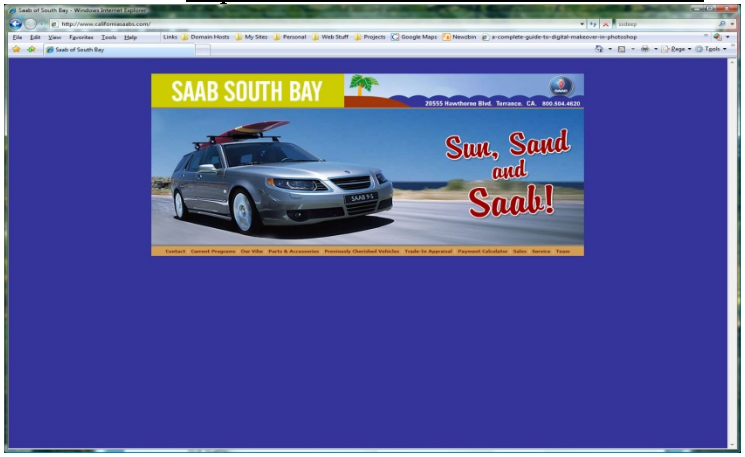
The following IRC traffic was observed:

```
PASS r0flc0mz
NICK [00|USA|609912]
USER XP-2946 * 0 :OWNER-SKT30L1TV
```

```
:psyBNC 001 [00|USA|609912] :MySQL  [00|USA|609912]!~XP-2946@rrcs-70-63-100-
148.midsouth.biz.rr.com
:psyBNC 376 [00|USA|609912] :
:[00|USA|609912] MODE [00|USA|609912] :+i
MODE [00|USA|609912] -x+i
JOIN #waj# p00n3d
:[00|USA|609912]!~XP-2946@rrcs-70-63-100-148.midsouth.biz.rr.com JOIN :#waj#
:psyBNC 332 [00|USA|609912] #waj# :
!t kill all -s|
!sftp 129.93.14.72 2755 1 1 ze1.exe -s|
!asc sym 30 3 0 -c -s|
!ascnetapi 30 3 0 -c -s|
!asc dcom139 30 3 0 -c -s|
!asc asn445 30 3 0 -c -s|
!asc rpc135 30 3 0 -c -s|
!it.wget -S|
!it.wget http://www.californiasaabs.com/bb2.exe c:\sdsed.exe r
:psyBNC 333 [00|USA|609912] #waj# 10:30 PM 1183993307
:psyBNC 366 [00|USA|609912] #waj# :End of /NAMES list.
MODE #waj#
PRIVMSG #waj# :.DOWNLOAD :: . Bad URL or DNS Error, error: <12002>
```

Additional Information

1 secondary injection was downloaded from #waj# channel. The source of the downloaded executable is http://www.californaisaabs.com/bb2.exe .


Saab of South Bay - Windows Internet Explorer
http://www.californiasaabs.com/
SAAB SOUTH BAY
20555 Hawthorne Blvd. Torrance, CA. 800.504.4620
Sun, Sand and Saab!

It seems to be a legitimate site unknowingly running an IRC server.

- **South Bay Saabs**
  - 20555 Hawthorne Blvd.
  - Torrance, CA 90503
  - Phone: 800.504.4620
  - Fax: 310.371.6150

DNS Queries: 74.52.234.114 (w.rtsfgwq.org) and 216.55.186.52 (californiasaabs.com)

Corresponding whois records:

74.52.234.114

```
OrgName:    ThePlanet.com Internet Services, Inc.
OrgID:      TPCM
Address:    1333 North Stemmons Freeway
Address:    Suite 110
City:       Dallas
StateProv:  TX
PostalCode: 75207
Country:    US
NetRange:   74.52.0.0 - 74.54.255.255
CIDR:       74.52.0.0/15, 74.54.0.0/16
NameServer: NS1.THEPLANET.COM
NameServer: NS2.THEPLANET.COM
Comment:
RegDate:    2006-02-17
Updated:    2007-07-11
```

216.55.186.52

```
OrgName:    Abacus America Inc.
OrgID:      ABAC
Address:    10350 Barnes Canyon Rd.
City:       San Diego
StateProv:  CA
PostalCode: 92121
Country:    US
NetRange:   216.55.128.0 - 216.55.191.255
CIDR:       216.55.128.0/18
NameServer: NS1.ABAC.COM
NameServer: NS2.ABAC.COM
RegDate:    1999-05-28
Updated:    2000-11-02
```

Bot 6

MD5:9f2aae0d6420b6be80b8bc0f57f76183

Period: 07/16/2007 – 07/23/2007

AV Description

None

Bot System Interaction

Tried to connect to **xx.ka3ek.com** for IRC botnet traffic.

File Report

1 file was added:

C:\Windows\system32\spooIsv.exe

spooIsv.exe (a.k.a. W32.Linkbot.M) is a worm that exploits the Microsoft Windows LSASS Buffer Overrun Vulnerability (BID 10108) in order to propagate. It also creates a back door on the compromised computer

DLL Report

7 DLL were loaded and 1 DLL was removed. A list of related DLLs is as follows:
C:\WINDOWS\System32\CLUSAPI.dll was removed from memory.
    (Note. Required when running windows SP1 update)
C:\WINDOWS\system32\winmm.dll was loaded into memory.
C:\WINDOWS\system32\wininet.dll was loaded into memory.
C:\WINDOWS\system32\pstorec.dll was loaded into memory.
C:\WINDOWS\System32\zipfldr.dll was loaded into memory.
C:\WINDOWS\system32\mpr.dll was loaded into memory.
C:\WINDOWS\system32\psapi.dll was loaded into memory.
C:\WINDOWS\System32\shdocvw.dll was loaded into memory

Services Report

None Reported

Registry Report

None Reported

Observed Traffic

The following IRC traffic was observed:

```
USER qxhgezqxhgezqxhgez :cdyotbtpkannjhlv
NICK TdrHImSL
PING :E0116AD4
PONG :E0116AD4
:irc.foonet.com 001 TdrHImSL :
:TdrHImSL!qxhgez@rrcs-70-63-100-148.midsouth.biz.rr.com
JOIN :#badbotbad
:irc.foonet.com 332 TdrHImSL #badbotbad :.remove
:irc.foonet.com 333 TdrHImSL #badbotbadjoeblow 1177950341
:irc.foonet.com 353 TdrHImSL = #badbotbad :TdrHImSL @joeblow
:irc.foonet.com 366 TdrHImSL #badbotbad :End of /NAMES list.
MODE TdrHImSL +xi
:irc.foonet.com NOTICE TdrHImSL :Setting/removing of usermode(s) 'xpqTds' has been disabled.
:TdrHImSL MODE TdrHImSL :+i
JOIN #last
MODE #badbotbad +smntu
:TdrHImSL!qxhgez@rrcs-70-63-100-148.midsouth.biz.rr.com
JOIN :#last
:irc.foonet.com 353 TdrHImSL = #last :TdrHImSL
:irc.foonet.com 366 TdrHImSL #last :End of /NAMES list.
:irc.foonet.com 482 TdrHImSL #badbotbad :You're not channel operator
MODE #last +smntu
:irc.foonet.com 482 TdrHImSL #last :You're not channel operator
PING :irc.foonet.com
PONG :irc.foonet.com
```

Also, UDP traffic with destination port 16390 was received from multiple sources.

In addition, our Sandnet module generated the following IRC traffic from Simulated Internet:

```
USER qskepcqskepcqskepc :akfylkcyzfvotlus
NICK KwGptJxQ
:MySQL 001 KwGptJxQ :MySQL  KwGptJxQ!~KwGptJxQ.5.6.7
:MySQL 376 KwGptJxQ :
MODE KwGptJxQ +xi
JOIN #last
:KwGptJxQ!x@x.org JOIN :#last
:MySQL 332 KwGptJxQ #last :!trace 15 120 500
:MySQL 333 KwGptJxQ #last a 1181153293
:MySQL 353 KwGptJxQ @ #last :KwGptJxQ @a @b
```

```
:MySQL 366 KwGptJxQ #last :End of /NAMES list.
MODE #last +smntu
```

We also investigated strings from Binary as follows:

```
Offset     (printable characters > 4)
 515936      C:\WINDOWS\System32\ADVAPI32.dll
 516464      C:\WINDOWS\system32
 527960      Themida
750628      3An internal exception occured (Address: 0x%x)
 869684      3Sorry, this application cannot run under a Virtual Machine
 750676      Please, contact support@oreans.com. Thank you!
 908088      Service Pack 1
 918646      spoolsvc.exe
 115296      admin$
 115912      administrat
 115924      administrateur
 115780      wwwadmin
120231      kInternet explorer password stealer
 121100      passwort
 121140      pass=
 121156      password=
```

Additional Information

There existed an open TCP connection between 70.63.100.148:139 and 70.63.191.86:4330 and the identified worm was installed and executed: C:\WINDOWS\system32\spooIsv.exe (PID: 1572) was started

DNS Queries: 67.43.236.66

Corresponding whois record:

```
OrgName: GloboTech Communications
OrgID: GLOBO
Address: 20 Rue Deschenes
City: Saint-Quentin
StateProv: NB
PostalCode: E8A-1M1
Country: CA
NetRange:   67.43.224.0 - 67.43.239.255
CIDR:       67.43.224.0/20
NetName:    GTCOMM
NetHandle:  NET-67-43-224-0-1
NameServer: DNS1.GTCOMM.NET
NameServer: NS1.GTCOMM.NET
Comment:    Standard hours are 8am to 9pm AST
Comment:    rwhois1.gtcomm.net port 4321
RegDate:    2004-03-25
Updated:    2004-03-25
```

```
OrgTechHandle: PQU-ARIN
OrgTechName:   Quimper, Pierre-Luc
OrgTechPhone:  +1-866-802-2200
OrgTechEmail:  plquimper@gtcomm.net
```

Bot 7

MD5: 94c74a66dd3838f8117601dc86dc7e5a

Period: 07/16/2007 – 07/23/2007

AV Description

ClamAV: TR/CryptExe.A

Bot System Interaction

Tried to connect to **nagoo.nagitiriheiwu.netchannel** for IRC botnettraffic.

File Report

None Reported

DLL Report

None Reported

Services Report

None Reported

Registry Report

None Reported

Observed Traffic

None Reported

Additional Information

DNS Queries: nagoo.nagitiriheiwu.netchannel was an unregistered domain name so it was not successful to obtain the corresponding whois record.

Bot 8

MD5: 5a81bc907a289536818e7a294232e403

Period: 07/17/2007 – 07/23/2007

AV Description

Symantec: backdoor.rbot.xfv

Bot System Interaction

Tried to connect to **home.najd.us**with the following IRC credential: #dd (Channel) and dpass (Key)

File Report

None Reported

DLL Report

None Reported

Services Report

None Reported

Registry Report

None Reported

Observed Traffic

Samba Traffic from the following IP address was observed: 70.63.199.159. Samba is an Open Source Software suite that provides seamless file and print services to SMB/CIFS clients.

Additional Information

No services or additional traffic discovered due to system crash.

DNS Queries**:** 207.158.49.42

Corresponding whois record:

OrgName: American Internet Services, LLC.
OrgID: AMERI-504

```
Address:    9305 Lightwave Ave.
City:       San Diego
StateProv:  CA
PostalCode: 92123
Country:    US

ReferralServer: rwhois://rwhois.americanis.net:4321

NetRange:   207.158.0.0 - 207.158.63.255
CIDR:       207.158.0.0/18
OriginAS:   AS6130
NetName:    AIS-WEST2
NetHandle:  NET-207-158-0-0-1
Parent:     NET-207-0-0-0-0
NetType:    Direct Allocation
NameServer: NS1.AMERICANIS.NET
NameServer: NS2.AMERICANIS.NET
Comment:    ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE.
RegDate:    1996-06-22
Updated:    2008-12-10

OrgAbuseHandle: ABUSE1714-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-858-576-4272
OrgAbuseEmail:

OrgNOCHandle: NOC2657-ARIN
OrgNOCName:   NOC
OrgNOCPhone:  +1-858-576-4272
OrgNOCEmail:

OrgTechHandle: AIS10-ARIN
OrgTechName:   AIS
OrgTechPhone:  +1-858-576-4272
OrgTechEmail:

OrgName:    Law Office of Walter Maund
OrgID:      LOWM
Address:    707 Broadway Stuite 1800
City:       San Diego
StateProv:  CA
PostalCode: 92101
Country:    US

NetRange:   207.158.49.40 - 207.158.49.47
CIDR:       207.158.49.40/29
```

```
NetName:    ADN-WALTERMAUND-NETBLK
NetHandle:  NET-207-158-49-40-1
Parent:     NET-207-158-0-0-1
NetType:    Reassigned
Comment:
RegDate:    2003-04-04
Updated:    2003-04-04

RNOCHandle: NAM1-ARIN
RNOCName:   Montante, Nick Alan
RNOCPhone:  +1-858-576-4272
RNOCEmail:

OrgTechHandle: JBO29-ARIN
OrgTechName:   Borobia, John
OrgTechPhone:  +1-619-234-8261
OrgTechEmail:

== Additional Information From rwhois://rwhois.americanis.net:4321 ==

network:Class-Name:network
network:ID:NETBLK-207.158.49.40/29
network:Auth-Area:207.158.0.0/18
network:Network-Name:22316-207.158.49.40/29
network:IP-Network:207.158.49.40/29
network:IP-Network-Block:207.158.49.40 - 207.158.49.47
network:Organization;I:ID22316
network:Tech-Contact;I:
network:Admin-Contact;I:
network:Created:20051103
network:Updated:20051103
network:Updated-By:

network:Class-Name:network
network:ID:AIS-SDTC-NETBLK-1
network:Auth-Area:207.158.0.0/18
network:Network-Name:1-207.158.0.0/18
network:IP-Network:207.158.0.0/18
network:IP-Network-Block:207.158.0.0 - 207.158.63.255
network:Organization;I:AHL-42
network:Tech-Contact;I:
network:Admin-Contact;I:
network:Created:20050308
network:Updated:20050308
network:Updated-By:
```

Bot 9

MD5: 6f485878487dd6c866845736c4977429

Period: 08/21/2007 – 08/26/2007

AV Description

Symantec: Trojan.Vundo. Trojan.Vundo is a component of an adware program that downloads and displays pop-up advertisements. It is known to be installed by visiting a Web site link contained in a spammed email.

Bot System Interaction

It seems the following sites are the destination: Fuck.urpal43sourpalhuh.com, Japan.youngpeyatech.info, Done.blacktiehsbdcs.com

File Report

1 file was added:
C:\Windows\system32\lssas.exe

DLL Report

6 DLLs were loaded. A list of DLLs is as follows:
C:\WINDOWS\system32\wininet.dll was loaded into memory.
C:\WINDOWS\system32\pstorec.dll was loaded into memory.
C:\WINDOWS\system32\zipfldr.dll was loaded into memory.
C:\WINDOWS\system32\mpr.dll was loaded into memory.
C:\WINDOWS\system32\psapi.dll was loaded into memory.
C:\WINDOWS\system32\shdocvw.dll was loaded into memory.

Services Report

None Reported

Registry Report

None Reported

Observed Traffic

None Reported

Additional Information

<u>DNS Queries</u>: 67.43.236.98
Corresponding <u>whois</u> record:

```
OrgName:        GloboTech Communications
OrgID:  GLOBO
Address:        PO Box 1402
City:   Saint-Quentin
StateProv:      NB
PostalCode: E8A-1A2
Country:        CA
NetRange:   67.43.224.0 - 67.43.239.255
CIDR: 67.43.224.0/20
NetName:        GTCOMM
NetHandle:  NET-67-43-224-0-1
Parent: NET-67-0-0-0-0
NetType:        Direct Allocation
NameServer: DNS1.GTCOMM.NET
NameServer: NS1.GTCOMM.NET
Comment:        Standard hours are 8am to 9pm AST
Comment:        rwhois1.gtcomm.net port 4321
RegDate:        2004-03-25
Updated:        2004-03-25
```

Bot 10

MD5: 2f6abb3f4cfdbce5e85949c06f86e1c2

Period: 10/08/2007 – 10/15/2007

AV Description

Dialer.Trafficjam is a dialer application that dials a premium rate service using a modem .

Bot System Interaction

Tried to connect to **Belsim.com** andBotprocess *angmang.exe* was started on the system

File Report

3 files were added

C:\WINDOWS\Prefetch\TRAY.EXE-1461F435.pf was added
C:\WINDOWS\system32\inetsrv\tray.exe was added

> Tray.exe is a process belonging to Paragon CD-ROM Emulator. A third party software vendor. This process has also been associated with a *homepage hi-jacker*application. Inetsrv directory is home for microsoft IIS server config files such as Metabase.xml, iisadmin.dll, smtpsvc.dll and more

C:\WINDOWS\Prefetch\RUNDLL32.EXE-264FBB8C.pf was added

DLL Report

10 DLLs were loaded. A list of DLLs is as follows:
C:\WINDOWS\system32\browselc.dll was loaded into memory.

> Shell Browser UI Library: is component of the file that provides functions for the shell browser interface in Windows.

C:\WINDOWS\system32\odbc32.dll was loaded into memory.

> Microsoft Data Access – ODBC: contains functions for the ODBC database query standard.

C:\WINDOWS\system32\icmp.dll was loaded into memory.

> Windows ICMP API: a module used by Windows 2000

C:\WINDOWS\system32\user32.dll was loaded into memory.

> Windows User API Client DLL: a module that contains Windows API functions related the Windows user interface (Window handling, basic UI functions).

C:\WINDOWS\system32\MLANG.dll was loaded into memory.

Multi Language Support DLL: module that provides multi-language support functions. It contains functions for translation of current Internet character sets to Unicode and back.

C:\WINDOWS\system32\wininet.dll was loaded into memory.

Internet Extensions for Win32: is a module that contains Internet-related functions used by Windows applications. Note: wininet.dll is a process which the Troj/Zlob-AO trojan tries to disguise itself as under the true process name of %systemroot%\mscornet.exe.

C:\WINDOWS\system32\avicap32.dll was loaded into memory.

Video For Windows API DLL: module that contains functions for the Windows API that is used to capture AVI movies and video from web cameras and other video hardware.

C:\WINDOWS\System32\zipfldr.dll was loaded into memory.

Compressed (zipped) Folders: is module that handles compressed container.

C:\WINDOWS\system32\Cabinet.dll was loaded into memory.

Microsoft Cabinet File API: module that contains functions used by a cabinet file API.

C:\WINDOWS\system32\shdocvw.dll was loaded into memory.

Microsoft Shell Doc Object and Control Library: library used by Windows applications to add basic file and networking operations.

Services Report

None Reported

Registry Report

The following registry information was updated:
…software\Microsoft\Windows\CurrentVersion\Run
"System Tray Monitor" = C:\WINDOWS\SYSTEM32\inetsrv\tray.exe

Observed Traffic

```
From Client
NICK [00][XP][SP2][USA]-252433088.
USER . 0 0 :

From Server
:irc.foonet.com 432  [00][XP][SP2][USA]-252433088. :Erroneous
        Nickname: Illegal characters
ERROR :Closing Link: [70.63.100.148] (Ping timeout)
```

Additional Information

The binary executable file appeared to be packed several times. Relevant packer information is as follows.

Packer Information

Entry Point:00001000
EP Section:.text
File Offset:00000400
First bytes: B8, D8, 3C, 02
Linker Info:5.12
Subsystem: Win32 GUI
PECompact 2.x -> Jeremy Collake

DNS Queries: 82.165.130.61 (Belsim.com)

Corresponding whois Record:

Server Type:	Apache/1.3.33 (Unix)
IP Address:	82.165.130.61
IP Location	United States - Schlund + Partner Ag
Response Code:	200
Blacklist Status:	Clear
Domain Status:	Registered And Active Website
registrant-firstname:	Dennis
registrant-lastname:	Chen
registrant-organization:	Dennis Chen, PL
registrant-street1:	2719 S. Maguire Road
registrant-pcode:	34761
registrant-state:	FL
registrant-city:	Ocoee
registrant-ccode:	US
registrant-phone:	+40.76545556
registrant-fax:	+40.76545502

Bot 11

MD5: 2aa59ba4251795deda72738d1c67be7c

Period: 10/16/2007 – 10/29/2007

AV Description

Symantec: W32.IRCbot
Also, vulnerabilities were found in SMB by Microsoft: MS05-011, MS05-027.
Server Message Block (SMB) is an application-level network protocol mainly applied to shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network. It also provides an authenticated Inter-process communication mechanism. It is mainly used by Microsoft Windows equipped computers, where it's known simply as "Microsoft Windows Network".

Bot System Interaction

Tried to connect to **67.43.236.98**

File Report

2 files were added

C:\WINDOWS\system32\csrs.exe
C:\WINDOWS\Prefetch\CSRS.EXE-368A04E2.pf

DLL Report

11 DLLs were loaded. A list of DLLs is as follows:
C:\WINDOWS\system32\browselc.dll was loaded into memory.

> Shell Browser UI Library: is component of the file that provides functions for the shell browser interface in Windows.

C:\WINDOWS\system32\usbui.dll was loaded into memory.

> USB UI Dll: a module that contains application programming interface (API) functions to manage the Universal Serial Bus User Interface.

C:\WINDOWS\system32\MLANG.dll was loaded into memory.

> Multi Language Support DLL: a module that provides multi-language support functions. It contains functions for translation of current Internet character sets to Unicode and back.

C:\WINDOWS\system32\wzcdlg.dll was loaded into memory.

Wireless Zero Configuration Service component: a module relating to the Wireless Zero Configuration Service which is a part of the Microsoft Windows Operating System

C:\WINDOWS\system32\Cabinet.dll was loaded into memory.

Microsoft Cabinet File API: a module that contains functions used by a cabinet file API. Required for essential applications to work properly.

C:\WINDOWS\system32\wininet.dll was loaded into memory.

Internet Extensions for Win32: is a module that contains Internet-related functions used by Windows applications. Note: wininet.dll is a process which the Troj/Zlob-AO trojan tries to disguise itself as under the true process name of %systemroot%\mscornet.exe.

C:\WINDOWS\System32\zipfldr.dll was loaded into memory.

Compressed (zipped) Folders: is module that handles compressed container.

C:\WINDOWS\system32\mpr.dll was loaded into memory.

Multiple Provider Router DLL: a module containing functions used to handle communication between the Windows operating system and the installed network providers.

C:\WINDOWS\system32\psapi.dll was loaded into memory.

Process Status Helper: a library file which provides support for process status.

C:\WINDOWS\System32\shdocvw.dll was loaded into memory.

Microsoft Shell Doc Object and Control Library: a library used by Windows applications to add basic file and networking operations.

C:\WINDOWS\system32\WINHTTP.dll was loaded into memory.

Windows HTTP Services: a component from the software Microsoft Windows Operating System version 5.2.0 by Microsoft Corporation

Services Report

None Reported

Registry Report

None Reported

Observed Traffic

```
Bot traffic
IP Address: 58.61.155.13  -->70.63.100.148
                12200 -->webcache8080
                12200 -->              8000
                12200 --> socks    1080
                12200 -->              3128
webcache        8080    -->      12200 [rst, ack]
                8000    -->      12200 [rst, ack]
socks   1080    -->      12200 [rst, ack]
                3128  -->        12200 [rst, ack]
```

```
IP Address: 70.62.75.63 --> 70.63.100.148
                    3904    -->      epmap [syn]
                    epmap -->        3904    [syn, ack]
                    3904    -->      epmap [fin, ack]
                    epmap -->        3904    [ack]
                    3904    -->      epmap [fin, ack]
                    epmap -->        3904    [ack]
```

Additional Information

The binary executable file appeared to be packed. Relevant packer information is as follows.

```
Packer Information
Entry Point:00003FCC
File Offset:00003FCC
First Bytes:55,8B,EC,B9
Linker Info:2.25
Subsystem:Win32 GUI
Borland Delphi 6.0-7.0
```

Also, there is no information about the maker of the added file **C:\WINDOWS\system32\csrs.exe**. The file is not a Windows core file. The program is not visible. File csrs.exe is located in the Windows folder, but it is not a Windows core file. csrs.exe is able to hide itself, monitor applications, record inputs. Therefore the technical security rating is *66% dangerous*.
DNS Queries: 69.14.32.48:5689 (petrosftp.boldlygoingnowhere.org) and 63.208.196.104 (wosten.shacknet.nu)
Corresponding whois Record:

69.14.32.48:5689

```
OrgName:      WideOpenWest LLC
OrgID:        WOPW
Address:      1674 Frontenac Rd
City:         Naperville
StateProv:    IL
PostalCode:   60563
Country:      US

NetRange:     69.14.0.0 - 69.14.255.255
CIDR:         69.14.0.0/16
NetName:      WIDEOPENWEST
NetHandle:    NET-69-14-0-0-1
Parent:       NET-69-0-0-0-0
NetType:      Direct Allocation
NameServer:   DNS1.WIDEOPENWEST.COM
NameServer:   DNS2.WIDEOPENWEST.COM
Comment:
```

RegDate:	2002-12-09
Updated:	2003-05-13

63.208.196.104
Technical Contact:
Melvin Foong
Starwing.Nu
12 Jalan USJ 2/4D
Subang Jaya
Selangor 47600
MY
Phone: +60 (03) 7319905 (voice)

58.61.155.13
Hostname:No hostname found
Domain:Unknown
Current reputation: Unverified
Registry:APNI
City:Guangzhou
Region:Guangdong
Country:China

70.62.75.63
Hostname:rrcs-70-62-753.midsouth.biz.rr.com
Domain:rr.com
Current reputation: Malicious
First seen:2007-06-07
Last seen:2007-10-27
Registry:RIPE
City:Wilmington
Region:North Carolina
Country:United States

67.43.236.98
Hostname:No hostname found
Domain:Unknown
Current reputation: Malicious
Registry:RIPE
City:Lachine
Region:Quebec
Country:Canada

In addition, there were several suspicious network connections and domain names:
(1) Network Connections:
connection between 70.63.100.148:123 and *:* was opened.
Network Time Protocol. Provides time synch between computers and

network systems

connection between 70.63.100.148:137 and *:* was opened.

Msinitnetbios-ns. for browsing, logon sequence, pass-thru validations, printing support, trust support, WinNT Secure Channel, and WINS registration.Security Concerns: Key target in auth & DOS attacks.

connection between 70.63.100.148:1900 and *:* was opened.

Ssdp. This UDP port is opened and used by Universal Plug N' Play (UPnP) devices to receive broadcasted messages from other UPnP devices. UPnP devices broadcast subnet-wide messages to simultaneously reach all other UPnP devices.

connection between 70.63.100.148:138 and *:* was opened.

NETBIOS Datagram Service. Similar to port 137.

connection between 70.63.100.148:139 and 0.0.0.0:0 was opened.

NetBIOS services used for directory replication, event viewer, file sharing, logon sequence, pass-thru validation, performance monitoring, printing, registry editor, server manager, trusts, user manager, WinNT Diagnostics, and WinNT Secure Channel.

(2) Domain names:

Japan.youngpeyatech.info
Teek.ihshsd8.com
Japan.youngpeyatech.info
Preek.oihduhdd.net
Fuck.urpal43sourpalhuh.com
Teek.ihshsd8.com
Dong.nagitiriheiwu.net
Done.blacktiehsbdcs.com
Done.blacktiehsbdcs.com
Japan.youngpeyatech.info
Italian.swiifatecihno.com

Bot 12

MD5:0e45505585dd628c004166c56e94504b

Period: 11/06/2007 – 11/12/2007

AV Description

Symantec: Trojan.SdBot-6699

Bot System Interaction

Tried to connect to **63.173.172.98**

File Report

2 files were added
C:\WINDOWS\system32\lssas.exe was added
    lssas.exe isa process which is registered as the
    W32.AGOBOT.RL Trojan. This Trojan allows attackers to access your computer from remote locations, stealing passwords, Internet banking and personal data. This process is a security risk and should be removed from your system.
C:\WINDOWS\Prefetch\LSSAS.EXE-0670E652.pf was added

DLL Report

C:\WINDOWS\system32\user32.dll was loaded into memory.
    Windows User API Client DLL: a module that contains Windows API functions related the Windows user interface (Window handling, basic UI functions, and so forth).
C:\WINDOWS\system32\wininet.dll was loaded into memory.
    Internet Extensions for Win32: is a module that contains Internet-related functions used by Windows applications. Note: wininet.dll is a process which the Troj/Zlob-AO trojan tries to disguise itself as under the true process name of %systemroot%\mscornet.exe.
C:\WINDOWS\system32\pstorec.dll was loaded into memory.
    Protected Storage COM interfaces
C:\WINDOWS\system32\psapi.dll was loaded into memory.
    Process Status Helper: a library file which provides support for process status.
C:\WINDOWS\system32\shdocvw.dll was loaded into memory.
    Microsoft Shell Doc Object and Control Library: a library used by Windows applications to add basic file and networking operations.

C:\WINDOWS\system32\mpr.dll was loaded into memory.

Multiple Provider Router DLL: a module containing functions used to handle communication between the Windows operating system and the installed network providers.

Services Report

None Reported

Registry Report

None Reported

Observed Traffic

The following IRC traffic was observed:

```
IRC Bot Traffic (24.123.184.62→63.173.172.98)
NICK FTTT820283635
USER vnjudhtnn 0 0 :FTTT820283635
PING :365AFB2A
PONG :365AFB2A
JOIN #dddpass
:irc.foonet.com 001 FTTT820283635 :
:FTTT820283635!vnjudhtnn@rrcs-24-123-184-62.se.biz.rr.com
JOIN :#badbotbad
:irc.foonet.com 332 FTTT820283635 #badbotbad :.remove
:irc.foonet.com 333 FTTT820283635 #badbotbadjoeblow 1193841701
:irc.foonet.com 353 FTTT820283635 = #badbotbad :FTTT820283635 @joeblow
:irc.foonet.com 366 FTTT820283635 #badbotbad :End of /NAMES list.
USERHOST FTTT820283635
MODE FTTT820283635 +x+i
JOIN #dddpass
:FTTT820283635!vnjudhtnn@rrcs-24-123-184-62.se.biz.rr.com
JOIN :#dd
:irc.foonet.com 353 FTTT820283635 = #dd :FTTT820283635
:irc.foonet.com 366 FTTT820283635 #dd :End of /NAMES list.
:irc.foonet.com 302 FTTT820283635 :FTTT820283635=+vnjudhtnn@rrcs-24-123-184-
62.se.biz.rr.com
:irc.foonet.com NOTICE FTTT820283635 :Setting/removing of usermode(s) 'xpqTds'
has been disabled.
:FTTT820283635 MODE FTTT820283635 :+i
PING :irc.foonet.com
PONG :irc.foonet.com
```

```
PING :irc.foonet.com
PONG :irc.foonet.com
```

Additional Information

The binary executable file appeared to be packed. Relevant packer information is as follows.

```
Packer Information
ASProtect 2.1x SKE ->AlexeySolodovnikov [Overlay]
Entrypoint: 00001000
File Offset: 00000400
First Bytes: 68, 01, 00, 48
Linker Info: 5.16
Subsystem: Win32 GUI
```

DNS Queries**:** 63.173.172.98

Corresponding whois record:

```
Registry:Unknown
City:Sana
Region:no region
Country:Yemen
```

Bot 13

MD5: e831bf8201d251bc496402921dfb17f1

Period: 11/26/2007 – 12/03/2007

AV Description

Symantec: Trojan.SdBot-4953

Bot System Interaction

Connected to **207.96.179.121**

File Report

2 files were added
C:\WINDOWS\system32\agldoc32.com-up.txt C:\WINDOWS\system32\agldoc32.com

DLL Report

8 DLLs were loaded. A list of DLLs is as follows:
C:\WINDOWS\system32\oleaut32.dll was loaded into memory.
    Microsoft OLE DLL: a library which contains core OLE functions
C:\WINDOWS\system32\odbc32.dll was loaded into memory.
    Microsoft Data Access – ODBC: contains functions for the ODBC database query standard.
C:\WINDOWS\system32\icmp.dll was loaded into memory.
    Windows ICMP API: a module used by Windows 2000
C:\WINDOWS\system32\dnsapi.dll was loaded into memory.
    DNS Client API DLL: a module that contains functions used by the DNS Client API
C:\WINDOWS\system32\WS2_32.DLL was loaded into memory.
    WinSock 2.0 32bit: File that contains the Windows Sockets API used by most Internet and network applications to handle network connections.
C:\WINDOWS\system32\wininet.dll was loaded into memory.
    Internet Extensions for Win32: is a module that contains Internet-related functions used by Windows applications.
C:\WINDOWS\system32\shdocvw.dll was loaded into memory.
    Microsoft Shell Doc Object and Control Library: library used by Windows applications to add basic file and networking operations.
C:\WINDOWS\system32\agldoc32.com was loaded into memory.
    Rogue DLL: no information was found about this file name

Services Report

None Reported

Registry Report

The following entry was added: …software\Microsoft\Windows\CurrentVersion\Run

Observed Traffic

The following IRC traffic was observed:

```
IP Address: 207.96.179.121
Port: 51115
NICK Q-763598738
USER mvfygniknse 0 0 :Q-763598738
PING :979F42FC
PONG :979F42FC
JOIN #dc dcpass
:irc.foonet.com 001 Q-763598738 :
:Q-763598738!mvfygnikns@rrcs-70-63-100-149.midsouth.biz.rr.com JOIN :#badbotbad
:irc.foonet.com 332 Q-763598738 #badbotbad :.remove
:irc.foonet.com 333 Q-763598738 #badbotbadjoeblow 1195670921
:irc.foonet.com 353 Q-763598738 = #badbotbad :Q-763598738 @joeblow
:irc.foonet.com 366 Q-763598738 #badbotbad :End of /NAMES list.

IP Address: 207.96.179.121
Port: 51115
USERHOST Q-763598738
MODE Q-763598738 -x+i
JOIN #dc dcpass
:Q-763598738!mvfygnikns@rrcs-70-63-100-149.midsouth.biz.rr.com JOIN :#dc
:irc.foonet.com 353 Q-763598738 = #dc :Q-763598738
:irc.foonet.com 366 Q-763598738 #dc :End of /NAMES list.
:irc.foonet.com 302 Q-763598738 :Q-763598738=+mvfygnikns@rrcs-70-63-100-149.midsouth.biz.rr.com
:irc.foonet.com NOTICE Q-763598738 :Setting/removing of usermode(s) 'xpqTds' has been disabled.
:Q-763598738 MODE Q-763598738 :+i
PING :irc.foonet.com
PONG :irc.foonet.com
```

Additional Information

The binary executable file appeared to be packed. Relevant packer information is as follows.

```
Packer Information
Entry Point: 0010CB23
```

```
EP Section: 3
File Offset: 0001E123
First bytes: E8, 00, 00, 00
Linker Info: 6.0
Subsystem: Win32 GUI
Nothing Found (packer not recognized)
```

Also, we were able to retrieve the system snapshot after the binary was installed:

```
Agldoc32 Process Information (Post Installation)
Process ID:  1956
        Owner:  DELLPC\Administrator
        C:      File  (RW-)   C:\WINDOWS\system32
        734: Section    \BaseNamedObjects\C:_Documents and
                        Settings_Administrator_Local
                        Settings_History_History.IE5_index.dat_32768
        738: File  (RW-)   C:\Documents and
                        Settings\Administrator\Local
                        Settings\History\History.IE5\index.dat
        740: Section    \BaseNamedObjects\C:_Documents and
                        Settings_Administrator_Cookies_index.dat_32768
        744: File  (RW-)   C:\Documents and
                        Settings\Administrator\Cookies\index.dat
        750: File  (RW-)
                C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
                Controls_6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
        754: Section      \BaseNamedObjects\C:_Documents and
                        Settings_Administrator_LocalSettings_Temporary Internet
                        Files_Content.IE5_index.dat_147456
        758: File  (RW-)   C:\Documents and
                        Settings\Administrator\Local
                        Settings\Temporary Internet Files\Content.IE5\index.dat
        784: File  (RW-)
                        C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Commo
                        n-Controls_6595b64144ccf1df_6.0.2600.2982_x-ww_ac3f9c03
        7CC: File  (R--)   C:\WINDOWS\system32\agldoc32.com-up.txt
        * A thread of this file is also found in the csrss.exe process
```

```
Agldoc32 Process Information (Post Restart)
Process ID:  256
        Owner:  DELLPC\Administrator
        4: KeyedEvent\KernelObjects\CritSecOutOfMemoryEvent
        8: Directory            \KnownDlls
        C: File  (RW-)          C:\Documents and Settings\Administrator
        10: Section
        14: Directory     \Windows
        18: Port
```

```
1C: Key           HKLM
20: Event
24: WindowStation \Windows\WindowStations\WinSta0
28: Desktop       \Default
2C: WindowStation \Windows\WindowStations\WinSta0
30: File  (RW-)   C:\WINDOWS\system32
34: File  (R--)
38: File  (R--)   C:\WINDOWS\system32\agldoc32.com-up.txt
* A thread of this file is also found in the csrss.exe process
```

The identified text file included the following information.

C:\WINDOWS\system32\agldoc32.com-up.txt
"**windows error** : An attempt was made to move the file pointer before the beginning of the file at
D:\Projects\My.SRC\Teggo\MoleBox\molebox2\bootup\boxmanager.cpp(283)"

DNS Queries: 207.96.179.121

Corresponding whois Record:

IP Location	Canada Joliette Communications Inter-monde
Resolve Host	media.intermonde.net
OrgName	Videotron Telecom Ltee
Address	2155, boul Pie-IX
StateProv	QC
Country	CA
Phone	31 10 710 4444