BITS

FINANCIAL SERVICES
ROUNDTABLE

MALWARE RISKS AND MITIGATION REPORT

June 2011

BITS
A DIVISION OF THE FINANCIAL SERVICES ROUNDTABLE
1001 PENNSYLVANIA AVENUE NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
202-289-4322

WWW.BITS.ORG

Table of Contents

1. Executive Summary

Malware is an abbreviation of the words malicious and software. The term refers to software that is deployed with malicious intent. Malware is easy to deploy remotely, and tracking the source of malware is hard. This combination has enabled commercial malware providers to supply sophisticated black markets for both malware and the information that it collects. Demand for sophisticated malware is created primarily by organized crime syndicates and state-sponsored espionage agents. The financial services industry is a primary target for malware-enabled cyber attacks because financial institutions (FIs) operate software that tracks ownership of monetary assets. Cybercriminals also directly target FI customers and business partners using malware-enabled attacks. This paper is intended to assist financial institutions by promoting awareness and understanding of the risks and the mitigation activities associated with the use of malware in the financial industry.

This report is composed of six (6) sections and four (4) appendices, beginning with this executive summary:

- Section 2 provides a brief historical overview of malware. It demonstrates that malware has evolved side-by-side with software technology and that this co-evolution may be expected to continue. It provides examples of how malware is deployed in critical infrastructure.
- Section 3 describes the criminal organizational structure that supports malware creation and distribution. It highlights negative consequences for the financial industry that result from the existence of this criminal infrastructure, which includes its expanded use for the purposes of nation-state espionage and sabotage.
- Section 4 lists cyber attack methods that are known to have utilized malware to damage financial services.
- Section 5 describes ways in which the financial sector, in collaboration with technology and business partners, may thwart malware-enabled cyber attacks.

2. Malware Evolution

Software-enabled crime is not a new concept [1]. Computer-enabled fraud and service theft evolved in parallel with the information technology that enabled it. Since the advent of mainframe-based automated bank account systems, FIs have been victims of malware-based cyber attacks. Criminals altered software to transfer other people's money to accounts they controlled, and emptied the accounts anonymously. As computers were shared on networks, these services experienced service theft, wherein criminals altered system software to hide reconnaissance activities which enabled theft of both valuable services and valuable information [2].

This co-evolution of technology services and cybercrime may have created some confusion in the general population, for whom attacks on technology do not seem to be as significant as attacks on physical assets. Those not familiar with the emerging technology itself find it difficult to understand the implications of software compromise. General confusion over cybercrime objectives is exacerbated by the element of opportunism in some types of cybercrime, wherein attackers do not select specific victims, but simply let rogue software loose to find its own targets. This type of cybercrime appears to some segments of the public as bad luck for the victim rather than as a direct result of adversarial intent.

Nevertheless, even opportunistic cybercriminals select their targets, if only by selecting the operating system platform on which malware may be processed. Where the platform is the latest version of an emerging technology, the selected victim class may be assumed to be those financially able to afford that new technology. Another selection made by cybercriminals is the specification of data that malware processes. Where data concerning credit card numbers is sought, the target victim class includes all credit card holders and associated institutions. Where the data sought is bank account numbers, all financial firms are targets. The attraction of cybercrime lies in the high return on investment, low-to-no-risk operating environments, and proliferation of vulnerable computing resources. The ubiquitous connectedness provided by the Internet has allowed for multiple elements of the criminal community to operate in tandem to pursue profit driven crime as well as other malicious activities, using malware.

To the casual observer, headlines about cyber attacks may seem unrelated. Attacks are scattered across geography and technology. They involve different companies and nationalities. As recently as five years ago, security standards publications identified malware and phishing attacks as separate threats [3]. However, today security analysts agree that various types of malware are used in conjunction [4]. Cooperation and collaboration among cybercriminals have created crime patterns that evolve in concert with emerging technology, and all users of emerging technology are victims. There is also evidence that cybercriminals operate in geopolitically-identifiable groups. As one analyst put it, "the phrase 'campaign' is more appropriate than 'adversary' [5]."

Malware is typically used to steal information that can be readily monetized, such as login credentials, credit card and bank account numbers, and intellectual property such as computer software, financial algorithms, and trade secrets. Although many cybercriminal groups are trafficking in commodities shared by multiple industry sectors, such as credit card numbers, there are some situations wherein a single company is obviously the target of a single adversary, whether it be an organized crime syndicate, nation-state, or a single operative. For example, the work of a single nation-state adversary was evident to Google upon analysis of its 2009 cyber attack [6]. The extent to which any given attack lands on one set of companies or customers rather than another depends on a variety of factors. These factors are explained in Section 4 of this report.

Just as information technology software tools and techniques have become more proficient, more effective, and more economical over time, malware crime patterns have become more finely tuned.

Malware creation and distribution channels are described in detail in Section 3. The remainder of this section describes in general how malware works and how it accomplishes crime.

2.1 Malware Categories

Malware may take as many forms as software. It may be deployed on desktops, servers, mobile phones, printers, and programmable electronic circuits. Sophisticated attacks have confirmed data can be stolen through well written malware residing only in system memory without leaving any footprint in the form of persistent data. Malware has been known to disable information security protection mechanisms such as desktop firewalls and anti-virus programs. Some even have the ability to subvert authentication, authorization, and audit functions. It has configured initialization files to maintain persistence even after an infected system is rebooted. Upon execution, sophisticated malware may self-replicate and/or lie dormant until summoned via its command features to extract data or erase files.

A single piece of malware is generally described by four attributes of its operation [7]:

Propagation:	The mechanism that enables malware to be distributed to multiple systems
Infection:	The installation routine used by the malware, as well as its ability to remain installed despite disinfection attempts
Self-Defense:	The method used to conceal its presence and resist analysis, these techniques may also be called *anti-reversing capabilities*
Capabilities:	Software functionality available to malware operator

Table 1 lists some examples of malware in the context of this taxonomy. It is not meant to be complete, but to provide an appreciation for the variety of software types and capabilities that fall into the general category of malware.

Table 1: Malware Categories

	Propagation	**Infection**	**Self-Defense**	**Capabilities**
Keylogger	Infected websites and/or USB or other media	Vulnerable browsers or unpatched OS or application	Replace IO device drivers or APIs	Collect user keystrokes including credentials
Rootkit	Infected websites and/or installs on servers by hackers or insiders	Exploited trusted admin access, vulnerable browsers, or unpatched OS or application	Replacing OS kernel-level API routines	Collect data and impersonate user activity for entire machine and its interfaces

Table 1: Malware Categories				
	Propagation	**Infection**	**Self-Defense**	**Capabilities**
Flaw Exploits	Execution of unexpected commands to flawed software by remote hackers	Vulnerable software-to-database and command execution interfaces	Impersonation of authorized users	Download or upload data from data repositories between target and malware operator site
Bot (the same bot on multiple machines from the same malware operator is called a botnet)	Bots are generally delivered via infected websites, or links to malicious websites embedded in phishing email.	User may voluntarily install individual bots based on deceptive messages in email or web instruction, or via browser/OS vulnerabilities.	Bot updates security patches and anti-virus on machine to ensure stable operation and keep other bots out. Lays dormant until activated.	When activated by botnet operator, the operator may direct bot to execute a variety of standard or custom functions.
Denial of Service (host or network)	IP packet delivery	Internet protocols that automate packet processing	Simultaneously attack from multiple sources	Consume computing resources on targets

Note that Table 1 refers only to single pieces of software and that there is no hierarchy in malware classification. However, alluded to in the description of a bot is the fact that a typical cybercrime will require multiple different types of software acting in coordination in order to achieve the full crime capability. For example, a criminal may use email spamming software (a form of flaw exploit) to trick a user into downloading a keylogger from an infected website. The criminal would then have to host a site for the keylogger to deliver the stolen credentials. The criminal would presumably use software to read and analyze the credentials, and then perhaps use vulnerability scanning software to see which websites identified by them have flawed software. The criminal may then use the user name and password to execute flaw exploits against the website. The steps a criminal must follow in order to accomplish a typical cybercrime are outlined in Figure 1 [5]. Activities included in each step are:

Reconnaissance: Criminal surveys the target to identify points of vulnerability, an attack-planning phase.

Assembly: Criminal creates, customizes, or otherwise obtains malware to satisfy attack requirements.

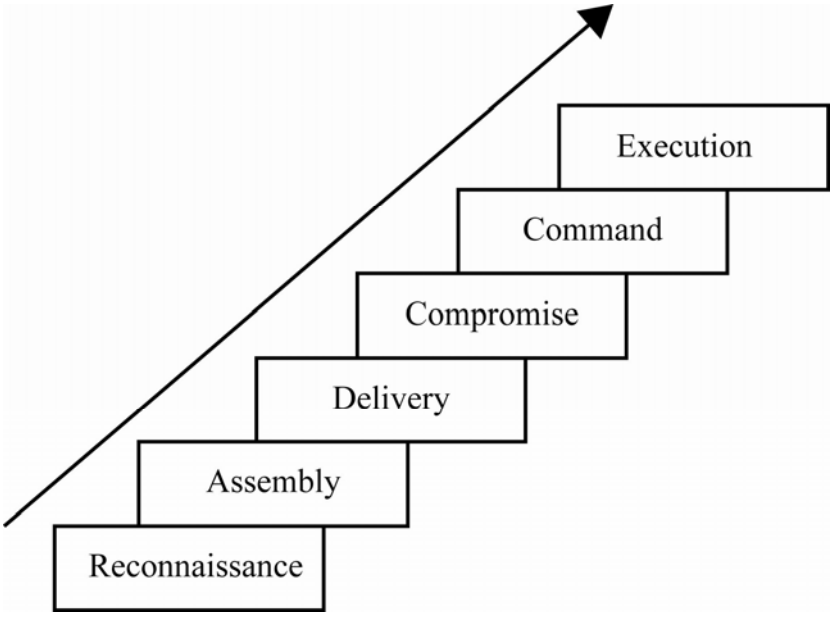
Delivery: Malware propagation occurs.

Compromise: Malware infection occurs.

Command: Malware capabilities are unleashed.

Execution: Malware delivers data to malware operator (exfiltration) or otherwise accomplishes attack objective.

Figure 1: Steps for Conducting Crime with Malware



Although there are a wide variety of words and phrases that the media uses to refer to malware, they all have their roots in the execution paths illustrated in Table 1 and Figure 1. The specialized terminology tends to refer to the type of crime perpetrated using the software rather than the technical description of the attack. For example:

Malvertising: The practice of paying for web advertisements and using them to cause malware propagation

Ransomware: The use of malware to block access to computers or data until a payment is made, also continues to be used for extortion purposes

Rogueware: Malware that is written to look and act like legitimate packages, in order to trick victims into downloading and installing it

Scareware: Malware that is written to look and act like legitimate security anti-virus packages, in order to trick victims into buying worthless software to fix nonexistent virus or spyware problems, scareware may be a form of rogueware

Spearphishing: Phishing attacks directed at wealthy or otherwise singularly attractive targets with specific knowledge, capability or expertise

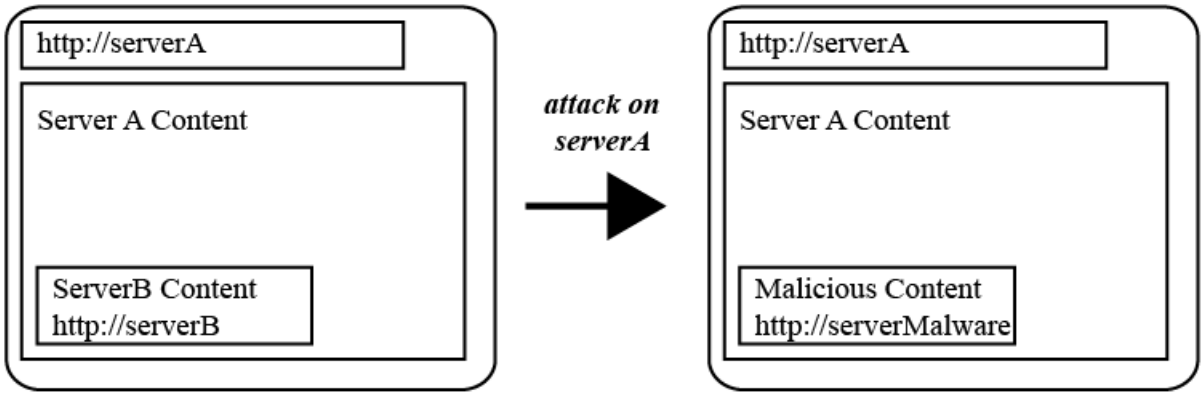
Spyware: The use of malware to observe any user activity, including keystrokes and screenshots, and network connections, typically used to transfer passwords and credit card numbers to the malware operator

2.2 Malware Example

As described in Section 2.1, malware usage is enabled by emerging technology, and evolves with it. For example, the advent of iFrame technology in web services has enabled a specific brand of malware. The technology allows a URL to be placed in a web page hosted on server A that displays content from server B. The user accessing server A does not see the call to server B, as server B's content appears displayed in the page rendered by server A. There are a variety of legitimate reasons why a legitimate website may want to display content from multiple servers simultaneously. There may be complex specialized algorithms required to display numerical data that is generated in real-time, and so, beyond the CPU capacity of a single web server. There may be business relationships that require display of partner logos or advertisements from business partner servers. For whatever reason, the legitimate iFrame feature exists.

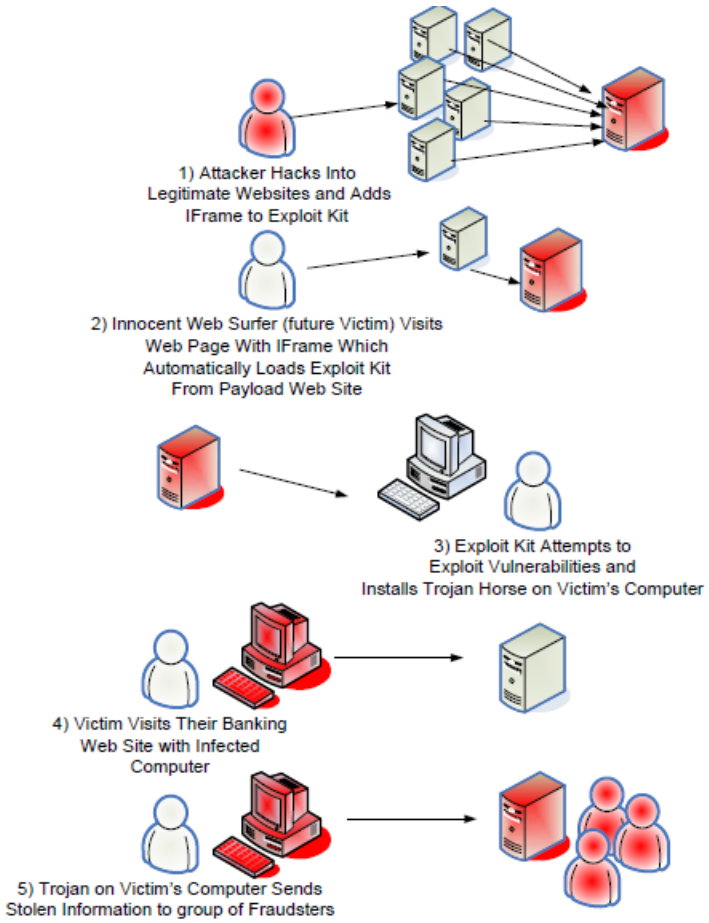
The iFrame feature by itself does not enable malware. Criminals take advantage of the feature by exploiting web server vulnerabilities and inserting their own servers in replacement, or in addition to a legitimately placed server B (for a full explanation of this vulnerability, see [8]). Figure 2 illustrates how the server is modified to set up for a subsequent attack on a web server user. There also are vulnerabilities in browsers with which users visit sites that have iFrames. The combination of server and browser vulnerabilities enable malware criminals to use iFrames for malware propagation and infection. The iFrame-enabled webserver, the code it links to on the malware host site, and the code that is downloaded to the user when the user accesses the iFrame are different pieces of malware. They are used in combination to infect the user. Only after the infection takes place for the last of these pieces, the malware on the end user target, is it fully enabled with self defense and functional capabilities required to harvest data.

Figure 2: Example iFrame Attack Setup



As described, successful crime execution using malware is a multi-step process. Figure 3 illustrates these steps using the iFrame attack as an example.

Figure 3: Example Malware Attack Scenario [8]



The actual malware installed by a propagation and infection process, such as that illustrated in Figure 3, will vary. An archetypal example is Zeus [9]. On an infected system, Zeus' self defense mechanisms include evasion of system-monitoring tools by modifying system Application Programming Interfaces (APIs). This enables it to hide Zeus' configuration files on disk and inspect incoming and outgoing network traffic. Zeus also disables the Windows firewall. Post-infection, Zeus capabilities include, but are not limited to:

- exporting private key certificates
- exporting protected storage passwords
- monitoring for file transfer and email passwords (FTP and POP3)
- logging keystrokes
- taking screenshots
- HTML injection
- form grabbing for transaction authentication numbers (TAN)

- automatic transaction hijacking (ATH)
- transfer of encrypted stolen credentials to malware operators in near real time (using Jabber)
- routing connections through the infected machine
- attacking other systems on the local network

2.3 Polymorphic Malware

Remediation of modern malware is becoming increasingly more difficult due to several factors. There are significantly more varieties of malware being found in the wild that exploit zero-day vulnerabilities. "Zero-day" modifies the word vulnerability to mean that the vulnerability is not known to potential victims, and so victims have had no days to prepare for it. Malware has also now been designed with polymorphic capabilities. Polymorphic malware changes certain characteristics of itself upon each instance or infection. This change can be in the form of a non-functional code change. This technique circumvents signature-based detection mechanisms because these typically use a hash algorithm to produce a unique signature from a file containing malware, so any change to the file will change its signature. Polymorphic malware can also change its own filename on each infection, and this also makes detection more difficult by traditional means.

3. Malware Supply and Demand

The root cause of malware is the black market for stolen information. Data thieves can sell their spoils in a variety of forums [10]. Examples of prices obtained for various types of stolen information are listed in Table 2 [11].

Table 2: Example Prices for Stolen Data	
CCV	$3.25
OS administrative login	$2.50
FTP exploit	$6.00
Full identity information	$5.00
Rich bank account credentials	$750.00
US passport information	$800.00
Router credentials	$12.50

In any dynamic marketplace, the prices claimed for a commodity will fluctuate with supply and demand. In any technology marketplace, prices will also fluctuate with the utility of the commodity, given changes in technology landscape. The dollars commanded for stolen commodities listed in Table 2 motivated the creation of secondary malware markets that produce software tools that make malware increasingly effective at enabling information theft. Individuals use software generally to automate tasks that are both tedious and resource intensive, and malware perpetrators are no exception. Automating malware delivery and data harvesting tasks reduces operating costs and

allows malicious perpetrators to obscure their activities. Malware delivery and operations systems have become increasingly modular, and these modules have themselves become a commodity. Prices obtained for modular software information theft enablers are listed in Table 3. The prices were observed in the same timeframe as the prices that were commanded for stolen information in Table 2. It is obvious that information on financial accounts may be sold for multiples above the cost to purchase the tools that enable the theft.

Table 3: Example Prices for Malware and Crimeware [11]	
Theft Enabling Commodity	**Price**
Keystroke logger	$25 on average
Botnets	$100 to $200 per 1,000 infections, depending on location
Spamming email service	$.01 per 1,000 emails, reliability of more than 85% delivered
Shop admins (Credit Card databases)	$100 to $300
Credit Card numbers without CCV2	$1 to $3
Credit Card numbers with CCV2	$1.50 to $10.00, depending on the country
Socks accounts	$5 to $40/month
Sniffer dumps	$50 to $100/month
Western Union exploits	$300 to $1,000
Remote desktops	$5 to $8
Scam letters	$3 to $5

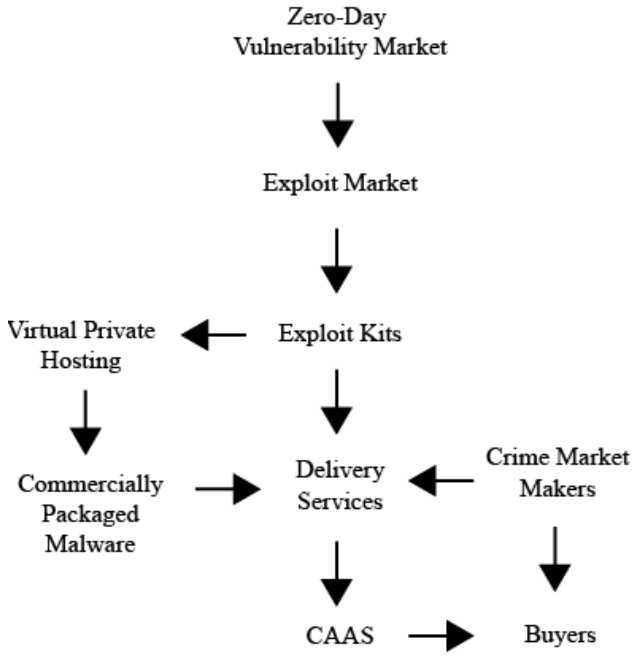
When such malware software support systems are discovered to exist, the software is referred to as *crimeware* [12]. Continuing the Zeus malware example from Section 2, a good example of crimeware is the Zeus toolkit. Zeus malware was introduced in 2006, and its corresponding crimeware followed in 2007. Zeus' crimeware takes advantage of its modular design, so attackers can configure and deploy new functionality very quickly. A user-friendly graphical interface allows an attacker to select the capabilities to be incorporated in a "release" as well as to select a personal encryption key for harvested data. Over 5,000 releases of the Zeus software have been created using Zeus crimeware [13]. Although several Zeus users have been identified and charged with cybercrimes, the Zeus crimeware authors remain at large.

3.1 The Malware Industry

Malware development and distribution is highly organized and controlled by criminal groups that have formalized and implemented business models to automate cybercrime. Just as the software industry has spawned a business model in reselling, installing, and maintaining legitimate code, the malware industry has spawned distribution and support networks to assist criminals in successful

malware usage. Developers of crimeware profit from the sale or lease of the malware to third parties who then use it to perpetrate identity theft and account fraud. Figure 4 illustrates the interaction between components in a typical crimeware business model. Individual groups of criminals coordinate their efforts, and the product is Crimeware as a Service (CAAS).

Figure 4: Malware Industry Process

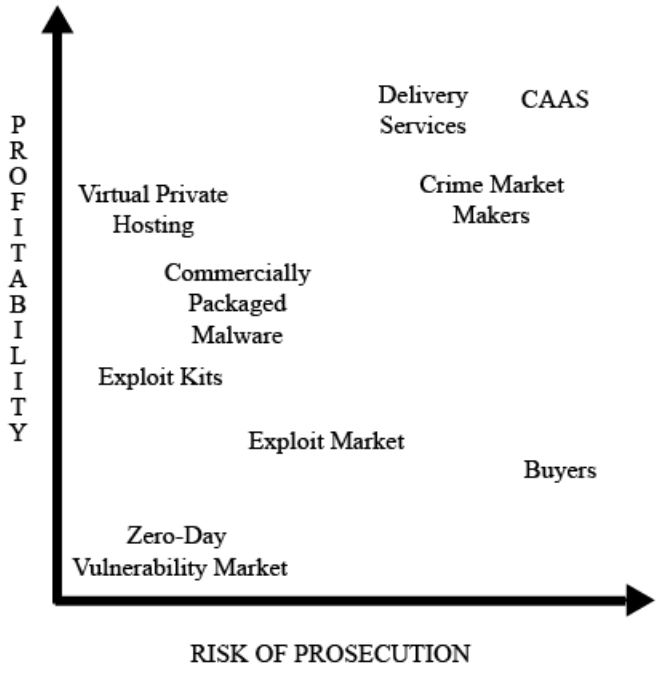


The process depicted in Figure 4 leads with software vulnerabilities being sought by criminals in a systematic way. The figure begins with "zero-day" vulnerabilities, because these are more valuable to malware creators because potential victims are unsuspecting. These vulnerabilities are sold to criminals who engineer malware to exploit the vulnerability, and aggregate multiple malware vulnerability exploits into kits whose components can be systematically installed as in the iFrame example in Section 2.3. Because many vulnerabilities exist in unpatched systems long after they have been announced, exploit kits may include combinations of zero-day and older attacks. The kits are configured to send harvested data to private hosting services, and this configuration may be customized for a given buyer. Crimeware market makers contact potential customers via email and chat, agree on prices and sell not just software, but crimeware services. They engage malware delivery services to operate the malware on behalf of buyers, who pay the market makers via anonymous ecommerce payment systems.

Crimeware operation is blatantly illegal, yet individual risk of criminal prosecution is minimized by the overall business model. Each malware profit center has a level of exposure corresponding only to its role in the overall marketplace. For example, in academic circles, the study of vulnerabilities is common. Academics write papers on engineering and reverse engineering of exploits, and this is not

considered criminal activity. The relative prosecution risk to profit ratio for each activity in Figure 4 is estimated in Figure 5.

Figure 5: Relative Risk to Profit for Participation in Crimeware Activity



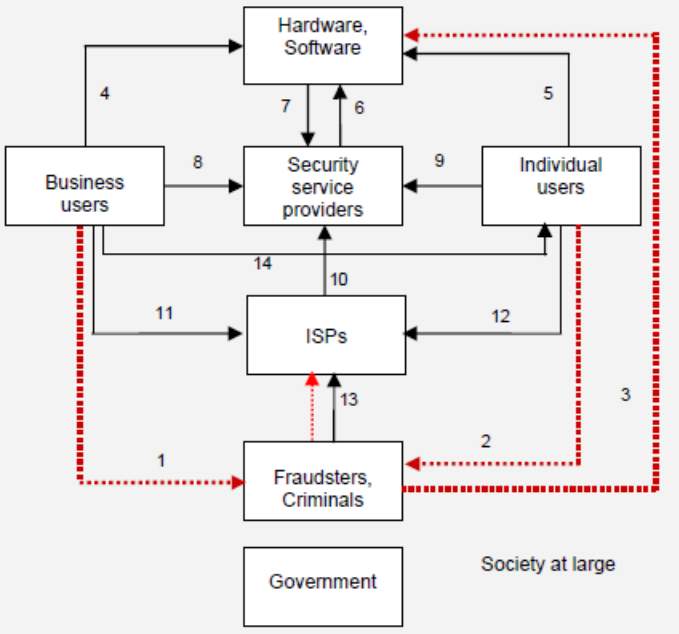
3.2 Malware Supply Chain

Earnings for malware development are time sensitive but are very low risk. During the lifecycle of malware, protections are developed to mitigate the risk. To remain competitive and profitable new malware must be released frequently. Security analysts are seeing dramatic increases in the number of malware specimens created and distributed. One report claims that a full third of all viruses that exist were created in 2010 [14]. The profit incentive driving these activities creates a persistent risk for financial institutions.

The supply chain in the malware industry encompasses more than just software. It is an elaborate collection of organizations, people, technologies, processes, services, and products. Financial services such as moneygrams, virtual credit cards, and online money transfer services allow anonymity between buyers and sellers. However, not all of the players in this black market are criminals. The marketing of malware, crimeware, and associated services and products can be found on both black market forums and legitimate sales channels. Crimeware operators will use legitimate online payment services to process purchases and then the payment details are used to facilitate fraudulent transactions. They will also use legitimate Internet Service Providers (ISP) to host databases of stolen data. Hence, another way to view the malware industry depicted in Figure 4 is to

follow the money. Figure 6 demonstrates the interaction between legal and illegal transaction flow in the malware market.

Figure 6: Malware Financial Flow [4]



In Figure 6, solid lines show legal financial flows and dotted lines show illegal financial flows. The lines are numbered with types of transactions included, and these are described as follows [4]:

1:	Extortion payments, click fraud, compensated costs of ID theft and phishing
2:	Uncompensated costs of ID theft and phishing, click through, stock price pump and dump schemes, email scams, and other forms of consumer fraud
3, 4, 5, 6:	Hardware purchases by criminals, corporate and individual users
7, 8, 9, 10:	Security service purchases by hardware manufacturers, corporate and individual users, ISPs
11, 12, 13:	ISP services purchased by corporate and individual users, criminals
14:	Payments to compensate consumers for damages from ID theft

The inclusion of legitimate business interests in the ecosystem of malware-enabled cybercrime sometimes makes crimeware and malware operators difficult to distinguish from Internet entrepreneurs.

3.3 Beyond Crime

In addition to its use for criminal purposes, malware also enables other malicious actors that pose risks for the financial services sector. The term Advanced Persistent Threat (APT) is now increasingly used to describe a category of malicious activities facing a growing number of government institutions and commercial organizations. As described in a recent Financial Services

Information Sharing and Analysis Center (FS-ISAC) report, "APT refers to an advanced, clandestine means to gain continuous, persistent intelligence on an individual, company or foreign nation state government or military [15]." The report shows there has been a history of APT attacks since 1986. Key risks posed by APT actors generally include efforts to access and exfiltrate data that contains sensitive and/or classified information. The information may be related to technology and operations, intellectual property, proprietary business processes, business strategy, and/or personal data pertaining to executives. APT activities include network mapping and software modification to gain and maintain remote access to a variety of systems within the target domain. Such sustained access, knowledge of networks and business processes allows perpetrators to lay groundwork for future disruptive activities. Increasingly, APT discussions also include the use of tools specifically designed to achieve disruptive effects such as Stuxnet, which is malware designed to attack Iran's nuclear power plants [16]. The possibility of attacks focused on data corruption in the future has also been identified. Key characteristics of APT activities include, but are not limited to:

- threat actors with clearly identified long-term objectives guiding their attacks
- structured, sustained intrusive activities to deploy, support and maintain exfiltration operations
- ability to conduct intelligence on individuals, organizations and processes that will prove to be valuable targets
- use of sophisticated software tools and techniques to conduct activities
- flexible and adaptable operations to avoid detection.

Public recognition of these activities has risen dramatically. Numerous reports exist related to on-going activities against governments and defense industries worldwide, specific activities focused on the US energy industry and the highly publicized attacks against Google, as part of Operation Aurora [17-19]. With regard to financial services, limited open source information exists regarding specific activities but the financial services sector is often identified in discussions and doctrinal writings about cyber warfare between nations [20].

The conduct of APT activities relies fundamentally on the use of malware to establish access, to maintain footholds within organizations and to exfiltrate sensitive data and/or conduct disruption of IT systems or networks. Directed efforts using spearphishing have been a principal approach of many of the operations against governments and the defense industry. Often, the payloads of spearphishing attacks include a range of malware targeted at the most common types of applications for enterprise users, particularly those in Microsoft Office and Adobe products. Often this malware uses well known code exploiting well known vulnerabilities, but APT activities also employ new and custom code not detectable by enterprise intrusion detection and anti-virus systems. APT actors are generally highly aware of the state of enterprise information security practices. They employ code and techniques not only to avoid detection but also frequently use malware to disable anti-virus, intrusion detection systems, and other security software on exploited computers, and even across broader portions of the enterprise. More significantly, APT actors may have a portfolio of capabilities at hand to ensure the ability to continue activities even when discovered. Malware

more unique to APT activities often includes redundant and diverse tools to conduct exfiltration of user credentials and sensitive data.

FIs must be cognizant of the growing risks posed by malware specifically designed to disrupt operations, particularly the operation of industrial control systems (ICS). The emergence of the Stuxnet worm in 2010 targeted at the Siemens ICS provides concrete evidence that cyberspace can have devastating effects on physical resources such as data center environment and power systems, electric grids, gas pipelines, water delivery systems, and manufacturing equipment [16]. While the original purpose of this malware appears to be targeted at the Siemens ICS utilized in nuclear programs in Iran, key features of the worm pose much larger concerns that should inform the financial services sector. The possibility of another actor capturing the code and repurposing it for other purposes such as disrupting power grids is a significant possibility. As a Department of Homeland Security official testified before a Senate committee, "What makes Stuxnet unique is that it uses a variety of previously seen individual cyber attack techniques, tactics, and procedures, automates them, and hides its presence so that the operator and the system have no reason to suspect that any malicious activity is occurring. The concern for the future of Stuxnet is that the underlying code could be adapted to target a broader range of control systems in any number of critical infrastructure sectors [21]." More generally, the financial services sector could be targeted by disruptive ICS malware specifically designed to exploit vulnerabilities in ICS applications used in this sector, specifically heating, ventilating, air-conditioning (HVAC) and power supply equipment used to monitor and control data centers.

The FS-ISAC has conducted a more detailed analysis of APT threats, risks and mitigations available to FS-ISAC members.

4. Malware in Financial Services

Malware is used by malicious parties, both inside and external to the organization, with different motivations. Examples of such motivations include financial gain, competitive advantage or, potentially, revenge for some perceived slight or adverse event. For example, according to the United States Computer Emergency Readiness Team (US-CERT), malware, as logic bombs, has been distributed by disaffected insiders to delete massive amounts of data. In one such case, malware "was designed to disrupt business operations [22]." In another case, a disgruntled systems administrator employed by a financial services firm caused more than $3 million in damage to the company's computer network, and was convicted of securities fraud for his failed plan to drive down the company's stock price upon activation of the logic bomb [23]. Cyber espionage, or theft of information to receive a competitive advantage, could be aimed at stealing information about a new technology product, uncovering strategic plans about a potential acquisition, or confidential data regarding litigation. A House Conference Report that accompanied the US Consolidated Appropriations Act of 2010 accurately observed "Cyber-based attacks and intrusions upon U.S. computer networks . . . result in substantial loss of critical intelligence by U.S. government,

academia, military, industry, financial and other domains [24]."

It is evident from past and ongoing cybercrime investigations that the financial industry hosts a good deal of malware. The US Secret Service (USSS) is the primary investigation resource for the US Department of Treasury. For the past two years, USSS shared their cybercrime case reports with the Verizon Incident Response team so they could be included in a collaborative effort to establish cybercrime metrics [25, 26]. The resulting report contains details on confirmed security breaches within firms that are either Verizon clients or in the investigative jurisdiction of the Secret Service (141 Verizon cases and 257 USSS cases in 2009, 94 Verizon cases and 661 USSS cases in 2010). Financial services firms were the primary targets in 33% of 2009 and 22% of 2010 cases, making them the most targeted sector in 2009, though in 2010 they were surpassed by hospitality and retail. However, hospitality and retail breaches also have negative consequences for FIs. Account balance targets in FIs represent the closest possible approximation to actual cash for the cybercriminal. FIs are not only targets, but they are also more likely than firms in other industries to detect and report cybercrime. Regulatory controls imposed on transaction reporting and risk management in the financial industry make it more probable that a breach will prompt forensic investigation than if the same breach occurred in another industry.

The Verizon/USSS set of data breach cases are reported using structured data that Verizon has suggested should be the basis for incident analysis metrics. Data on each case is decomposed into four major categories, and each of these have subcategories [27]. An incident is considered to be fully described if reliable data exists to fill in the framework. For example:

- Agent
  - Source: External
  - Type: Organized crime
  - Origin: Brazil
- Action
  - Category: Hacking
  - Type: SQL injection
  - Path: Web application
- Asset
  - System: Database server
  - Platform: CPE X
  - Data: Personally identifiable information
  - Amount: 45,000 records
- Attribute
  - Type: Confidentiality

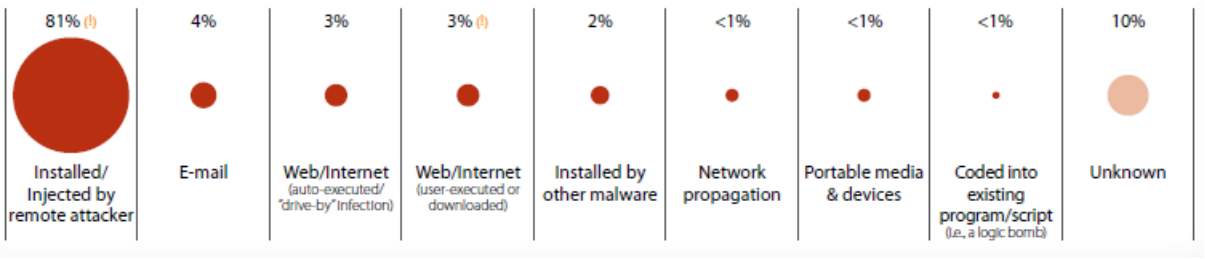
The investigative teams have classified incidents according to this standard meta-data structure in order to provide an industry standard framework within which to measure and compare data

breach frequency, associate controls, link impact, and many other concepts required for risk management. The framework has been supplemented with an online repository available for other investigation teams to contribute data [27]. Its tacit endorsement by the USSS suggests that it may be expected to be used by both public and private sector investigators and assessors going forward.

4.1 Malware Infection Vectors

The Verizon data breach classification suggests that malware paths are an important consideration in the criminal decision on technology choice, and this decision reflects the criminal assessment of FI vulnerability to a given attack vector. Figure 7 shows the relative percentages of infection vectors identified in the Verizon report.

Figure 7: Malware Infection Vectors by Percent of Breaches [25]



Each of these vectors is explained in the sections that follow.

4.1.1 Installed/Injected by Remote Attacker

This type of attack is accomplished by a perpetrator with access to internal operating systems from an external source. It may be accomplished by exploiting vulnerabilities that allow remote command execution via exposed software (e.g. SQL injection into web URLs, see [28]). It may also be accomplished via commands issued by malware via remote perpetrator command and control interfaces.

4.1.2 Email

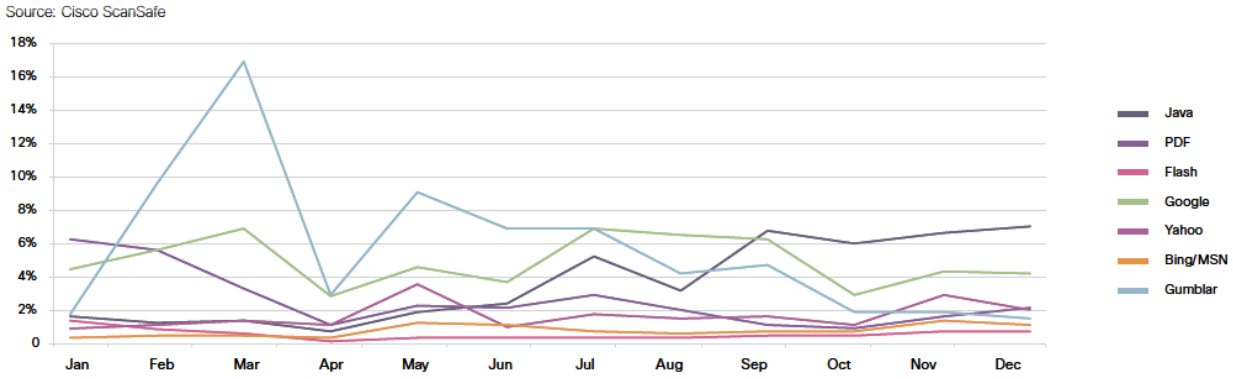
The discussion of malware propagation techniques in Section 2 highlighted phishing as a vector [29]. Phishing techniques originally were used to impersonate a bank or other institution with which a user may have an account, and encouraged the user to click a link in the email that would bring them to a site that looked like their banking site, but was actually fake. That site would either directly collect credentials, or download malware that would later collect them. As less easily detectable techniques for installing malware have been developed, random phishing techniques for malware propagation have become less common. Nevertheless, these techniques still exist and are increasingly customized as part of an overall campaign of attack.

4.1.3 Web/Internet Auto-Infection

The web is a popular attack vector for the simple reason that its use is ubiquitous. Malware injection processes that are generally classified as auto-infection occur without any overt action on the part of the user, such as inclusion of malware that automatically exploits a browser vulnerability in the iFrame example of Section 2. The propagation and infection both occur without the user's active participation or knowledge. Malvertising, the practice of placing malware in fake (or real) online ads, is also an increasing source of auto-injection attacks [30]. Malware operators may place ads with links to malicious sites in order to spread malware or the ads could also contain scripts which execute code on the PC.

High default trust settings on browsers and users operating with administrative privileges increase the effectiveness of this attack vector, which is enabled via a combination of vulnerable software and infected websites. These websites may be owned and operated by criminals, yet not conspicuously enough to be blocked by commercially available security services. They are often legitimate sites on which criminals have installed malware propagation code. Figure 8 provides an example of the types of software and search engines that are common delivery mechanisms for auto-injection attacks. It identifies the percentage of attacks per source in customer traffic observed by Cisco.

Figure 8: Sources of Drive-By Vulnerable Source [31]



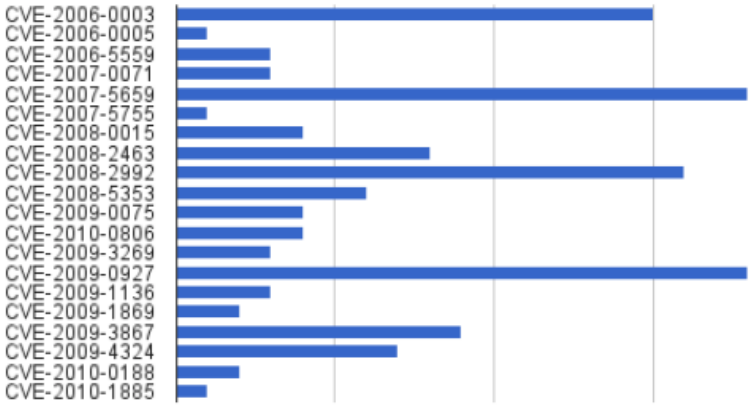
4.1.4 Web/Internet User-Initiated

Malware writers use creative methods to lure random users into executing malicious injection code. Drive-bys can happen by simply visiting a compromised or malicious website, viewing an email message and also by clicking on deceptive pop-up windows. Many of the latter incorporate a social engineering aspect to persuade the user to follow a malicious link. (For example, a pop-up that reads, "You are infected with a virus, click here to clean your system!").

These attacks rely less on browser vulnerabilities, but do require administrative access to infect at a level that will escape detection. Figure 9 classifies drive-by exploits by their Common Vulnerabilities and Exposure (CVE) number as assigned by a CVE Candidate Numbering Authority (CNA) for the exploit that it uses (for a complete description of each CVE, see [28]). This clustering is presumably due to the prevalence and ease of use of the exploit kits used to deploy attacks. Because exploit

kits are easily modified, even if patches were immediately deployed for this set of CVEs, the kit could be effective in exploiting a different set of vulnerabilities once new CVEs become available.

Figure 9: Sources of Drive-By Exploited Vulnerability [32]



4.1.5 Installed by Other Malware

In any of the above attack vectors, malicious software may be planted within the internal network. Although most FIs block most inbound traffic, it is rare for a commercial institution to block outbound web browsing. Malware with command and control capabilities will often connect back to the malware operator's site using common browsing protocols, and this allows malware on the internal network to receive both software and commands from the outside. Bots will often be equipped with multiple URLs so that if a malware operator site is taken down (whether due to maintenance or by law enforcement), another will be contacted which will have the same ability to issue commands to bots. Data collection networks are supported with a large number of proxy servers configured to relay data to the malware operator and to update bots with new addresses for data collection servers as the malware network evolves [33].

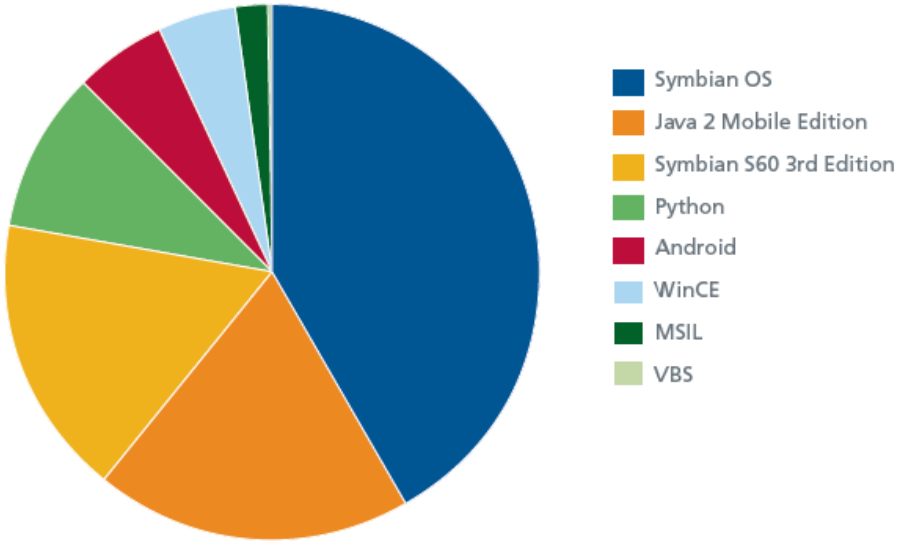
4.1.6 Network Propagation

Network periphery security is the first line of defense in keeping out hackers, and yet it is common for network firewalls to change and network engineer and operator mistakes, whether intentional or unintentional, sometimes have the consequence of allowing unfiltered Internet traffic into private networks. Even where firewall rules have not changed, changes to configurations of Internet-facing equipment behind firewalls may have the effect of allowing unauthorized access. Malware operators constantly attempt connections to addresses within the Internet address range owned by targets to see if the opportunity for unfettered access may exist. Although the network propagations attacks that took advantage of vulnerabilities in common network protocols (e.g. SQL Slammer) have not been prevalent recently, the potential for such attacks still exists.

4.1.7 Portable Media and Devices

Although portable media and devices are currently used in a small percentage of attacks, this vector category was a new addition to the 2011 Data Breach Report in recognition that the vector has unique properties for attack enablement. Where FIs approve a set of mobile devices for authorized network and data access, that device becomes a target of attacker reconnaissance. There are typically not mature security processes in place to identify and patch vulnerabilities in mobile devices, and their operating systems are purposely designed to allow ease of communication at the expense of access control. As more and more mobile devices are equipped with browsing capability, their utility as a platform from which to launch malware attacks may be expected to grow to the level of Web/Internet attacks [34-36]. Figure 10 shows the results of a McAfee Labs study on the number of separate malware instances identified by mobile platform. While the total number of mobile malware instances does not approach that of desktop computer or servers, Figure 10, in comparison with previous years, demonstrates that both the number and variety of mobile malware is increasing. This indicates a growing interest in the mobile environment by malware creators and operators.

Figure 10: Mobile Malware Platforms [36]



A paradigm example of desktop malware is spyware that evades detection while transmitting keystrokes and other observations on the desktop environment to a remote observer; it is considered even more insidious if it allows commands to be entered into the device from a malware operator. Yet this type of spy capability software is distributed through legitimate software distribution channels for mobile devices [37]. The openness of the Bluetooth protocol by which many of these devices communicate further blurs the line between legitimate and illegitimate observation of mobile communication.

4.1.8 Coded into FI Software

In order to embed malware into FI software, insider access is generally required. There are cases where insiders behave corruptly on their own in acts of fraud or revenge [38]; however, insiders may be compromised by outsiders to behave corruptly via bribery or social engineering. Insiders may also unintentionally create cyber risk and access to sensitive data for outsiders.

While cases often involve malicious insiders who developed the code or administer the system on which it runs [22], some known cases of this type were committed by outsiders. One of these involved an external agent that had access to the system for over six months. During this time, he studied the input/output process and developed custom malware to provide ongoing access to newly created internal data [39].

4.1.9 Social Media

A significant 19% of cases (Figure 11) cannot be ascribed to any of the attack vectors so far mentioned, and while none of the categories recognize social media as the primary source of cyber attacks, social media has been cited as a source of malware in very significant cases [40]. *Social media* is a generic term for Internet sites that allow users with similar interests to create web content in a collaborative manner. Examples of these sites are Facebook, Orkut, Hi5, MySpace, LinkedIn. They are also generically referred to as *social networking sites*, as the groups of people that collaborate on any one site are called a *social network*. With the increasing popularity of social media and the large communities of Internet users that it attracts, social media sites have become fertile hunting ground for malware operators.

Social media applications include functions that open communication channels with friends and acquaintances, and allow users to develop networks of people with like interests. It relies, for its operation, on trust between users. Whether or not a user on a social networking site has ever met the people with whom they communicate in person, there is an assumption that the people in a social network are friends rather than foes. The Internet provides a cloak of anonymity for people with malicious intent and allows them to use social media to masquerade as friends.

Friends in a social network frequently post links to a shared web page, and others in the group follow those links to view the shared content. Hence, one successful method of malware delivery via social media is to join a group of which the target is a member and post a link leading to a malicious site on a web page shared by the group. As in the *Web/Internet User-Initiated* attacks described in Section 4.1.3, the link takes the reader to a malware operator's website which automatically triggers a malware propagation and infection. Social networking attacks also may be launched from a trusted social networking site itself. As many of these sites allow collaborative application development and sharing, any member of a group may deploy malicious code that would likely be executed by the others.

Another option for using social media is to attack a primary target in two stages. In stage 1, the

malware operator targets friends of the primary target user, infects their computers, and captures the friend's login credentials for email and social media. With this information, the malware operator will then log in to the friend's accounts and post innocuous-looking links that lead to malware infection. They may also impersonate the friend by sending direct emails or instant messages to the primary target, encouraging them to select malicious links.

4.2 Internal Targets

As described in Section 2, the first step in a cyber attack is reconnaissance, the step in which an adversary surveys a target to identify points of vulnerability. It is an attack planning phase. However, in targeted attacks, this phase may be expected to continue throughout the lifetime of the malware install. Command and control facilities described in Section 4.1.5 will typically be used to continue reconnaissance within an internal network. Results will fuel further attack plans.

Malware authors mining an internal network for information have been creative. During 2010 an increase in focused attacks has shown attackers to package open source, toolkits and well architected botnets as part of their approach. In the past several years, malware professionals have been known to develop custom exploit code intended for a specific target after learning about the environment on their internal networks. Custom code increases overall malware effectiveness because it may exploit legacy protocol weaknesses that are not usually found on the public Internet, and often overlooked because internal networks are trusted. Custom code also allows malware operators to incorporate features to avoid internal monitoring systems to evade detection. Internal malware Internet communication is typically encrypted to evade content filters that may be installed in FI perimeters. Figure 11 lists some malware capabilities that may be expected to continue within an internal network once malware has gained a foothold.

5. Securing the Ecosystem

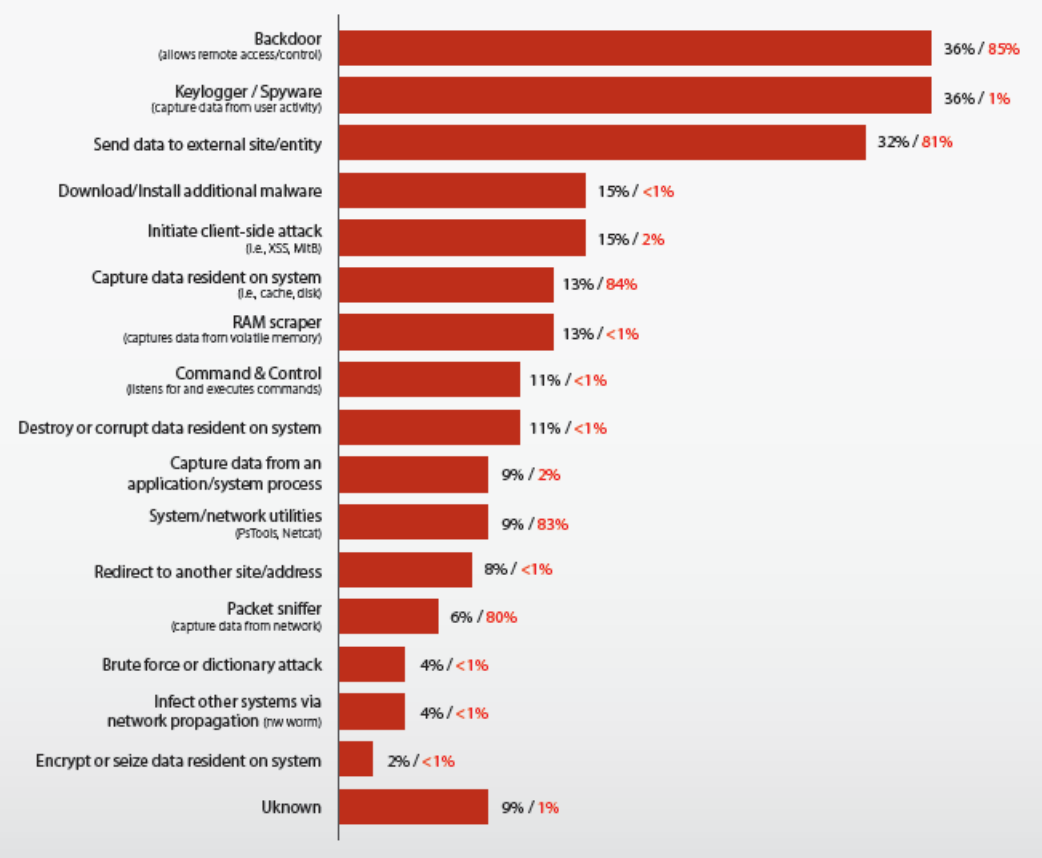
No FI is an island, and neither is the financial services industry as a whole technically self-sufficient. Successful malware attacks on FIs and FI customers often are traced to vulnerability exploits that originate from devices, components, and agents across the ecosystem in which the FI has deployed service. The vulnerabilities may be due to human or automated responses to attack, and are often outside of the FI's direct influence. Therefore, a key element of FI anti-malware strategy must be to acknowledge and face the problem of vulnerable ecommerce infrastructure. It is incumbent upon the financial industry to support cross-industry engagements to reduce systemic risk of malware by leveraging its collective influence on external entities.

There are at least five different types of security risks introduced by malware to financial institutions, including risk of attack on:

1. the financial institution directly
2. a financial institution service provider

3. a financial institution customer
4. multiple financial insitution customers
5. the financial services industry

Figure 11: Internal Malware Capabilities [26]



Within the categories of customer attacks, there will be different risks associated with the type of customer relationship, e.g., individual versus corporate clients. FI risk management strategies will differ based on the target of the attack. FIs should examine the flow of sensitive data through computing devices, and conduct multiple risk assessment scenarios. Each scenario should assume that different subsets of the devices through which sensitive data flows are infected with malware. Each scenario should be analyzed from multiple perspectives. For example, here are some simple questions to be answered in the course of each assessment:

1. What is the potential harm to <ourselves/our partner/ our customer> if <the device(s) involved in the scenario> is infected with <type of malware>?
2. How might we detect the infection?

3. How could we remediate the infection?
4. If we are unable to remediate the infection, is there someone else who could? How would we initiate that process?
5. If we are unable to detect the infection, when/how will we become aware of the consequences of the infection?
6. Is there a stage of the attack where we might become aware of the attack before <we/our partner/our customer> suffers harm?

If and where any of the analysis of malware infection scenarios results in probable damage or loss, FIs should consider products, services, partnerships, or industry initiatives that may be leveraged to improve the scenario's risk profile. Of course, this exercise will be guided by the FI's evaluation with respect to both risk tolerance and cost/benefit trade-offs.

Options for risk mitigation will also vary, and these will be based on the attack vector as well as the target. In order for any FI to successfully complete a scenario-based malware risk assessment, it must employ personnel who are cognizant of malware threats from all kinds of technical devices, including customized corporate devices, personal devices used for FI business communication or transactions, and third-party devices such as partner-provided network connections or airport or hotel kiosks used by traveling employees for remote access. As the threat environment continually evolves, personnel must continually seek new sources of current information on the types of malware being distributed and the common modus operandi deployed by cybercriminals. The FS-ISAC exists to serve this purpose, and has several processes with which to facilitate the communication of threat, vulnerability, and countermeasure information among FIs, software vendors, and government intelligence sources.

5.1 Situational Awareness

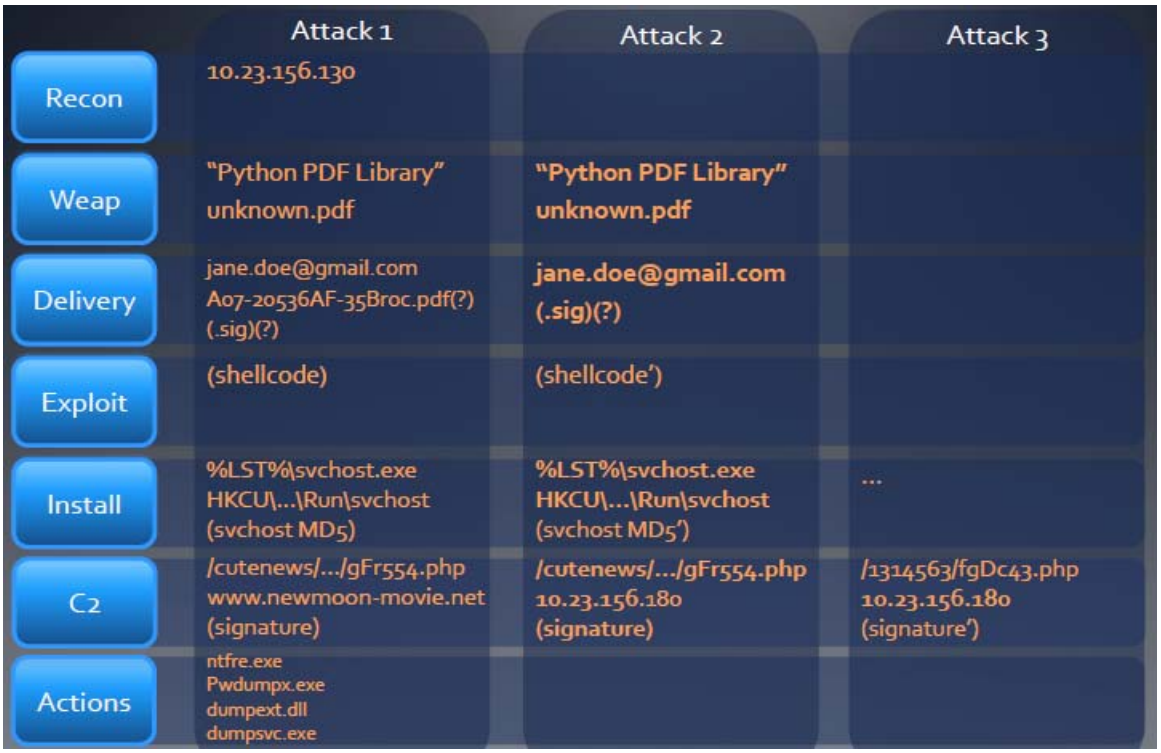
Regardless of its source, for a malware attack to be effective, each of the multiple steps – reconnaissance, assembly, delivery, compromise and execution (Figure 1) – must be successful. Reconnaissance may occur internally or from remote sources. Assembly may make use of java toolkits, php scripts, or command line batches. Delivery and compromise may occur via Web-Internet User-Initiated attacks or any other vector listed in Section 4.1. Command stages may include remote control of dormant bots or active and continuous keystroke logging. Exfiltration may be continuous or malware may stash data locally until it is retrieved. There are also a variety of other attack choice combinations, limited only by the imagination and programming skills of the adversary.

Although end-user awareness and training had typically provided defense in depth in security measures, malware attacks tend to follow the same pattern as a variety of legitimate software installation processes that conflict with typical FI security software setting, and so easily escapes even vigilant end-user detection. Users have been inundated with security instructions over the past decade that have not been effective in reducing their vulnerability to data loss and identity theft,

while at the same time they are constantly exposed to unnecessary security pop-up warnings. So real malware would appear to them to be yet another false positive. Unless an FI can develop accurate guidance on how to tell the difference between false positives and malware, most security advice will seems like a poor cost-benefit tradeoff to users, and so will be rationally rejected [41].

Moreover, malware operators will constantly vary attacks so that if any one is discovered, it will not lead to the detection of a similar one. Figure 12 is an example of alternative pathways for attack progression. It is important that FI detection processes be as flexible and adaptable as the capabilities of the adversary. The earlier in this attack progression an FI can detect that an attack is underway, the more damage may be averted.

Figure 12: Alternative Attack Choices [5]



FIs must be careful not to over-rely on traditional anti-virus software to detect malware infections. Polymorphic malware has made those methods unreliable. To keep pace with these new malware trends, many anti-virus and anti-malware software providers are incorporating heuristic capabilities into their products. These monitor software process behavior and attempt to identify anomalies. Heuristic malware detection can be effective, but often at the price of system performance.

While polymorphic malware may be capable of evading detection by traditional mechanisms, it can often be detected through the effects of the actions it takes. Organizations that monitor for unauthorized file level changes and for unauthorized or unusual communications patterns both within a network and through the network's perimeter may have a view into activity associated with

malware. Botnet and APT command and control activity can often be detected at the network level with specialized appliances being offered by a number of security vendors. This activity can also be gleaned from the analysis of server, proxy and firewall logs.

FIs typically monitor multiple aspects of their operation, and these monitoring processes may be engaged to assist in identifying and minimizing the impact of malware attacks. For example, FIs have monitoring processes that detect red flags in customer transactions. These range from anomalies in web server logs to unusual customer transaction patterns [42]. FIs also have monitoring processes designed to detect and respond to events that impact technology operations. Malware operators will attempt to stay below the radar of these monitoring processes, so FIs may need to adjust them in order to bring malware to the forefront of situation awareness. Red flag detection processes in different departments or business units may be combined with IT incident detection. Where malware incidents are detected, appropriate responses should not only mitigate the financial damage, but may involve redesigning internal processes to ensure the same attack vector will not be successful in the future.

Figure 13: Enterprise Incident Response [43]

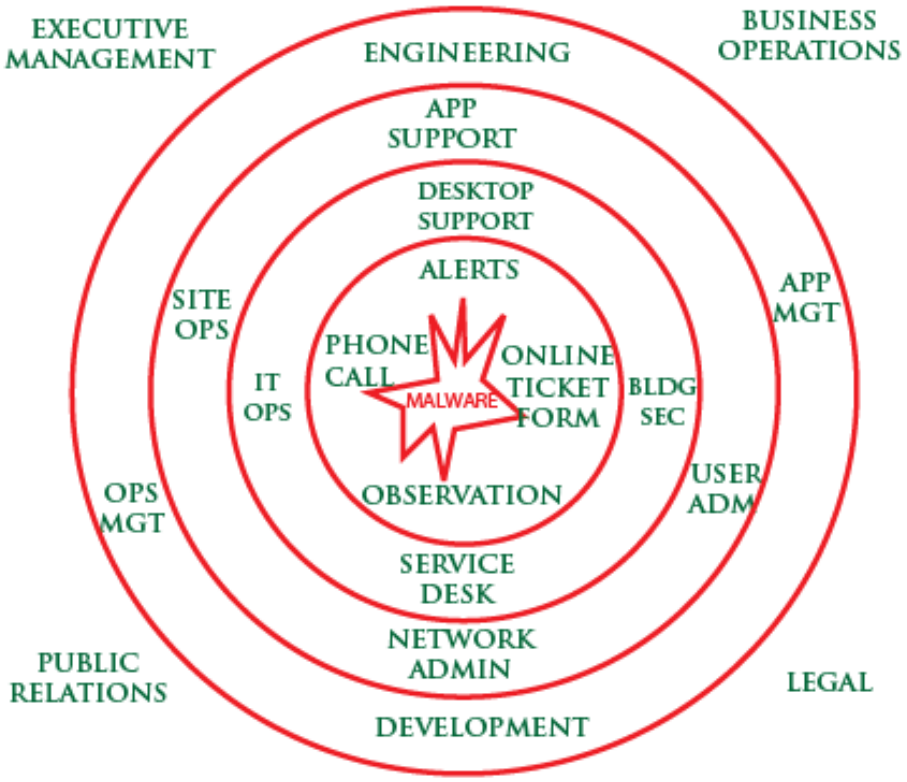


Figure 13 depicts a typical FI enterprise incident monitoring and response process that may be utilized to detect and respond to malware. Those with responsibilities for first response to technology and operations incidents are typically technicians who follow rote procedures to

determine the scope of an incident, resolve it if possible, and if not, hand it off to a more skilled administrative contact in the problem domain. This next level of support will attempt to resolve problems, but also recognize when the problem solution is beyond their capability and so requires escalation to more specialized expertise such as that found in systems engineers or application developers. Wherever an FI has such an alert and incident response process in place, whether based on automated monitoring or end-user trouble reports, there should be increased recognition at all levels of escalation that the root cause of the incident may be malware.

Additional processes designed to respond to malware that FIs should consider implementing at an enterprise level, if they are not already incorporated into existing incident detection response process, include:

Identification:	to ensure that incidents that have been identified as caused by malware are catalogued as such so that appropriate follow-up may be thorough and provide comprehensive insight into the overall state of the malware situation in proper context
Eradication:	to ensure that systems infected with malware are removed from service and reconstituted in such a way that does not allow malware persistence post reconstitution; reconstitution differs from recovery in that it implies root-cause forensic analysis and system configurations developed to ensure that the entity is no longer vulnerable to the same type of attack
Resilience:	to ensure that malware incidents do not have a lasting effect on business operations, damaging impact is minimized, and that operations processes are modified to incorporate prevention and detection techniques that would prevent the same type of attack in the future

The proper selection of controls to be included in each process will of course be based on circumstances specific to the FI business process. However, the scope of controls may extend to the customer, vendor, or business partner environment. For example, malware at a customer site may result in transfer of customer account balances to a malware operator. In this case, the FI may identify and catalogue the event via a Red Flag monitoring process, recommend that the customer initiate an eradication process, and provide services such as positive pay or two-factor authentication as resilience measures.

5.2 Risk Management

A 2010 end-of-year Gartner technology report warned clients to make a strategic planning assumption that by 2015, a G20 nation's critical infrastructure will be disrupted and damaged by online sabotage [44]. The report cautioned that, although such attacks may appear to begin with a narrow scope, they should be assumed to be capable of lasting repercussions due to the inclusion of multimodal attack techniques over time. By several estimates, a large percentage of both internal and external users experienced an average of more than 100 web malware encounters per month, increasing the probability that any given user will be infected [31, 32]. Although specific numbers in various surveys that chronicle increasing costs of data breaches may be debated, it is obvious that

both the variety of incidents and the quantity of data lost is constantly rising, and that each incident is accompanied by monetary loss [45-47]. FIs should do their own risk analysis. According to the US Secret Service, given current evidence that there are large criminal communities directly targeting the US financial sector, FI exposure to malware is extremely high and should be treated with the probability of 1 in FI risk management calculations [13].

Malware presents a range of evolving risks: reputational, regulatory, financial, and legal. Reputational risk is increased because of the high visibility created by reporting requirements and the volume of information at risk. Regulatory risk is derived from the types of information assets targeted by malware operators, which include personally identifiable information, account information, and deposits, as well as the criticality of the service and the provider to the monetary system. Security requirements for these information assets are included in the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), Payment Card Industry (PCI) Data Security Standard, and the Health Insurance Portability and Accountability Act (HIPAA) [48-51]. Financial risk may be estimated using potential losses associated with successful malware attacks. Legal risk may be associated with civil challenges on due care and due diligence issues [52].

Proceeding on the assumption that malware presents risk to FIs, there are a number of standard controls that may mitigate the risk. The first and most important is software change control. Software change control refers to a process whereby software is developed, compiled into packages for installation, labeled with version numbers, deployed by authorized personnel, and tracked on production systems. To be effective against malware, software change control processes must continue to track software through its deployment and operation. Changes to software must be automatically detected. Upon detection of a change, the change must be analyzed by someone with sufficient knowledge and reference materials to tell the difference between an authorized change and an unauthorized change. The reference materials should include tests such as cryptographic checksums that can be used to verify that code deployed in production is the same as the package that was delivered from a development environment or vendor. These detection processes must occur immediately after changes are detected. Changes must be detected on all operating system platforms and monitored for integrity, as malware operators are likely to attempt to disable or corrupt the software used for change monitoring.

Change monitoring should not be limited to software, but should extend to security configuration and role assignments such as start-up variables, firewall rules, and privileged accounts. Privileged account monitoring must be established in conjunction with a policy of authorized account usage so that authorized use may be distinguished from unauthorized use. For example, where users or software running in an administrator context is typical in a firm, this scenario used to install malware would not be detected as an intrusion. Even desktop administrators should be furnished with separate accounts reserved for privileged operations. Ideally, administrative access would be segmented so that systems would be subject to malware compromise via only a small percentage of total system users.

Another standard control that is a critical component of any malware mitigation strategy is control over the network periphery. This control requires that an FI establish a clear policy that allows administrators to determine authorized from unauthorized connections, and oversight that ensures compliance with these policies. Firewall rules and security configurations over all network equipment should also be subject to change control as described above for software. FIs with network peripheries that are too large to manually review firewall rules in near real-time should have automated means to determine policy compliance for both inbound and outbound network connections. Lists of malicious sites are published and announced to FIs by the FS-ISAC. Connections to or from the FI network to any published malicious site should be restricted via automated means. Both inbound and outbound network traffic should be examined for known malware patterns and signatures using intrusion and/or prevention detection systems. Any discretionary Internet traffic generated by FI users that may be a conduit for malicious content, such as email and web browsing, should be routed to choke points where proxy servers may be employed to inspect content for malware signatures as well as sensitive data. Proxy servers are frequently capable of decrypting encrypted web traffic, and these servers should block encrypted traffic if it cannot be decrypted for inspection (of course, exceptions may be made for authorized business applications).

A third critical component of any malware mitigation strategy is vulnerability management. Operating system and application security standards should be established that, if followed, will ensure compliance with FI objectives for access to system programs, facilities, and data. These standards should be enforced with automated compliance-checking software, and that software should be monitored for integrity. All operating system and software security patches should be applied to any system for which they are available. Where vendors no longer support software patch processes, or do not commit to fixing security vulnerabilities in a given commercial product, FIs should consider alternative software vendors or versions for which security patches are available.

FIs should also consider what may constitute evidence of malware intrusion in their technology environment, and identify patterns of activity that it may be possible to log and automatically detect in a manner that would trigger an incident response. Where it is not feasible to automate detection, manual log review procedures may be necessary to identify evidence of intrusion. Candidates for log monitoring include, but are not limited to, failed outbound email server connections attempts, network scanning, and excessive domain name queries [53]. Due care should be exercised to ensure that the logs are collected as expected, and that they are archived with integrity.

Metrics on software change control, network periphery control, vulnerability management, and log management, as well as digital identity and incident response metrics, should be devised and employed as part of a comprehensive security management strategy. These metrics should be generated and reviewed as part of continuous operations monitoring processes and used in the course of daily security management.

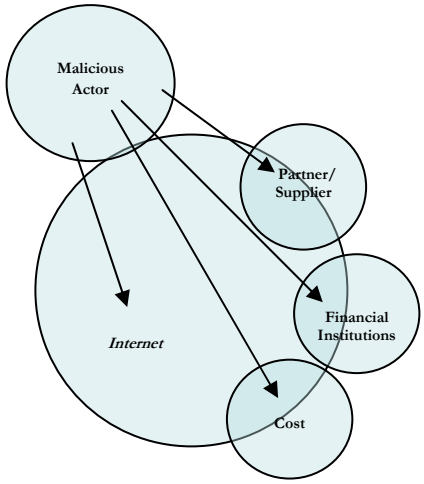
5.3 Cross-Industry Anti-Malware Roles and Responsibilities

Though FIs are a high value target for malware-based exploitation, the financial sector does not operate in cyberspace in isolation. Other institutions are not only targets for malware, but more importantly, they are exploited as the means by which attacks are perpetrated against FIs. Any device capable of running operator-installed software is a potential attack vector, and much of the software run by FIs is not under FI control. This distinction has been characterized as the *managed* versus *unmanaged device* issue. Yet even in cases where FIs manage electronic devices, software updates may be delegated to vendors and are usually accomplished via automatic downloads.

A business or technology partner that provides software or electronic processing that is used to support customer relationships is generally referred to as a "third party" to distinguish it from the two-party relationship an FI has with its customer. The decisions third parties make about their own anti-malware practices have a direct impact on the efficacy of FI anti-malware strategies, sometimes with grave consequences. It is therefore imperative that the financial services sector set clear requirements for third party stakeholders.

Moreover, the Internet ecosystem that FIs inhabit is populated by service providers that are not currently considered third parties in the traditional sense of the term. These are technology operators that facilitate Internet communications between FIs and customers, but are not contractually or otherwise bound to specifically support FI services. Figure 14 illustrates that FIs operate in an Internet environment that is facilitated by Internet Service Providers (ISPs), Internet eXchange Points (IXPs), and administrative institutions such as Internet Corporation for Assigned Names and Numbers (ICANN), among other technology operators.

Figure 14: Financial Industry Cyber Ecosystem



These facilitators run critical aspects of Internet operations that may yield attack vectors. A good example of this dependency involves domain name service providers. Internet domain names are registered by FIs and are administered internally or through third party domain name service providers. Administrators correlate domain names to numeric network addresses of computers

owned and operated by or on behalf of the FI. Customers know only the FI domain names, not the IP addresses, and therefore must rely on the domain name system to direct them to legitimate FI network resources. However, perpetrators of cybercrime exist in the same ecosystem, and may be expected to attack any vulnerable component if that attack vector could provide information that may ultimately lead to a successful attack against an FI. For example, if a provider of domain name services to a customer or FI business partner is corrupted, then those customers and business partners who type an FI domain name into their browser may be directed instead to a malicious site. In such cases, criminal operations are beyond the FI scope of operations, and correspondingly beyond its ability to quickly detect or respond.

A recent exercise tested the ability of financial institutions, card processors, businesses, and retailers to respond to major cyber attacks against payment systems [54]. Attack vectors used against the financial industry in the exercise included many of those described in Section 4. Over 600 FIs, card processors, retailers, and business customers participated in the exercise, and all reported that they would have been severely negatively impacted from the attack. For example, most participating financial institutions (58%) don't have a contingency plan focused on Distributed Denial of Service (DDoS) and a majority of those that do rely on Internet Service Providers to provide mitigation. Yet a recent Arbor network survey of ISPs reveals that a full 50% of their DDoS mitigation strategies are known to further degrade service, essentially completing the attack as a first step toward defense [55].

The decisions that domain name service providers and other cyber facilitators make with respect to anti-malware practices have a direct impact on the efficacy of FI strategies. It is therefore important that each FI set clear requirements for security practices at service providers as part of any cyber-related service level agreement. These practices should not simply refer to financial industry standards, but should specify that service providers must create and maintain continuous security situational awareness and defense capabilities that correspond to the risk that malware may present to the integrity of the contracted-for services. Where service providers do not share traditional third-party relationships with FIs, such requirements must nevertheless be articulated in order to provide a basis for defining due diligence on the part of service providers, and potential corresponding claims of negligence.

Table 4 is an example of reasonable expectations that FIs may have for Internet ecosystem technology providers who may or may not be traditional third parties for the financial services industry. The first column in Table 4 lists examples of the types of these businesses generically by product or service. The second column identifies technology controls that the provider in the corresponding row may reasonably be expected to perform in order to minimize potential damage due to malware. The third column classifies the control in the second column according to the information security industry triad of *prevent, detect, recover*. The word "prevent" in the third column indicates that the control activity identified in the second column may prevent a "malware event" before it happens. The word "detect" in the third column indicates that the control activity identified in the second column contributed to FI capability to discover when a "malware event" occurred. The word "recover" in the third column indicates that the control activity identified in

the second column may reduce the risk of harm to the ecosystem from a participant that has been infected, and/or improve the capability of an FI to disinfect a device after a "malware event" has occurred.

Table 4 includes stakeholders who could be partnering with FIs and their other customers to improve the ecosystem's overall resistance to malware. The table highlights the unique contribution of each contributor to each phase of the anti-malware cycle. The intent of this section is to not list all the things currently being done or that could be done, but to place focus on behaviors that are either rare or non-existent, but if more widely adopted, would reduce the risk of harm to FIs from malware-enabled exploitation.

Table 4: Potential Role of Technology Providers in Minimizing Malware Risk to the Internet Ecosystem

Stakeholder	Control Activity	Control Type
Advertising Services	A wide variety of media outlets sell advertising to media, retail, and other internet sites. These services should provide due diligence to ensure that malware is not delivered via advertisements.	prevent
Anti-Malware Vendors	Anti-Malware software vendors should improve malware detection capability by pursuing advances in both methods and timing for client updates. They should participate in efforts to establish malware detection metrics.	detect
	Anti-Malware software vendors should also improve malware isolation features, fail in safe mode, and also ship products with the more secure settings as default.	recover
Application Stores	Application (App) Stores vend software for a variety of digital devices, including mobile phones and desktops. They should improve due diligence efforts to ensure the applications they sell do not contain known malware or otherwise obviously suspect software.	prevent
Certificate Authorities	Certificate Authorities (CA) play a key role in the security of online banking applications in that proper application of the technology allows a customer to identify imitation banking sites. However, recent failure in the security of CA administrative functions secure has resulted in issuance of "valid" SSL and EV-SSL certifications to criminal elements. CAs need to evolve their technology and service offerings to prevent these malicious activities.	prevent

Domain Name Service Registrars	Domain Name Service (DNS) Registrars should play a key role in malware prevention by improving due diligence so that cybercriminals find it harder to register new domains to perpetrate phishing attacks and/or malware drive-by sites.	prevent
	It is absolutely critical that DNS Registrars maintain accurate data on domain name owners so FIs can perform effective investigation into instances of abuse. Unavailable or inaccurate registration data increases the cost of online fraud investigation and remediation activity.	recover
Email Hosts	Various industry standards have been developed to prevent email spoofing and spamming at the server level. Email hosts should observe Internet Engineering Task Force (IETF) standards and BITS recommendations for enabling email authentication and validation processing on both inbound and outbound mail streams [56].	prevent
ICANN	ICANN issues generic Top Level Domains (gTLDs) for specific purposes but generally does not enforce the manner in which they are used (e.g. .com, .edu). A gTLD issued for financial services should be restricted to FI registrations. In this environment, technologies could automatically provide higher levels of security for FI online services.	prevent
Internet Service Providers	Internet Service Providers (ISPs) should ensure that their networks do not allow traffic that spoofs IP addresses.	prevent
	ISPs should offer proxy services that block known malware and criminal sites by default.	prevent
	Both land-line and mobile ISPs are in a unique position within the ecosystem to detect patterns of malicious activity such as botnet traffic and malware infection signatures.	detect
	ISPs that detect malware should either warn or educate the system owner, and/or quarantine the affected system as appropriate to safeguard other systems.	recover
Mail User Agent Vendors	Mail User Agents (MUAs) like Outlook, Apple Mail, Thunderbird, etc. can help prevent malware infections by leveraging security indicators and business rules that users can leverage to identify when a message in their inbox (or spam folder) is suspect.	prevent

Operating System Vendors	Operating Systems (OS) vendors that include features for internet connectivity and operator-installed software should provide improved platform functionality to prevent unauthorized software installation. They should take advantage of advances in trusted computing technology to accomplish these goals.	prevent
	OS vendors should provide customers with the ability to identify and catalogue all software on their system, and disable the ability of malware to evade standard software monitoring utilities.	detect
	OS vendors should maintain rapid incident response capabilities that allow customers to report security incidents and provide accelerated distribution services for security patches.	detect
	OS vendors should consider offering customers malware remediation services, wherein the vendor can assist in cleaning up a subscriber's device of the malware without otherwise impacting its productive operation.	recover
Web Browser Vendors	Web browsers should have safe modes wherein no software may be installed on a local machine no matter what the user behavior. Vendors can help prevent malware infections by collecting information about malware-infected websites and enabling safeguards in the browser that warn or block a user from visiting known infected sites.	prevent
	Web browsers should provide logs and statistics of software installation and operation that originates via browser functionality such as downloads and plug-ins.	detect
Web Browser Plug-in Vendors	Vendors that encourage users and web developers to incorporate their software into web-enabled environments should include security features that allow users to limit the access of the plug-in to specific operations that may be secured at the operating system level. These security configurations should be configured by default upon installation.	prevent
	Web browsers plug-ins should provide logs and statistics of files accessed and operations performed by the plug-in, and these should be archived and available for inspection.	detect

Web Server Hosts	Web server hosting providers should follow strict software security and change control procedures to prevent vulnerabilities that allow unauthorized malware to be planted on their sites.	prevent
	Web hosting providers should provide whistle-blower reporting facilities to receive and respond to notifications that a website that they host has been discovered to include malware.	detect
	Web hosting providers should create, maintain, and follow standard procedures to effectively quarantine malware on a client's website. Web hosting providers should proactively test their sites to detect the presence of unauthorized malware.	respond
Critical Infrastructure Regulators	Regulators should consider the above recommendations for malware risk reduction for entities within their scope in establishing regulatory requirements for ecommerce and Internet safety.	prevent
End Users	End users should assume responsibility to update and maintain their systems to the extent possible to enhance security. Additionally, these users should take responsibility for protecting information necessary to implement security measures such as PINs.	prevent

6. Conclusion

Malware is both insidious and pervasive. The financial services industry is a prime target, making it imperative for financial institutions to prepare to face malware attacks and prevent financial loss, damage to reputation, reduction in customer assets, data breaches, regulatory oversight, and/or lack of management control over technology assets. FIs should recognize that malware operators rely on a strong and stable financial industry in order to profit from crime. They are unlikely to target critical transaction processing systems for fear that their own fraudulent transactions will not be processed. Unless there is a hostile intent to cause damage, as in a nation-state declaration of war, malware operators are likely to maneuver between the seams of authorized business processes, and inject just enough variation required to execute their criminal mission. Moreover, although crimeware and state-sponsored cyber attacks and campaigns are the most visible form of attack, FIs should recognize the increasing threat from both external and internal sources, and take practical measures to detect and defend against potential internal malware interference with business process.

FIs should evaluate their vulnerability to the malware described in this report and implement

appropriate safeguards to minimize any potential for damaging impact. This should not only include the implementation of layered preventative measures, but also measures to detect the presence of malware and a plan to respond to malware once it is detected. The plan should be exercised periodically as is done for business continuity and disaster recovery planning purposes. Response plans should be integrated into the financial institutions' overall crisis management process so that highly impactful attacks are responded to with the appropriate level of senior management involvement and oversight. Integrating the plan within the overall crisis management process will ensure that escalation points are defined, governance processes are in place, and there are representatives from the appropriate functional units that might be called upon to assist in management of the response and communications to stakeholders.

Appendix A. Terms and Definitions

Bot:	derived from the word "robot," and used in a variety of Internet contexts, in the context of this paper, it refers to a program that runs in the background on a personal computer of an unsuspecting user, having been installed by malware
Botnet:	a collection of bots that receive instructions from the same "master" program
Data Host:	company that maintains servers on the Internet that process data for customers using a standard technology such as web or email servers
Exfiltration:	method by which malware exports data from an infected host, typically refers to an unauthorized process of acquiring data from a computer system through network channels or unauthorized portable media
Footprint:	with reference to a software component is used to indicate the physical characteristics of a file such as its size, the file names as well as the operating system's resource utilization. These characteristics help to uniquely identify the various software components encountered during the investigative process.
Jabber:	a communications protocol used for instant messaging
Kernel:	operating system component that serves as a bridge between software applications and system services provided by hardware, and typically designed to facilitate a trusted channel between the OS user and system-level functionality
Malware:	malicious software, any and all software that is deployed with malicious intent
Operating System:	software that directly manages and controls interaction with hardware devices that combine to compose a computer, provides common services to applications, and makes resources available to users
Phishing:	email-born malware propagation systems
Rootkit:	enables privileged access to a system and the ability to hide that access by subverting the provided authentication, authorization, and audit functions
Socks:	a protocol that allows multiple network connections to route network traffic through a single network-enable device
Zero-Day:	modifier for the word threat or attack, meaning that the vulnerability that is used by the threat agent is not known to potential victims

Appendix B. Acronyms

API:	Application Programming Interface
ATH:	Automatic Transaction Hijacking
APT:	Advanced Persistent Threat
CA:	Certification Authority
CCV:	a primary Credit Card verification number, which is read automatically from the card, also may be referred to as CVV, card verification value, or CSC, card security code
CCV2:	a second Credit Card verification number, which is typically printed on a card and provided to a merchant by a card holder when a purchase is made remotely
CNA:	CVE Candidate Numbering Authority
CPE:	Common Platform Enumeration, a NIST standard (see http://nvd.nist.gov)
CVE:	Common Vulnerabilities and Exposures, a dictionary of publicly known security vulnerabilities and exposures using common terms and names under a project managed by The MITRE Corporation (see http://cve.mitre.org)
FTP:	File Transfer Protocol
gTLD:	generic Top Level Domain
HTML:	Hypertext Markup Language, a form of code used to display web pages
HVAC :	Heating, Ventilating, Air-Conditioning technology
ICANN:	Internet Corporation for Assigned Names and Numbers, a non-profit corporation created in 1998 to manage the distribution of Internet addresses
ICS:	industrial control systems
IO:	Input, Output
IRC:	Internet Relay Chat
ISP:	Internet Service Provider, a company that connects customers to the Internet
IXP:	Internet eXchange Point, a physical infrastructure through which Internet service providers (ISPs) exchange Internet traffic with financial institutions
MUA:	Mail User Agent
NIST:	National Institute of Standards and Technology
OS:	Operating System
POP3:	Post Office Protocol, version 3
TAN:	transaction authentication numbers
URL:	Universal Resource Locator

Appendix C. Contributors

Jennifer L. Bayuk, Jennifer L. Bayuk, LLC
Doug Cavit, Microsoft
Eric Guerrino, Bank of New York Mellon
James Mahony, PNC Financial Services Group
Brett McDowell, PayPal
William Nelson, FS-ISAC
Rick Snevel, KeyBank
Peter Staarfanger, Synovus

BITS thanks VeriSign's iDefense organization for providing key research material which made a substantial contribution to this effort.

BITS Staff Lead: Greg Rattray

About BITS
BITS addresses issues at the intersection of financial services, technology and public policy, where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services. BITS is the technology policy division of The Financial Services Roundtable, which represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Roundtable member companies provide fuel for America's economic engine, accounting directly for $92.7 trillion in managed assets, $1.2 trillion in revenue, and 2.3 million jobs. For more information, go to http://www.bits.org/.

Appendix D. Citations

1. Krauss, L. and E. MacGahan, *Computer Fraud and Countermeasures*. 1979, Englewood Cliffs, NJ Prentice-Hall.

2. Stoll, C., *The Cuckoo's Egg*. 1989: Doubleday.

3. Mell, P., K. Kent, and J. Nusbaum, *Guide to Malware Incident Prevention and Handling, SP800-83*. 2005, National Institute of Standards and Technology.

4. International Telecommunication Union, *ITU Study on the Financial Aspects of Network Security: Malware and Spam*. 2008.

5. Cloppert, M., *Evolution of APT State of the ART and Intelligence-Driven Response*, in *US Digital Forensic and Incident Response Summit* 2010, SANS: http://computer-forensics.sans.org.

6. Jacobs, A. and M. Helft, *Google, Citing Attack, Threatens to Exit China*, in *New York Times*. 2010.

7. Zeltser, L., *Analyzing Malicious Software* in *Cyberforensics*, J. Bayuk, Editor. 2010, Springer.

8. The VeriSign® iDefense® Malicious Code Operations Team, *IFrame Attacks – An Examination of the Business of IFrame Exploitation*, malcodeops@idefense.com, Editor. March 28, 2008, VeriSign® iDefense®

9. The VeriSign® iDefense® Intelligence Operations Team, *Notable Malware for 2010*. April 21, 2010, VeriSign® iDefense®

10. Menn, J., *Fatal System Error*. 2010: Perseus Books Group.

11. Geer, D.E. and D.G. Conway, *The Owned Price Index*. IEEE Security & Privacy, 2009. 7(1): p. 86-87.

12. Jakobsson, M. and Z. Ramzan, eds. *Crimeware: Understanding New Attacks and Defenses*. 2008, Safari Technical Books.

13. Koffman, S., *USSS Malware Update for FS/ISAC*. March 14, 2011.

14. Panda Labs, *PandaLabs Annual Report 2010*, www.pandasecurity.com.

15. FS-ISAC, *Threat Viewpoint, Advanced Persistent Threat*. 2011.

16. Krebs, B., *'Stuxnet' Worm Far More Sophisticated Than Previously Thought*. KregsOnSecurity.com, September 22, 2010.

17. Wingfield, N. and B. Worthen, *Microsoft Battles Cyber Criminals* in *Wall Street Journal*. 2010.

18. Davidson, P., *Cyberspies have hacked into power grid, officials say*, in *USA Today*. 2009.

19. Clarke, R.A. and R.K. Knake, *Cyberwar*. 2010: HarperCollins.

20. Gallaher, M.P., A.N. Link, and B.R. Rowe, *Cyber Security, Economic Strategies and Public Policy Alternatives*. 2008: Edward Elgar.

21. *Securing Critical Infrastructure in the Age of Stuxnet, Sean P. McGurk, acting director of the Homeland Security Department's Cybersecurity Center*, in *US Senate Homeland Security and Governmental Affairs Committee*. November 17, 2010.

22. Cappelli, D., et al., *Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition (Version 3.1)*. 2009, Carnegie Mellon University.

23. Christie, C.J., *Former UBS Computer Systems Manager Gets 97 Months for Unleashing "Logic Bomb" on Company Network*. US DOJ Press Release (News), December 13, 2006.

24. *Conference Report to Accompany H.R. 3288, Department of Transportation and Housing and Urban Development, and Related Agencies Appropriations Act, 2010,* Dec. 8, 2009.

25. Baker, W., et al., *Data Breach Investigations Report, http://www.verizonbusiness.com/go/2011dbir*. 2011: Verizon Business.

26. Baker, W., et al., *Data Breach Investigations Report, http://www.verizonbusiness.com/go/2010databreachreport/*. 2010: Verizon Business.

27. Verizon Business, *Verizon Incident Sharing Metrics Framework, http://securityblog.verizonbusiness.com/2010/02/19/veris-framework*. 2010.

28. *National Vulnerability Database*. Available from: http://nvd.nist.gov/.

29. Anti-Phishing Working Group, *Phishing Activity Trends Report, 2nd Qtr*. 2010.

30. Deloitte Touche Tohmatsu (DTT), *Media Predictions TMT Trends 2009*. 2009.

31. Cisco Systems, *Cisco Global Threat Report 4Q2010*. 2011.

32. Dasient Blog, *The Dasient Q4 Malware Update*. 2011.

33. Sinclair, G., C. Nunnery, and B.B.H. Kang. *The waledac protocol: The how and why*. in *Malicious and Unwanted Software (MALWARE), 2009 4th International Conference on*. 2009.

34. The VeriSign® iDefense® Intelligence Operations Team, *Mobile Threats*. November 13, 2009, VeriSign® iDefense®

35. Kwan, M., *Hack Any RFID-Enabled Credit Card for Eight Bucks* in *Mobile Magazine*. 2008.

36. McAfee Labs, *McAfee Threats Report: Fourth Quarter 2010*. 2011.

37. United States Computer Emergency Readiness Team, *Cyber Threats to Mobile Devices* 2010, US-CERT.

38. Sims, S., *Insider Threat Investigations*, in *Cyberforensics*, J. Bayuk, Editor. 2010, Springer.

39. *United States of America versus Albert Gonzalez*. 2010, United States District Court, District of New Jersey.

40. Stamos, A., *Aurora and Advanced Persistent Threat Response Recommendations*. 2010, iSEC Partners.

41. Herley, C., *So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users*, in *New security paradigms workshop*. 2009, ACM: Oxford, United Kingdom.

42. FS-ISAC Account Takeover Task Force, *On-line Fraud Detection White Paper*. 2011.

43. Bayuk, J., *Securing Web Applications* in *CSO Executive Series on Application Security*, CXO Media, January, 2009.

44. Gammage, B., et al., *Gartner's Top Predictions for IT Organizations and Users, 2011and Beyond*. 2010.

45. Ponemon Institute, *U.S. Cost of a Data Breach Study, http://www.ponemon.org*. 2010.

46. Wingfield, N., I. Sherr, and B. Worthen, *Hacker Raids Sony Videogame Network*, in *Wall Street Journal*. 2010.

47. McMillan, R., *Epsilon: A watershed for an industry under siege*, in *ComputerWorld*. 2011.

48. *Gramm–Leach–Bliley Act, US 106-102*. 1999.

49. *Sarbanes-Oxley Act, US116 Stat. 745*. 2002.

50. Payment Card Industry (PCI) Security Standards Council, *Payment Card Industry (PCI) Data Security Standard, Version 1.2*. 2008.

51. HIPAA, *Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule*, US Department of Health and Human Services, Editor. 2003: Federal Register Vol. 68, No. 34.

52. Wolf, C., *Proskauer on Privacy*. 2008, Practicing Law Institute.

53. United States Computer Emergency Readiness Team, *Malware Threats and Mitigation Strategies*. 2005, US-CERT.

54. Delta-Risk, I., *Cyber-Attack Against Payment Processes February 2010 FS-ISAC Exercise After Action Report*. 2010, US Financial Services Sharing and Analysis Center.

55. Arbor Networks, *Worldwide Infrastructure Security Report, Volume VI*. 2010.

56. BITS, *BITS Email Security Toolkit*. 2007, The Financial Services Roundtable, http://bits.org/p_publications.htm.