Data-stealing Malware on the Rise—Solutions to Keep Businesses and Consumers Safe

Focus Report Series

June 2009

Table of Contents

Introduction

The Data-stealing Malware Report is the inaugural report in a new series of quarterly focus reports published by Trend Micro to address the rapidly changing, ever-evolving threat environment. The Focus Report Series is based on data from TrendLabs, Trend Micro's global network of research, service, and support centers committed to constant threat surveillance and attack prevention. With accurate, real-time data, TrendLabs delivers effective, timely security measures designed to detect, pre-empt, and eliminate attacks. With more than 800 security experts worldwide and 24x7 operations, TrendLabs is headquartered in the Philippines with regional labs in the United States, Japan, France, Germany, and China. TrendLabs' regional presence and round-the-clock operations enable immediate identification and timely response to targeted, regional threats.

TrendLabs monitors potential security threats and conducts research and analysis that is used to develop technologies that identify, detect, and eliminate new threats. Using a combination of technologies and data collection methods including "honey pots" for email, web crawlers, and web, email and file reputation services augmented with feedback mechanisms and correlation technologies, Trend Micro researchers proactively gain intelligence about the latest threats.

TrendLabs has a finger on the pulse of daily security threats that impact a worldwide customer base. TrendLabs and Trend Micro threat technologies detect many threat varieties, which are discussed in this report including malware, crimeware/grayware, software vulnerabilities, mobile threats, spam, phishing, rootkits, and botnets.

Executive Summary

Data-stealing malware is a dangerous web threat category that has shown tremendous growth in the last few years. Occurring as a chain of events, data-

stealing malware is usually the second or third component of a sequential multi-pronged attack. Users contract the malware by clicking on a malicious link in an email or by innocently visiting an infected web page. The end result is usually the same—infection by Trojan. Trojans are especially worrisome as they appear to be ordinary software programs, videos or music files. Their actions, however, are anything but benign. Trojans work to establish a channel with a remote server then use a variety of techniques to steal information from their host. Trojan infections are on the rise and according to Trend Micro data, the Trojan threat category has grown exponentially in every country across the globe over the last three years.

Most data-stealing malware originates from cybercriminals and their purpose is varied, although almost always nefarious in intent. Data-stealing malware are used to gather and steal banking logins and credit card numbers, intellectual property, confidential data, administrative passwords, address books, and to spread malware that assimilates PCs into botnets. Malware authors vary—from professional criminals who sell the data on the Black Market to disgruntled employees who leak information to the outside for profit or revenge. In the past three years, data breaches have grown more serious. For example, the retail grocer, Hannaford Brothers, lost 4.2 million credit card numbers in a daring hacker breach that cost the company both financially and in brand image. Reasons for breaches vary—from lax security protections to lack of stringent standards. Consequences of data leaks are dire as corporations pay out millions of dollars in class action lawsuits filed by the consumers whose data has been stolen. Companies also suffer from a loss in market share, falling stock prices, and a tarnished brand image. Consumers lose too in the form of identity theft—a serious problem that can cause financial upset and years of work to unravel the theft and reclaim stolen identities.

In addition to cybercrime, data-stealing malware is also being used to further terrorism and to launch attacks against government targets. Some believe that clever hackers may have already compromised the U.S. electrical grid and cyber terrorist attacks have been documented in Europe in recent years. Cyber espionage

is an additional concern and occurs when data-stealing malware is surreptitiously installed on corporate servers to siphon off intellectual property such as product designs, contract information, business plans, and other trade secrets.

To date, law enforcement efforts toward cybercrime have been fragmented, largely due to lack of a coordinated effort. Although most law enforcement agencies have a department assigned to manage computer crime, these groups do not regularly communicate or share resources. Enforcement efforts are complicated by the fact that malware attacks typically cross international borders, making criminals especially difficult to hunt down and prosecute. A lack of laws protecting consumers poses an additional challenge. Several bills have been introduced recently to Congress to address this matter and the new U.S. administration is discussing appointing a cyber security director to address national security problems related to cybercrime, cyber espionage, and malware attacks on consumers.

Several task forces have been formed that provide an early foundation for increased collaboration within the security community. Examples include the group that orchestrated the takedown of the notorious and disreputable hosting provider, McColo, the Conficker Working Group, formed to address concerns about the Conficker worm, the Cooperative Cyber Defense Centre of Excellence sponsored by NATO, and non-profit grass roots organizations like the Anti-Phishing Working Group and StopBadware.org. Experts are also advocating a “neighborhood watch” approach to increase research and findings on bad actors in the interest of creating a knowledge base that will help task forces combat cybercrime.

In addition to task forces, standards have been established to help enforce data security. Developed by the Payment Card Industry (PCI), PCI standards promote vigilance through established controls to regulate security. The standards apply to organizations that process credit card information; however, they do not always protect consumers. Several weaknesses within the standards, such as limited encryption requirements, have inspired criticism within the security community.

Although PCI compliance improves security, it is considered a first step only and most experts agree that more protections are needed going forward to safeguard data.

Technology solutions can also be implemented to combat data-stealing malware. For example, Trend Micro Smart Protection Network provides multilayered threat protection that blocks malware in the Internet cloud before it has a chance to infiltrate the network. The Intrusion Defense Firewall provides an additional layer of protection at the endpoint through network-level Host Intrusion Prevention System (HIPS). Additional tools, such as Trend Micro LeakProof™ extend additional broad protections at the endpoint to prevent data leakage within companies.

Despite the growth of data-stealing malware, best practices can help both consumers and businesses to combat this growing problem. Consumers are advised to install firewalls and reputable antivirus software and to keep them up to date. Applications software and operating systems should also be updated and patched regularly. Consumers are also advised not to open unknown attachments or to click on suspicious web links, especially if sent from someone unknown. Social networking sites provide an additional avenue for infection so consumers are advised to use strict privacy settings in those sites and to be vigilant about passwords on these and other sites. In addition, one cannot assume that social networking email or email sent by "friends" is legitimate. Often cybercriminals will pose as a friend on these sites to gain the trust of victims. Consumers should also reconsider divulging personal information online and consider storing personal information offline. Gamers are advised not to publish an IP address on other rites. Finally, turning the computer off when not in use and performing regular back-ups as a protection are also sound advice.

> "Data-stealing malware serves the needs of financially motivated criminals who leverage the Internet for what it does best—provide valuable information."
>
> Jamz Yaneza, Threat Research Manager, Trend Micro

Businesses are advised to follow many of the same suggestions provided to consumers with the added best practice of educating all employees about emerging threats to help boost awareness of data-stealing malware and cybercrime within an organization. Additionally, companies should set strict access policies about who can and cannot access certain information and should keep a list of the location of sensitive information and who has access to it. Use of chat, IM, and other dangerous communications channels should be limited to protect the network and roaming users should receive the same updates and security software as in-house employees. Both consumers and businesses have a responsibility to understand the danger of data-stealing malware and to adopt a careful yet comprehensive approach toward data security.

Data-stealing Malware—An Overview

As one of the most dangerous categories of web threats today, data-stealing malware showed tremendous growth in 2008 and is therefore an area of concern for consumer and business audiences alike. According to Anti-Phishing Working Group (APWG) statistics, the number of sites infecting PCs with password-stealing crimeware reached an all time high of 31,173 in December 2008—an 827 percent increase from January.[1]

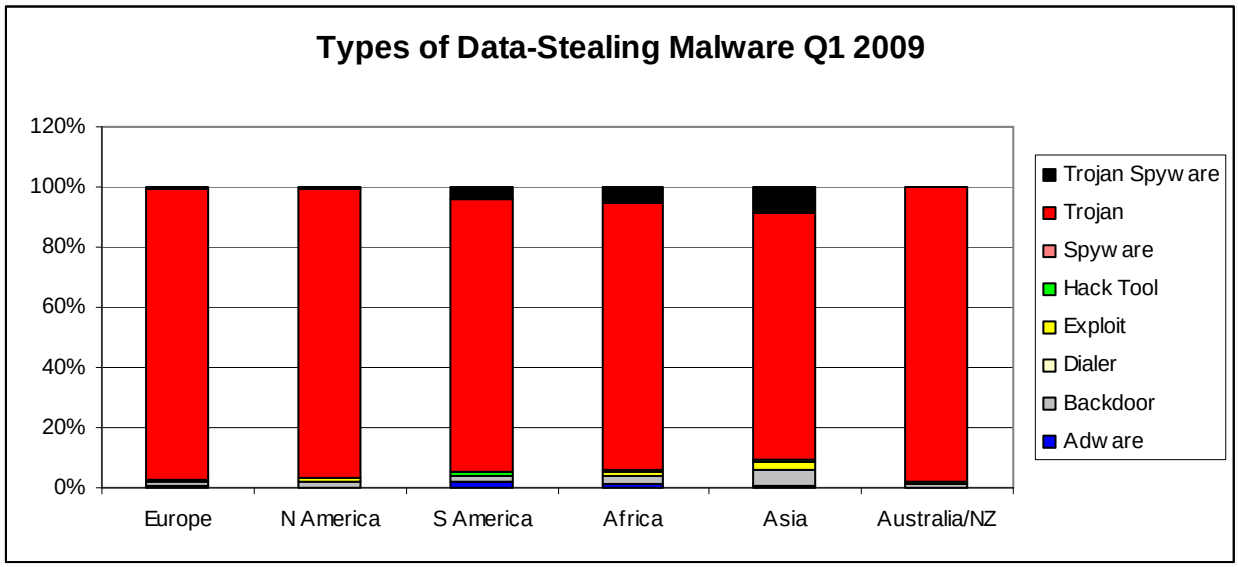

Figure 1: Trojans dominate the data-stealing malware category

Data-stealing malware is usually the second or third component of a sequential multi-pronged web attack and encompasses malware such as keyloggers, screen scrapers, spyware, adware, backdoors, or bots. According to Jamz Yaneza, Threat Research Manager for Trend Micro, "Once you open up the network, there are endless ways to steal information. Malware are created for specific purposes. Sometimes the malware are intended to steal specific sets of information or sometimes it is the beginning of a larger scale assault." These malware steal personal and proprietary information from victims for direct use or for selling in the digital underground. Says Yaneza, "As a threat category, data-stealing malware is experiencing tremendous growth because it serves the needs of financially motivated criminals who leverage the Internet for what it does best—provides valuable information."

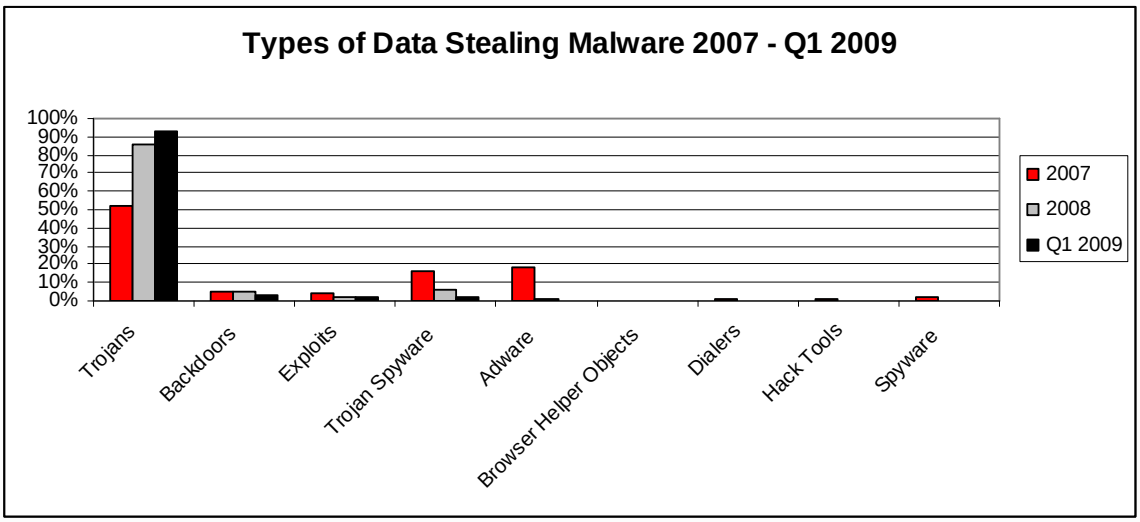

Figure 2: Trojans dominate data-stealing malware category worldwide

When targeting individual machines, cybercriminals may use spam containing malicious links to entice users to download data-stealing malware. Users can also contract data-stealing malware by visiting what appear to be innocent-looking web pages, in the process becoming infected with malware. This technique, known as "drive-by-download" is particularly insidious because it occurs transparently without the user's knowledge. After visiting infected web pages, a download initiates infection by Trojan.

Trojan attacks pose a serious threat to computer security as they typically arrive disguised as something benign such as a screen saver, game, or joke. Today's Trojan is extremely sophisticated and can be configured to send itself to everybody in an email address book, for example, or through an open IRC channel. Once a Trojan establishes a channel with a malicious remote server, it uses a wide variety of techniques to steal information. Some Trojans allow hackers to exert "remote control" over a computer by assimilating it into a botnet. Others install keyloggers that log a user's every keystroke to gather data or they insert screen scrapers that record images or screen shots showing passwords or account information. In this

way, Trojans can surreptitiously gather all the personal or sensitive information stored on a hard drive unless information is securely encrypted. Social Security numbers, credit card, and bank account numbers and administrative and gaming passwords are then up for grabs.

Trojans are the fastest growing category of malware, according to data from TrendLabs (see Figure 1). Trojans and Trojan spyware are also the predominant type of data-stealing malware in all countries monitored by TrendLabs, including Australia, Asia, Africa, South America, North America, and Europe (see Figure 2).

A Growing Problem

The same cybercriminal gangs in Russia and Eastern Europe known for botnet building and other large scale attacks regularly incorporate data-stealing malware into their arsenal of tools. In China, for example, hackers used an Internet Explorer zero-day vulnerability to steal login credentials to online gaming platforms. The black market logins were then sold online for profit. Eastern European hackers, however, would probably use the same exploit for different purposes—probably to target online banking logins and credit card information. Geopolitical motivations also exist for using data-stealing malware and differ depending upon where hackers reside.[2]

Figure 1: Fake Facebook notification

Earlier this year, three, rogue applications exploited vulnerabilities within Facebook to steal users' personal information. Users that clicked on fake notification links received malware that spammed all the user's Facebook friends, harvesting personal information along the way (see Figure 3). Although no crimes have been directly linked to the stolen information, Jamz Yaneza, Threat Research Manager at Trend Micro, theorizes that the personal information divulged on Facebook and other

social networking sites could eventually be used to hack into users' bank or credit card accounts. According to Yaneza, this trend will continue until the people who create social networking sites like Facebook make safety certification mandatory for all applications.

According to Trend Micro Senior Threat Researcher, Paul Ferguson, another recent example of data-stealing malware is the Conficker worm, which was recently in the news. Conficker, also known as Downup, Downadup, and Kido, is a worm that targets the Windows operating system and was first detected in November 2008. Once a machine is infected, the worm can download and install additional malware from attacker-controlled websites. This could include a password stealer or software to remotely control computers. Says Ferguson, "The worm was apparently designed to propagate as part of a botnet and can thus transmit data remotely if needed."

\Data Breaches and Leakages

In other cases, criminals or disgruntled employees sneak data-stealing malware onto corporate networks and then customer data or confidential company information is silently transmitted outside the network—a new twist on industrial espionage. Criminals have also become adept at exploiting open entry points that are critical to employee's productivity—like port 80 used for web surfing and web mail.

Instances of data stealing range from a single user losing personal data from a PC to thousands of records stolen in large-scale data breaches. According to Gartner, 7.5 percent of U.S. adults lost money as a result of financial fraud last year, mostly due to data breaches.[3] The most recent large-scale data breach occurred last year involving Heartland Payment Systems, one of the five largest payment processors in the U.S. The breach occurred when hackers believed to be linked to a cybercrime syndicate managed to sneak a keystroke logger onto the company's credit card

In March 2008, data from 4.2 million credit card numbers were stolen in transmission as a result of malware installed on all of Hannaford Brothers' servers in 300 stores.

processing system. Although Heartland has provided no information about how the software penetrated the network or how many card numbers were stolen, at least 160 banks in the U.S., Canada, Guam, and elsewhere are reported to have been affected. Heartland serves 250,000 business locations and conducts more than four billion business transactions per year.[4] Processing companies like Heartland will continue to be a target for cybercriminals due to the value of the data they handle. According to the 2009 Verizon Data Breach Investigations Report, 93 percent of all electronic records breaches occurred in the financial services industry and 90 percent had ties to organized crime.[5]

In July 2007, a Pfizer employee removed files from the company exposing 34,000 people to potential identity fraud and was the third data breach to occur at the company in three months. The breach disclosed the names and Social Security numbers of affected employees and also included home addresses, telephone numbers, fax numbers, email addresses, credit card and bank account numbers, and other personal information.[6]

In some instances, data breaches occur because security protections are either too lax or are missing entirely. According to Randal Vaughn, Professor of Information Systems at Baylor University, “Amazingly, companies that run their own web server do not always know what is running on it. To save money in today’s economy, many companies are outsourcing application development. An unskilled developer can easily write a web application with a vulnerability that exposes the entire network to malware. Companies must safeguard every possible access point to secure their networks.”

Dire Consequences

Consequences of data-stealing malware vary, depending upon the severity of the attacks. Consumers risk identity theft and related financial losses. A recent FTC

study found that identity theft was by far the biggest complaint to the agency, representing 26 percent of the total problems reported.[7]

Identity theft occurs when cybercriminals steal important personal information from unsuspecting consumers and then use the information to make a profit—either selling the information outright to a third party or using the data themselves to charge up credit cards or drain bank accounts. The valuable information, such as Social Security numbers, credit or bank account numbers, or driver's license numbers is then used to commit fraud. According to a study by Gartner Inc., approximately 15 million Americans were victimized by some sort of identity-theft related fraud in the 12 months ending in mid-2006. These statistics represent more than a 50 percent increase since 2003 when the Federal Trade Commission (FTC) reported 9.9 million American adult identity theft victims.[8]

Corporations suffer when confidential corporate and/or customer records are stolen, causing downtime and reduced productivity as IT teams scramble to investigate and repair the breach. When large-scale breaches occur, financial losses can skyrocket as companies incur legal costs to fight lawsuits, pay out huge settlements, then they pay again in the loss of brand image and plunging market shares. A huge attack that occurred over a three-year period against the TJX Companies (owner of TJ Maxx, Home Goods and other retail outlets) was one of the largest breaches yet reported with more than 45 million credit and debit card numbers exposed. A consumer class action suit resulted in TJX having to pay out a $200 million settlement. Reduced consumer confidence caused consequent plunging stock prices for TJX after the January 2007 attack (see Figure 4). In

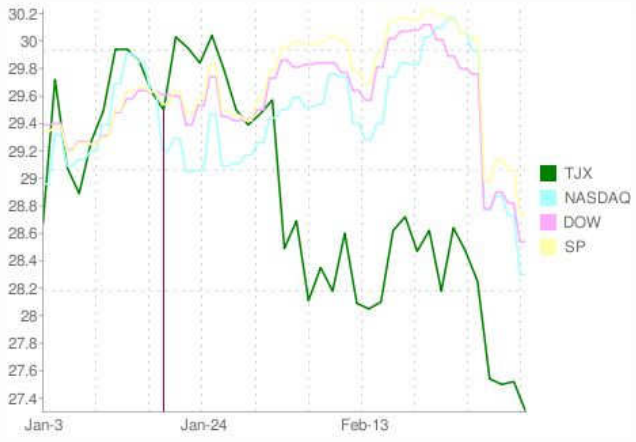

Figure 2: TJX stock price plummets after breach is announced

addition, the FTC filed official complaints against TJX alleging the retailer did not take appropriate security measures to protect consumers.

Three class action suits were filed against payment processor, Heartland Payment Systems, on behalf of all U.S. cardholders with stolen credit or debit card data in what is being called "the biggest data breach ever." The lawsuit contends that Heartland failed to adequately safeguard cardholders' data. In this case, cybercriminals used a wardriving technique to find holes in retailers' wireless networks. The criminals also installed sniffer software to capture password and account data on the stores' networks and launched SQL injection attacks to access credit card databases. To date, company officials have estimated that last year's well-publicized data breach cost the company $12.6 million. In addition to legal fees, both MasterCard and Visa fined the company for failing to demonstrate compliance to security standards at the time of the breach.

According to Paul Ferguson, Senior Threat Researcher for Trend Micro, one of the most damaging aspects of cybercrime has been the huge hit on consumer confidence, which is especially damaging in today's economy. At a time when the economy could benefit most from consumer confidence, unchecked online criminal activity is causing many consumers to turn away from using the Internet. According to its biannual Security Index Report, Unisys polled 1,000 UK citizens in April and 88 percent claimed to be worried about criminals stealing their credit card or bank account information. Unisys experts theorize that the global financial crisis has already undermined confidence in financial institutes and that the economy itself has driven the recent surge in cybercrime as criminals turn to online fraud to make money.[9]

To prove this point, a new study of online safety awareness by the Identity Theft Resource Center found that 85 percent of respondents expressed concern about the safety of transmitting information over the Internet and more than half of those asked expressed a need for improvement in data protections. Survey authors concluded

that, "It is clear that the root problem, and the cause of consumer fear in online transactions, is the concern that their information will somehow be stolen or used fraudulently."[10]

Attacks from the Inside

A study from the Ponemon Institute LLC released in March 2009 found that more than 88 percent of all data breaches involved insider negligence, while the remaining 12 percent were the result of a malicious act. The study also found that companies' costs from data breaches rose to an average $202 per record compromised in 2008, up 2.5 percent from 2007 and 11 percent from 2006.

A study from the Ponemon Institute LLC released in March 2009 found that more than 88 percent of all data breaches involved insider negligence.

Experts theorize that the well-known Hannaford Brothers grocery store chain breach that occurred in March 2008 may have been an inside job. Data from 4.2 million credit cards was stolen in transmission as a result of malware installed on all Hannaford's servers in 300 stores. Investigators discovered that the captured data was then being sent overseas. The methodologies used to install the malware and extract the data led to speculation that the Hannaford breach was an inside job as it is unlikely an outsider could have successfully distributed the correct malware to all the appropriate systems, as observed in the attack. In addition, the sophistication of the credit card interception software led investigators to believe that the criminals used prototypes to develop and test the malware prior to deployment, which would have been readily accessible to an employee.[11] Hannaford suffered greatly in the attack—both in terms of damages paid out in consumer law suits and in a tarnished brand image.

Not all data breaches are as large and widespread as the well-publicized Hannaford breach. Smaller breaches occur almost daily. For example, in April more than 15,000 students at Kapiolani Community College were exposed to identity theft

because data-stealing malware was found loaded on a computer that contained the personal information of students who had applied for financial aid. Although the computer did not itself contain sensitive data, it was connected to a network with access to names, addresses, phone numbers, birth dates, and Social Security numbers.

Cyber Terrorism

In addition to businesses and universities, government websites are also a common target for malware writers. In the U.S. alone, the number of known breaches of government computers with malware more than doubled between 2006 and 2008, according to the Department of Homeland Security.[12] For example, in January the state of Oregon lost 45 Social Security numbers to an online scammer who sent a virus to a computer at the Department of Human Services. A bogus email was used to deliver the virus and when clicked upon, downloaded a keylogger that captured and forwarded Social Security numbers to an external address.

It is possible that the U.S. electrical grid may have already been compromised by cyber terrorists who leave behind malware that would allow them to remotely disrupt service.

According to Trend Micro Senior Threat Researcher, Paul Ferguson, it is possible that cyber terrorists may have already planted malware within the U.S. electrical grid that would allow them to remotely disrupt service. Cyber terrorism is not limited to the U.S., however. In 2007, Estonian computer networks were crippled when serious distributed denial of service (DDoS) attacks against government and civilian sites were reputedly linked back to Russian operatives. DDoS attacks involve hundreds or even thousands of computers hitting a website simultaneously, therefore crashing servers and knocking sites offline. At the time, Russia and Estonia were involved in a dispute over the Estonians' removal of a Soviet war memorial. As a small, high tech country, the attacks were especially damaging as the websites of parliament, ministries, banks, the media, and other organizations were disabled.

An additional hacktivist event occurred when the French Embassy's website in Beijing was inaccessible for several days after a full-scale cyber attack following President Nicolas Sarkozy's meeting with Tibetan spiritual leader, the Dalai Lama. Although angered by the visit with the Dalai Lama, who has called for Tibetan autonomy within China, the Chinese government denied involvement in the cyber hack against France. Experts now widely believe instead that a Chinese hacking group staged the attack for nationalistic purposes.

"Virtually anyone with a computer and Internet access can wreak havoc. In the U.S., hacker attacks have been documented on county or state government sites," says Senior Threat Researcher, Paul Ferguson. "Smaller organizations have a limited IT budget and few IT staff so they hire a third party to build a website. Over time, the site fails to be maintained or upgraded, exposing vulnerabilities that hacktivists then leverage to express political views."

Cyber Espionage

Cyber espionage is an additional reason that malware is being planted on computers. Every year, U.S. corporations suffer billions of dollars in intellectual property losses when software, product designs, contracts, diagrams, drug formulations, business plans, and other trade secrets are illegally copied and sold to competitors on the black market for profit, or used for extortion. Business networks provide the perfect medium for cybercriminals capable of breaching their defenses. Large numbers of computers with high speed access make networks lucrative targets for botnet farmers recruiting "zombies." Dishonest or disgruntled employees steal intellectual property, like corporate trade secrets, email archives, or customer lists, by planting data-stealing malware from inside. According to Paul Ferguson, Senior Threat Researcher for Trend Micro, "Anyone can install malware

> "We have even seen data-stealing malware attacks against U.S. defense contractors—believed to be Chinese—launched to steal confidential trade secrets."
>
> *Paul Ferguson,* Senior Threat Researcher*, Trend Micro*

from a thumb drive within minutes and then just walk away. The data-stealing malware left behind then works silently in the background, quietly sending valuable information to crooks outside the network."

Last year an Indian infotech company lost an $8 million contract to a Chinese outsourcing firm. Upon closer examination, the Indian company discovered Chinese hackers had compromised the computers of several top executives and had used the security hole to gather information about the bid. The Chinese company then undercut the bid and landed the lucrative contract.[13] "Cybercriminals are using malware for financial gain and for geopolitical purposes," says Ferguson. "We have even seen data-stealing malware attacks against U.S. defense contractors—believed to be Chinese—launched to steal confidential trade secrets. However, it's hard to connect the dots back to the people really pulling the strings because of the anonymous nature of the Internet."

Fighting Back Against Cybercrime

Fragmented Law Enforcement

So far, attempts to stem the rising tide of cybercrime have been fragmented and largely ineffective. One of the biggest reasons is that no one organization can make a significant impact alone and few are equipped to combat online crime on a large scale. For example in the U.S., the Department of Justice, the Secret Service, the Federal Bureau of Investigation (FBI) and each state has established some sort of Internet crime agency or department, yet these groups rarely collaborate and more often work alone to solve cases that transcend state and even international boundaries. As difficult as it is to address nationwide cybercrime, international cybercrime poses an even greater challenge, particularly when crimes occur in unfriendly nations.

As cybercrime grows more common and more sophisticated, law enforcement agencies are overwhelmed and their activities grow increasingly ineffective. The sheer volume of threats makes it impossible to pursue every criminal incident involving illegal loss of data. Law enforcement agencies also lack the resources, technical skills, mandate, and in some cases, political will, to respond to each and every complaint. According to Randal Vaughn, Professor of Information Systems at Baylor University, "The remote nature of these crimes make them difficult to track the source and the tendency to cross state and country boundaries makes it incredibly difficult to prosecute. Computer crime laws vary from nation to nation and some countries do not have computer crime laws on the books."

As difficult as it is to address nationwide cybercrime, international cybercrime poses an even greater challenge, particularly when crimes occur in unfriendly nations.

Although the U.S. has several computer crime laws in place, there are few laws that directly protect consumers when their personal information has been stolen. For example, there is no federal law that requires companies that have suffered a data breach to notify affected users, customers, or employees, although several state laws exist. Some state laws require public disclosure and dictate that a breached company must notify law enforcement before notifying consumers in order to protect ensuing investigations. This can unfortunately cause a delay in disseminating information about the breach to affected consumers. In addition, although the laws require consumers to be eventually notified, companies do not have to notify consumers if the data has been shown to be encrypted.

There were two bills introduced recently to Congress that would help protect consumers from the effects of data-stealing malware and the repercussions of identity theft. Senator Dianne Feinstein (D-California) introduced Bill S.139, the Notification of Risk to Personal Data Act, which would require federal agencies or businesses to notify victims and the media when personal data has been lost—without unreasonable delay. The bill does, however, include limited exemptions for law enforcement and national security. It also dictates that the Secret Service be

notified if more than 10,000 individuals' records are stolen or if a breached database contains more than one million entries or belongs to the federal government or involves national security or law enforcement.[14] The bill is an attempt to properly inform victims of security breaches when their personal data has been compromised so they can take the appropriate steps to protect themselves.

The second bill, Bill S. 141, attempts to limit the use of Social Security numbers in the interest of promoting consumer safety. The bill prohibits federal, state, and local governments from listing Social Security numbers on online records or from printing the numbers on government checks. Additionally it would prevent inmates from employment opportunities that would allow access to Social Security numbers and places limits on businesses that request the numbers in the interest of protecting consumers.[15] Both bills were introduced after a significant increase in data breaches was reported in 2008. According to the Identity Theft Resource Center, 47 percent more breaches were reported than in 2007.[16]

In addition, two U.S. senators introduced legislation in April to create a U.S. cyber security czar who would act as the country's top official on all cyber security matters, including coordinating efforts between the government and the private sector. Although the U.S. currently has cyber security systems in place, lawmakers introduced the legislation to address America's perceived vulnerability to cybercrime, cyber espionage, and cyber attacks an as an urgent national security problem.[17]

Task Forces

Although there is no one organized group that fights cybercrime on a national or international basis, some groups are making in-roads and have achieved several successes that demonstrate the value of joining forces. For example, thanks to a group of security researchers who regularly collect data on malicious Internet activity, the plug was pulled on San Jose-based McColo Corporation—one of the world's most disreputable hosting providers. With suspected links to the Russian Business

Network (RBN) in St. Petersburg, McColo was believed to have hosted command and control infrastructure for several of the world's largest identified botnets, which were controlling hundreds of thousands of zombie PCs involved in email spam, spamvertising, malware, child porn, credit card theft, fraud, and get-rich-quick scams.

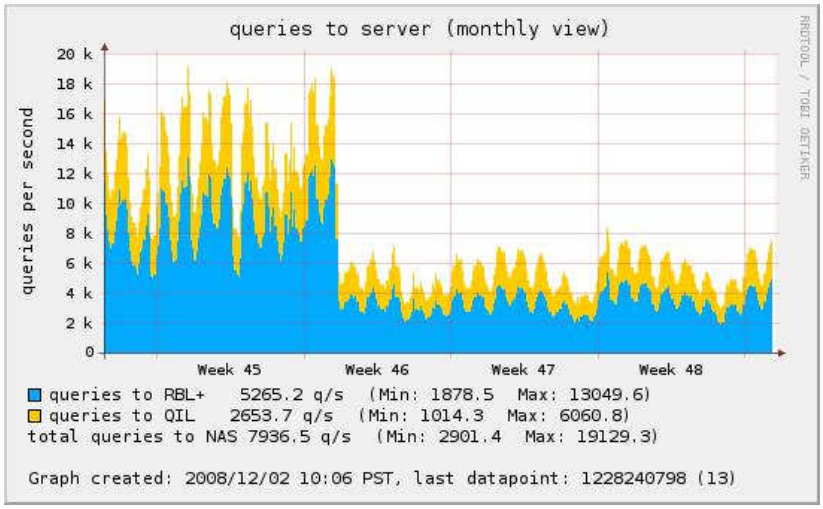

Figure 3: Trend Micro spam counts—note the drop at week 45 where the McColo shutdown occurred

McColo was finally disconnected from the Internet when years of investigation culminated in a complete shutdown, eliminating an unbelievable 50 to 75 percent of the world's junk email in a single day (see Figure 5). Trend Micro contributed research and intelligence to a report posted on HostExploit.com and a Washington Post article that detailed the criminal activity occurring inside McColo for the past two years. Advanced Threat Researcher, Paul Ferguson worked with other security researchers to compile the report, which was directly responsible for causing McColo's upstream ISPs to terminate connectivity after the information was publicized. The McColo success story is an example of what can be achieved when the security industry partners with other stakeholders to combat cybercrime.

The Conficker Working Group, a task force comprised of security researchers, Internet service providers, domain name registries, universities, law enforcement agencies, and other cross-industry stakeholders, was recently formed to combat the Conficker worm, a computer worm that targets the Microsoft Windows operating system via a combination of advanced malware techniques. Conficker is believed to have originated with the same Russian/Ukrainian cybercriminal operation believed to be behind many other profitable criminal operations such as the Russian Business

Network (RBN), Atrivo/Intercage, McColo, the Storm botnet, the Waledac botnet, rogue antivirus campaigns, and other criminal activities. So far, the Conficker Working Group has proven to be an effective, truly multi-stakeholder effort. According to Paul Ferguson, "The Conficker Working Group approach can be easily adapted for the overall cybercrime landscape."

> "The Conficker Working Group approach can be easily adapted for the overall cybercrime landscape."
>
> *Paul Ferguson,* Senior Threat Researcher*, Trend Micro*

Recently a group of NATO members, including the U.S. and Germany, established a cyber security think tank called the Cooperative Cyber Defense Centre of Excellence in an effort to prevent small bands of hackers from launching attacks that could negatively impact the world economy. The group, made up of a combination of military, technology, scientific and legal experts, analyze emerging viruses and other web threats then pass on alerts to sponsoring NATO members. They are also working to establish an alliance to help other members defend against acts of "cyber war," as differentiated from hacker mischief or cybercrime.

Additionally, the Anti-Phishing Working Group (APWG) created an initiative that includes civilian network operators and researchers who have volunteered to try to bridge the cybercrime data-sharing gap between public law enforcement, private network security, investigative intelligence, network measurement and experimentation, and related policy. The Emergent Law Enforcement Network Security Initiative (eLENS) effort promotes uniform data exchange guidelines that address the full life cycle of information flow. The effort is composed of small groups and strives to improve cooperation between law enforcement and network security professionals to clearly communicate procedures, organization and management of data. Says Randal Vaughn, Professor of Information Systems at Baylor University, "eLENS is an example of information sharing at its best. The various stakeholders in

the cybercrime arena are finally catching on that we need an organized effort to share data about cybercrime."

Similarly, StopBadware.org is a partnership among academic institutions, technology industry leaders, and volunteers committed to protecting Internet and computer users from malware threats to privacy and security. The organization is a leading independent authority on malware trends and serves as a focal point for the development of a collaborative approach to increasing security.

Many security researchers, including those at Trend Micro, advocate a community-minded, "neighborhood watch" approach, based upon reporting malicious activities when they occur. As more information sharing about data-stealing malware occurs, a public record of bad actors and malware attacks can be created to assist established task forces and other groups to help stop cybercrime. Says Paul Ferguson, "There is a growing open source effort to catalog bad actors and stop criminal activities at the source. The only way we can stop cybercrime is to hit the crooks in their pocketbooks where it hurts them the most. By shutting them down, denying them Internet access, and refusing to allow them to register false domains, we can prevent them from making money, which is the real reason that data-stealing malware exists."

PCI Standards and Limitations

The security industry enforces standards that protect data against data-stealing malware and other threats. The Payment Card Industry (PCI) sponsors the best known certification, which is critical in terms of protecting consumers from identity theft. The PCI Data Security Standard is a worldwide information security standard established by the Payment Card Industry Security Standards Council (PCI SSC) to assist organizations that hold, process, or pass credit cardholder information to prevent credit card fraud. The standards promote increased vigilance and established controls to regulate data security.

Unfortunately, the standards do not always protect consumers. In the case of the Hannaford Brothers breach, discussed earlier in this report, the company was supposedly PCI-certified the previous year and had just received recertification. The problem occurred in the manner with which the data was transmitted. PCI certification only requires encrypting data that is transmitted across an open network—typically wireless or Internet. With retail operations, data is rarely encrypted between the point of sale and the store server, which is where the Hannaford breach occurred. Retail merchants rarely encrypt data between the cash register and the store server.

According to Paul Ferguson, PCI certification features several weaknesses. In addition to limited encryption requirements and lack of database protections, PCI certification is only valuable when a network remains unchanged. Comments Ferguson, "PCI compliance does not always indicate safety or security. IT staff can make a change to the infrastructure after compliance is achieved and that single change can unwittingly expose the network to vulnerabilities. In addition, PCI compliance does not protect against an employee clicking on a malicious link, thus triggering the download of malware onto a company's network."

Discussions about broadening the encryption requirements for PCI compliance are ongoing. Some experts believe, however, that additional encryption might unnecessarily burden already hard-hit merchants with additional encryption upgrades. More important perhaps is addressing the server weaknesses that allow data-stealing malware inside the network in the first place, as well as the issue of database protection. At this point in time, PCI compliance continues to leave companies vulnerable to both insider threats and external database attacks. As the threat of data-stealing malware increases, new protections must be developed to safeguard data through all levels of the transaction lifecycle—from point of contact or sale to the final storage location for the data.

Technology Solutions

For years, security protections have been focused on protecting the endpoints—where most people access data. In today's multi-threat environment, however, Trend Micro has developed a strategy that protects the whole network, not just the endpoints. As shown in Figure 6, Trend Micro Smart Protection Network enables a multilayered threat prevention approach that is built upon the concept of proactively blocking data-stealing malware in the Internet cloud before they can infiltrate a network. In addition, the Smart Protection Network prevents data from being transmitted outside the network to combat data-stealing malware that may have been installed on the inside with the intention of transmitting data back out to malicious servers.

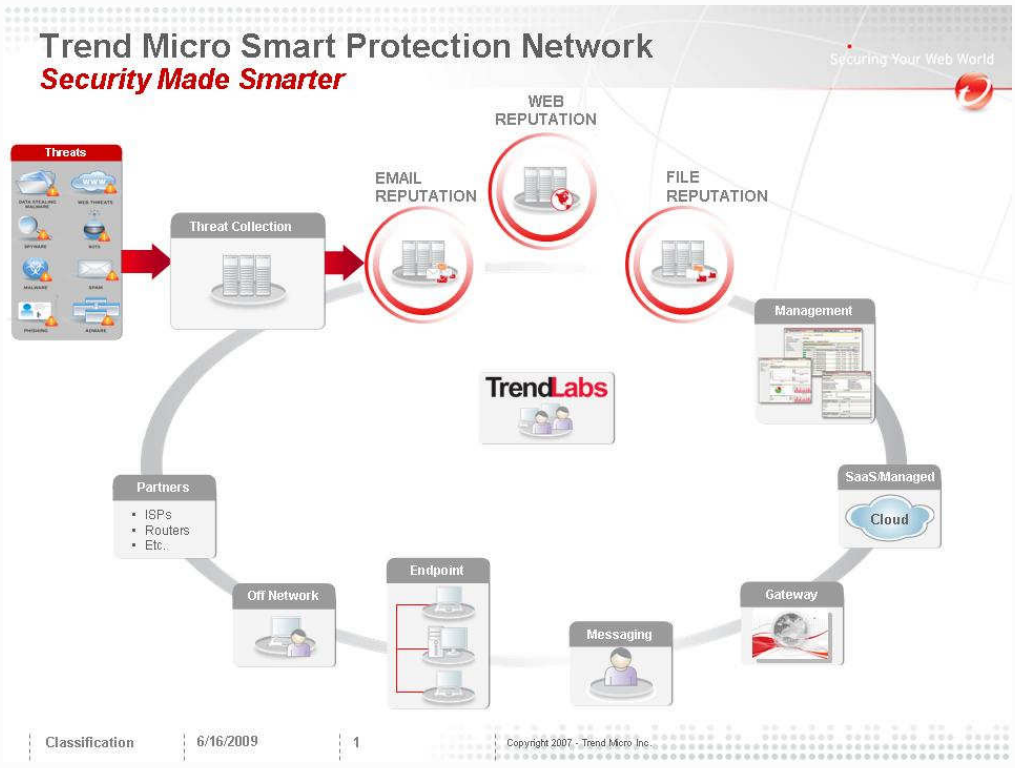

Figure 4: Trend Micro Smart Protection Network provides a technology solution that addresses today's multi-faceted attacks

The Smart Protection Network uses a correlated approach that addresses the tendency for cybercriminals today to launch multi-pronged, combined attacks composed of a number of different web threats. Using correlation technology and behavioral analysis, the Smart Protection Network correlates combinations of threat activities to evaluate their potential for danger. It analyzes email, embedded links, file attachments, and hosted web files to identify new IPs, domains, URLs, and files that can be instantly added to reputation databases to quickly block new threats. By examining the relationships between and across different components, the Smart Protection Network provides a realistic view of potential threats to deliver a holistic, comprehensive view of the threat landscape.

In addition to correlation and behavior analysis, the Smart Protection Network gathers information from behavior analysis at the gateway and loops it back into the system to provide the Web Reputation technology and database with site-threat

correlation data. The Email Reputation database composed of bad IPs and domains is also updated. In addition, endpoint information is looped back to the file scanning capability at the gateway, network servers, and the Web Reputation capability in the cloud. Both feed-through and loop-back mechanisms are used in concert to ensure real-time protection from data-stealing malware and other threats across an entire network.

Trend Micro also recently introduced an Intrusion Defense Firewall by Third Brigade that provides earlier, stronger endpoint protection by supplementing the network-level Host Intrusion Prevention System (HIPS). Trend Micro recently purchased Third Brigade to accelerate to provide customers with access to critical security and compliance software and vulnerability response services required to protect physical, virtual, and cloud servers, and corporate endpoints, from sophisticated malware and malicious attacks. A high-performance, deep-packet inspection engine monitors incoming and outgoing traffic for network protocol deviations, suspicious content that signals an attack, or security policy violations. As a plug-in for the Trend Micro anti-malware application, OfficeScan™, the Intrusion Defense Firewall is an added security measure that helps protect the endpoint against vulnerability exploits, denial of service attacks, illegitimate network traffic, and web threats.

Following Trend Micro's multilayered approach, companies can gain more control over data leaks using software tools like Trend Micro LeakProof™. LeakProof extends broad protection at the endpoint for data at rest, in use, and in motion by combining endpoint enforcement with highly accurate fingerprinting called DataDNA™. The tool also features interactive alerts that educate employees on leak prevention. The anti-leak agent provides intelligent content filtering and policy enforcement, and the DataDNA server provides policy management and violation monitoring. In this way, organizations can reduce accidental breaches and increase vigilance to protect both consumer and corporate data.

Best Practices

Best Practices for Consumers

Despite the growing prevalence of data-stealing malware due to infected web pages and spam, the following steps can help consumers minimize their exposure to these and other threats:

- **Protect your PC.**
    - Install a firewall to help block malicious Internet traffic before it reaches your computer.
    - Install an Internet security suite like Trend Micro Internet Security that includes spam filtering and blocking as well as anti-malware, anti-spyware, and malicious URL-blocking capabilities.
- **Keep your PC current with the latest software updates and patches.**
    - Apply the latest security updates and patches to your software programs and operating systems and enable automatic updates where possible. Since cybercriminals typically take advantage of flaws in software to plant malware on your PC, keeping your software current will minimize your exposure to vulnerabilities.
    - Set antivirus software to update daily, so that when it scans (either scheduled scan or real-time scan), it runs with the most recent pattern information. Do not let subscriptions expire.
- **Use caution when online.**
    - Beware of unexpected or strange-looking emails and instant messages (IMs) regardless of sender. Never open attachments or click on links in

these emails and IMs. If you trust the sender, scan attachments before opening.

- Beware of web pages requiring software installation. Scan programs before executing. Always read the end user license agreement (EULA) and cancel if you notice other programs being downloaded in conjunction with the desired program. Do not download files with .EXE extensions and refrain from downloading “free” audio and video files.
- Avoid being tricked by hidden file extensions by “unhiding” them in Windows Explorer. Select “unhide” under Tools\Folder Options\View and apply to all folders.
- Create safe passwords. Use different passwords for different websites. For example, do not use your online banking password for your social networking accounts.
- Check default privacy settings on social networking sites and change them to increase the security of your private and personal information.

Best Practices for Businesses

For enterprises, mid-size corporations, and small businesses, Trend Micro recommends multilayered, multi-threat protection in the cloud, at the Internet gateway, and on the PC or server to combat data-stealing malware and other threats. In addition, best practices for protecting the workplace include the following:

- **Keep PCs and servers current with the latest software updates and patches.**
  - Minimize your exposure to vulnerabilities by applying the latest security updates and patches to your software programs and operating systems. Enable automatic updates where possible.
- **Protect sensitive and confidential data.**

  - Employ a date leak prevention solution, such as Trend Micro™ LeakProof™ to monitor potential information leaks at the point of use.
  - Protect customer information with encryption solutions.

- **Protect PCs, servers and networks for external and internal threats.**
  - Secure your endpoints with a comprehensive security solution that includes web, email and file reputation.
  - Ensure the protection of remote workers both on and off the network.
  - Limit chat and other potentially dangerous communications channels to prevent unnecessary protocols from entering the corporate network.
- **Establish data protection policies and educate employees.**
  - Set clear policies that dictate specifically who can access certain data to reduce data leakage. Policies should be clearly written and distributed to key employees and then enforced across the enterprise.
  - Make sure employees are aware of the ways that threats can enter their computers and how they can help lower the risk of exposure. Invite employees to learn more online at websites such as the Identity Theft Resource Center and Trend Micro's threat resource center TrendWatch.
  - Ensure that employees never provide personal or confidential information in response to unsolicited online requests. Know where all sensitive data is stored and establish clear policies on data storage.

Conclusion

As consumers face the increased risk of identity theft and as corporations lose billions of dollars per year in large-scale data breaches, clearly a new approach is needed to fight the effects of data-stealing malware and the criminal organizations

behind these attacks. To date, ad hoc efforts have been only partially effective and usually provide short-lived results. Instead, a coordinated global response involving multiple stakeholders must occur to stem the rising tide of cybercrime. Security companies, researchers, law enforcement, educators, government officials, and even consumers must band together to identify malware, share information, and disrupt the operations of criminal gangs and bot operators. Malicious activities need to be closely monitored and reported with a free exchange of information to promote a better understanding of data-stealing malware and other threats. The entire Internet community must work together to bring down the big business of cybercrime and put cybercriminals on the defensive.

About Trend Micro

Trend Micro Incorporated, a global leader in Internet content security, focuses on securing the exchange of digital information for businesses and consumers. A pioneer and industry vanguard, Trend Micro is advancing integrated threat management technology to protect operational continuity, personal information, and property from malware, spam, data leaks, and the newest web threats. Its flexible solutions, available in multiple form factors, are supported 24/7 by threat intelligence experts around the globe. A transnational company, with headquarters in Tokyo, Trend Micro's trusted security solutions are sold through its business partners worldwide. Please visit www.trendmicro.com.

---

1 Anti Phishing Working Group website, http://www.antiphishing.org.

2 Dan Goodijn, ' Data-sniffing Trojans Burrow Into Eastern European ATMs," The Register, June 3, 2009, http://www.theregister.co.uk/2009/06/03/atm_trojans/

3 Elinor Mills, "Gartner: Financial Fraud Hits 7.5 Percent of U.S. Adults," CNET News, March 3, 2009, http://news.cnet.com/8301-1009_3-10186176-83.html

4 Richard Adhikari, "Cyber Thieves Hit Payment Processor Heartland," InternetNews.com, January 21, 2009, http://www.internetnews.com/security/article.php/3797551

5 “2009 Verizon Data Breach Investigations Report,” http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

6 “Data Security Breach at Pfizer Affects Thousands,” Information Security Magazine, September 5, 2007, http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1270736,00.html

7 Larry Dignan, “ID Theft Up, and 2—Somethings Suffer Most,” CNET News, February 27, 2009, http://news.cnet.com/8301-1009_3-10173702-83.html?tag=mncol;txt

8 “Gartner Says Number of Identity Theft Victims Has Increased More Than 50 Percent Since 2003,” Gartner website, March 6, 2007, http://www.gartner.com/it/page.jsp?id=501912.

9 Phil Muncaster, “Soaring Online Crime Hits Consumer Confidence,” Vnunet.com, April 20, 2009, http://www.vnunet.com/vnunet/news/2240628/consumer-online-fears-grow

10 “Consumers Increasingly Concerned About Online Transactions,” ConsumerAffairs.com, May 26. 2009, http://www.consumeraffairs.com/news04/2009/05/online_concern.html

11 Richard Koman, “Grocery Chain Data Breach Offers Lessons for CIOs,” Newsfactor.com, March 31, 2008, http://www.newsfactor.com/story.xhtml?story_id=59056

12 Paul Haven, “Cyber-Spy vs. Cyber-Spy,” TechNewsWorld.com, April 12, 2009, http://www.technewsworld.com/story/viruses-malware/66782.html?wlc=1241718857

13 Joseph, Josy, “Indian InfoTech Sector Is Main Focus of Chinese Spying,” Daily News & Analysis India, December 15, 2008. http://www.dnaindia.com/report.asp?newsid=1213993&pageid=0

14 Richard Adhikari, “New Data Breach Privacy Bills in Congress,” InternetNews.com, January 9, 2009, http://www.internetnews.com/government/article.php/3795191/New+Data+Breach+Privacy+Bills+in+Congress.htm

15 Ibid.

16 “Security Breaches 2008,” Identity Theft Resource Center website, March 26, 2009, ttp://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2008.shtml.

17 Roy Mark, “Lawmakers Call for National Cyber Security Czar,” *eWeek.com*, April 1, 2009, http://www.eweek.com/c/a/Security/Lawmakers-Call-for-National-Cyber-Security-Czar-675177/.