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

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.