Symantec.™

Prepared Testimony and
Statement for the Record of

Cheri F. McGuire
Vice President, Global Government Affairs & Cybersecurity Policy
Symantec Corporation

Hearing on

"The Expanding Cyber Threat"

Before the

House Committee on Science, Space, and Technology
Subcommittee on Research and Technology

January 27, 2015

2318 Rayburn House Office Building

Distinguished members of the Subcommittee, thank you for the opportunity to testify today on behalf of Symantec Corporation.

My name is Cheri McGuire and I am the Vice President for Global Government Affairs and Cybersecurity Policy at Symantec. I am responsible for Symantec's global public policy agenda and government engagement strategy, which includes cybersecurity, data integrity, critical infrastructure protection (CIP), and privacy. I lead a team of professionals spanning the U.S., Canada, Europe, and Asia, and represent the company in key policy organizations. In this capacity, I work extensively with industry and government organizations, and currently serve on the World Economic Forum Global Agenda Council on Cybersecurity as well as on the boards of the Information Technology Industry Council, the US Information Technology Office (USITO) in China, and the National Cyber Security Alliance. From 2010 to 2012 I was Chair of the Information Technology Sector Coordinating Council (IT SCC) – one of 16 critical sectors identified by the President and the US Department of Homeland Security (DHS) to partner with the government on CIP and cybersecurity. I am also a past board member of the IT Information Sharing and Analysis Center (IT-ISAC). Previously, I served in various positions at DHS, including as head of the National Cyber Security Division and US Computer Emergency Readiness Team (US-CERT).

Symantec protects much of the world's information, and is a global leader in security, backup and availability solutions. We are the largest security software company in the world, with over 32 years of experience developing Internet security technology and helping consumers, businesses and governments secure and manage their information and identities. Our products and services protect people's information and their privacy across platforms – from the smallest mobile device, to the enterprise data center, to cloud-based systems. We have established some of the most comprehensive sources of Internet threat data in the world through our Global Intelligence Network, which is comprised of millions of attack sensors recording thousands of events per second, and we maintain 10 Security Response Centers around the globe. In addition, we process billions of e-mail messages and web requests across our 14 global data centers. All of these resources allow us to capture worldwide security data that give our analysts a unique view of the entire Internet threat landscape.

The cyber headlines of the past year have focused largely on massive data breaches, but that is just one corner of the cyber threat landscape. In my testimony today, I will discuss:

- Some common types of attacks;
- Methods attackers use to compromise systems;
- Partnering to fight cybercrime; and
- How individuals and organizations can protect themselves.

The Current Cyber Threat Landscape

Most of the recent headlines about cyber attacks have focused on data breaches across the spectrum of industries. Sadly, breaches have become an all too common occurrence, impacting not only those breached but also creating geo-political challenges for governments around the world. The organizations that suffered significant breaches over the past year include a "who's who" of the business world: Target, Michael's, Home Depot, The New York Times, and Sony are just a sampling of recent victims.

The theft of personally identifiable information (PII) in this timeframe was unprecedented. According to our most recent Internet Security Threat Report (ISTR), over 550 million identities were exposed in 2013, and eight different breaches exposed 10 million identities or more. We expect that our final statistics from 2014 will be similarly alarming. Interestingly, the Online Trust Alliance just released a report that found that 90% of last year's breaches could have been prevented if businesses relooked at their cyber risk strategies and implemented basic cyber best practices.[1]

While the focus on these public breaches and the identities put at risk is certainly warranted, it is important not to lose sight of the other types of cyber activity that are equally concerning and that can also have dangerous and broad consequences. There are a wide range of tools available to the cyber attacker, and the attacks we see today range from basic confidence schemes to massive denial of service attacks to sophisticated (and potentially destructive) intrusions into critical infrastructure systems. The economic impact can be immediate with the theft of money, or more long term and structural, such as through the theft of intellectual property. It can ruin a company or individual's reputation or finances, and it can impact citizens' trust in their government.

Attackers run the gamut and include highly organized criminal enterprises, individual cybercriminals, so-called "hacktivists," and state-sponsored groups. The motivations vary – the criminals generally are looking for some type of financial gain, the hacktivists are seeking to promote or advance some cause, and the state actors can be engaged in espionage (whether traditional spycraft or economic espionage) or infiltrating critical infrastructure systems. These lines, however, are not set in stone, as criminals and even state actors might pose as hacktivists, and criminals sometimes will offer their skills to the highest bidder. Attribution has always been difficult in the cyber landscape, and is further complicated by the ability of cyber actors to mask their motives and objectives through misdirection and obfuscation.

Common Types of Attacks

Distributed Denial of Service ("DDoS")

Distributed denial-of-service (DDoS) attacks attempt to deny service to legitimate users by overwhelming the target with activity. The most common method is to flood a server with network traffic from multiple sources (hence "distributed"). These attacks are often conducted through "botnets" – armies of compromised computers that are made up of victim machines that stretch across the globe and are controlled by "bot herders" or "bot masters."[2] One recent study found that over 60% of traffic on the internet today is from bots.[3]

DDoS attacks have grown larger year over year and in 2014 some attacks reached 400 Gigabits per second, a previously unimaginable volume of data. This is roughly equivalent to blasting a network every second with the data stored on more than 10 DVDs. In the past few years we have seen attacks go from the equivalent of a garden hose to a fire hose to the outflow pipes of the Hoover dam. Even the most prepared networks can buckle under that volume of data the first time it is directed at them, which is why even some of the country's biggest financial institutions initially suffered outages from recent DDoS attacks. In addition to increasing in volume, the attacks are getting more sophisticated and varying the methods used, which makes them harder to mitigate. In particular, in 2014 attackers used new techniques to amplify the strength of an attack which made it easier for even the "average" attack to reach levels of volume that were unthinkable just years before.[4]

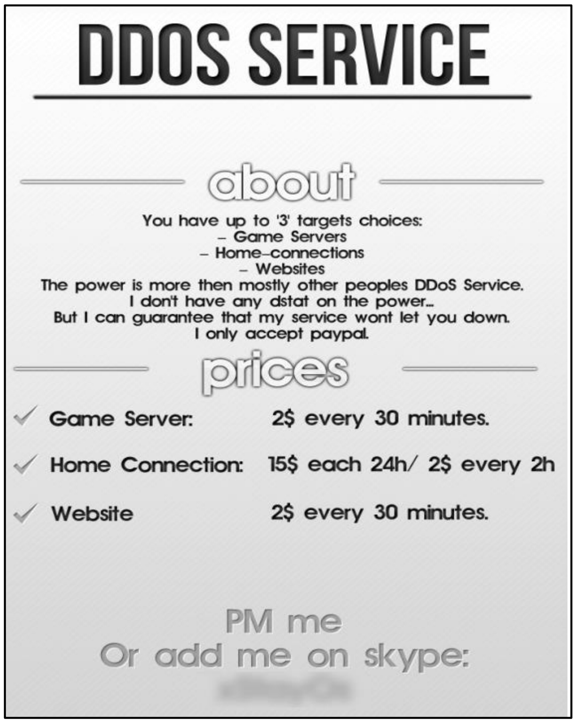
[1] https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented

[2] "Bots and Botnets – A Growing Threat," *Symantec,* http://us.norton.com/botnet/

[3] Igal Zeifman, "Report: Bot Traffic is up to 61.5% of all Website Traffic," *Incapsula*, December 9, 2013, http://incapsula.com/blog/bot-traffic-report-2013.html.

[4] Symantec, "*Security Response: The Continued Rise of DDoS Attacks,*" October 21, 2014, Pg. 25.

According to a survey by Neustar, 60% of companies were impacted by a DDoS attack in 2013 and 87 percent were hit more than once.[5] The most affected sectors were the gaming, media, and software industries. The purpose of most attacks is to disrupt, not to destroy. Cybercriminals can rent DDoS attack services on the black market for as little as $5, allowing them to conduct a short, minutes-long DDoS attack against any chosen target (fig. 1).[6] If successful, even such a short attack is enough to garner attention – or to distract an organization's security team, as another recent use of DDoS attacks has been to provide cover for other, more sophisticated attacks. Organized crime groups have been known to launch DDoS attacks against banks to divert the attention and resources of the bank's security team while the main attack is launched, which can include draining customer accounts or stealing credit card information.



DDOS SERVICE

about

You have up to '3' targets choices:
- Game Servers
- Home-connections
- Websites
The power is more then mostly other peoples DDoS Service.
I don't have any dstat on the power...
But I can guarantee that my service wont let you down.
I only accept paypal.

prices

✓ Game Server:	2$ every 30 minutes.
✓ Home Connection:	15$ each 24h/ 2$ every 2h
✓ Website	2$ every 30 minutes.

PM me
Or add me on skype:
[redacted]

Fig. 1. Example of a DDoS service for hire – this one is directed at online gamers.

Targeted Attacks

Targeted attacks are another tool in the cybercriminal's tool box, and the attached graphic illustrates some common attack methods as well as the economics of cybercrime (see *Path of A Cybercriminal*, attached on page 12). Some attacks are directed at a company's servers and systems, where attackers search for unpatched vulnerabilities on websites or undefended connections to the internet. But most rely on social engineering – in the simplest of terms, trying to trick people into doing something that they would never do if fully aware of their actions. They can be targeted at almost any level, even at an entire sector of the economy or a group of similar organizations or companies. They also can target a particular company or a unit within the company (*e.g.*, research and development or finance) or even a specific person.

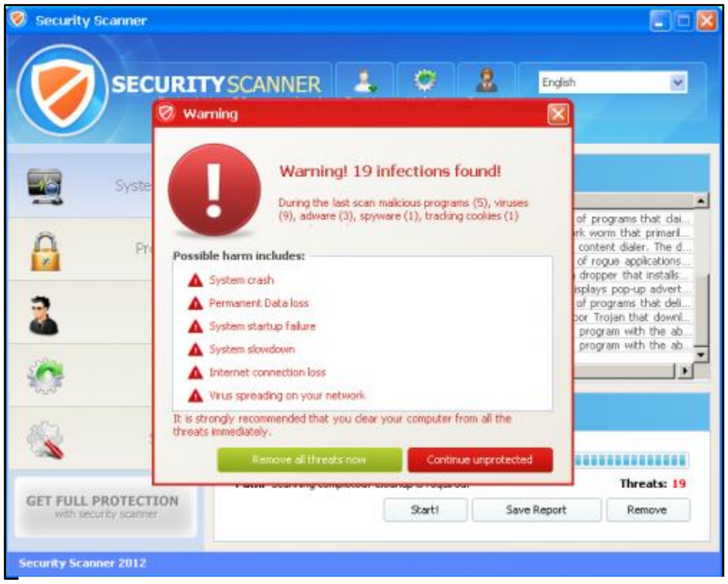
Most of the data breaches and other attacks that have been in the news were the result of a targeted attack, but the goal of the attacker can vary greatly. One constant is that after attackers select a target

[5] Neustar, "*2014, The Danger Deepens: Neustar Annual DDoS Attacks and Impact Report,*" June 2014, Pg. 3.
[6] Symantec, "*Security Response: The Continued Rise of DDoS Attacks,*" October 21, 2014, Pg. 12.

they will set out to gain access to the systems they want to compromise and once inside there are few limits on what they can do if the system is not well-protected. The malware used today is largely commoditized, and while we still see some that is custom-crafted, most of the attacks rely on attack kits that are sold on the cyber black market. But even these commodity attack kits are highly sophisticated and are designed to avoid detection – some even come with guarantees from the criminal seller that they will not be stopped by common security measures. This makes it all the more important – but also more challenging – to stay ahead of them.

Scams, Blackmail, and other Cyber Theft

Like most crime, cyber attacks are often financially motivated, and some of the most common (and most successful) involve getting victims to pay out money, whether through trickery or direct threats. One early and widely successful attack of this type was known as "scareware" (fig. 2). Scareware is a form of malware that will open a window on your device that claims your system is infected, and offer to "clean" it for a fee. Some forms of scareware open pop-ups claiming to be from major security companies (including Symantec), and if a user clicks in the window they are taken to a fake website that can look very much like that of the real company. Of course, in most cases the only infection on your computer is the scareware itself. Victims are lucky if they only lose the $20 or $30 "cost" for the fake software, but most are out much more as they typically provide credit card information to pay the scammer in the mistaken belief they are purchasing legitimate security software. Not only did they authorize a payment to the scammer, but they also provided financial information that could then be sold on the criminal underground. And by allowing the scammer to install the supposed cleaning software on their device, they give the criminal the ability to install additional malware and potentially steal more financial information or turn their system into a zombie soldier in a botnet.


Warning! 19 infections found!

During the last scan malicious programs (5), viruses (9), adware (3), spyware (1), tracking cookies (1)

Possible harm includes:

- System crash
- Permanent Data loss
- System startup failure
- System slowdown
- Internet connection loss
- Virus spreading on your network

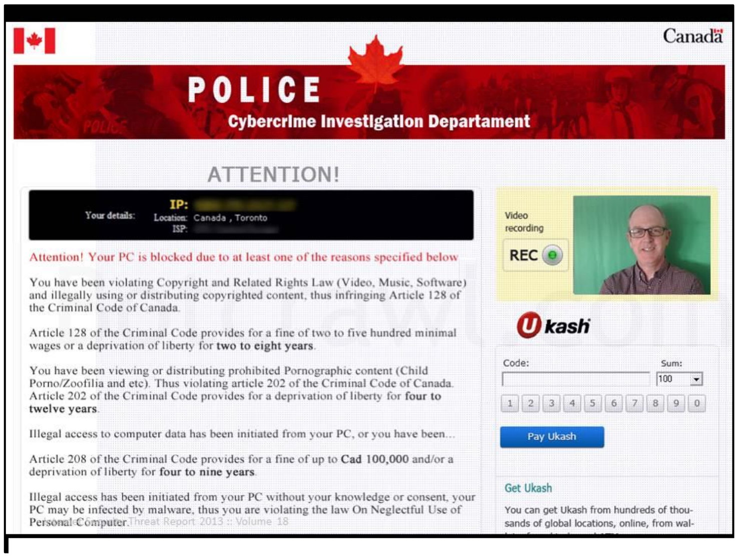
It is strongly recommended that you clear your computer from all the threats immediately.

Threats: 19

Fig. 2. An example of Scareware. The pop-ups proclaim that the victim's computer is infected, and often cannot be closed.

First widely seen in 2007, scareware began to diminish in 2011 after users became alerted to the scams and they became much less effective. Nevertheless, criminals have made millions from this type of scam.

Once scareware began to be less effective, criminals turned to "ransomware," and it has grown significantly since 2012. Ransomware is another type of deception where the malware locks the victim's device and displays a screen that purports to be from a law enforcement entity local to the user. The lock screen states that there is illegal content on the computer – everything from pirated movies to child pornography – and instructs the victim to pay a “fine” for their “crime” (fig. 3). The criminals claim that the victim’s device will be unlocked once the “fine” is paid, but in reality the device frequently remains locked. Should your device become infected, it is important to disconnect it quickly from the Internet and any other computers or devices. This will help prevent the theft of additional personal information from your computer as well as keep the infection from spreading further and stop your computer from being used as part of a botnet. Both of these types of attacks can be removed from your computer and we offer instructions and free tools on our Norton.com website to assist victims in doing so. Unfortunately, some of the more sophisticated variants can require some expertise to remediate.



Your details: IP: [redacted]
Location: Canada , Toronto
ISP: [redacted]

Attention! Your PC is blocked due to at least one of the reasons specified below

You have been violating Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article 128 of the Criminal Code of Canada.

Article 128 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for **two to eight years**.

You have been viewing or distributing prohibited Pornographic content (Child Porno/Zoofilia and etc). Thus violating article 202 of the Criminal Code of Canada. Article 202 of the Criminal Code provides for a deprivation of liberty for **four to twelve years**.

Illegal access to computer data has been initiated from your PC, or you have been...

Article 208 of the Criminal Code provides for a fine of up to **Cad 100,000** and/or a deprivation of liberty for **four to nine years**.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law On Neglectful Use of Personal Computer.

Code:

Sum: 100

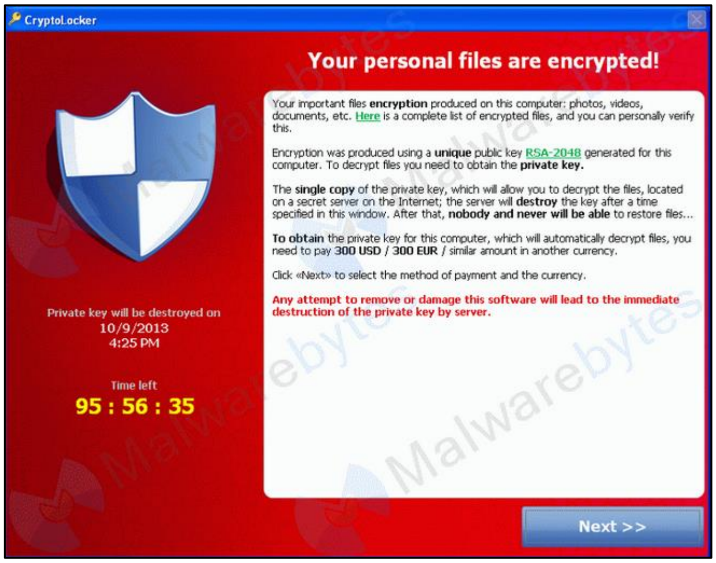
Get Ukash

You can get Ukash from hundreds of thousands of global locations, online, from wal-

Fig. 3. This ransomware targeted victims in Canada; victims in other countries would see logos of law enforcement local to them. It used built-in webcams to take a victim’s picture to further frighten them.

Unfortunately, criminals have moved beyond even ransomware and are now using a more insidious and harmful form of malware known as “ransomcrypt.” While scareware and ransomware are more classic confidence schemes, ransomcrypt is straight-up blackmail: pay a ransom or your computer will be erased (fig. 4). And unlike scareware and ransomware, there is often no easy way to get rid of it – the criminals use high-grade encryption technology to scramble the victim’s computer, and only they have the key to unlock it. Unless the system is backed up, the victim faces the difficult choice of paying the criminals or losing all the data, and there have been reports of even police departments paying to regain control of their systems.[7]

[7] John E. Dunn, "US police department pays $750 Cryptolocker Trojan ransom demand," *tech world*, November 19, 2013, http://www.techworld.com/news/security/us-police-department-pays-750-cryptolocker-trojan-ransom-demand-3489937/



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/9/2013
4:25 PM

Time left
95 : 56 : 35

Fig. 4. This is a screenshot of Cryptolocker, a sophisticated piece of ransomcrypt that was disrupted this summer by an international takedown effort, in which Symantec participated.

This is not meant to suggest that the criminals are unstoppable; in fact, in June 2014 we were part of a team that helped take down Cryptolocker. Symantec assisted the FBI and several other international law enforcement agencies to mount a major operation during which authorities seized a large portion of the infrastructure that had been used by the cybercriminals. As a result of Symantec's research into the threat, we were able to provide technical insights into their operation and impact. Since June, the Cryptolocker infection rate has dropped to near zero. But other forms are still out there, and the fight goes on.

Threats to Critical Infrastructure

Critical infrastructure such as the power grid, water system, and mass transit are also at risk. As more of these devices become connected and are controlled remotely, attackers have more opportunities to try to exploit them. In June 2014, we notified and provided detailed Indicators of Compromise (IoC) to more than 40 national computer security incident response teams around the world about a new threat we named *DragonFly*.[8] This was an ongoing cyber espionage campaign against a range of targets, mainly in the energy sector, which gave attackers control over computers that they could have used to damage or destroy critical machinery and disrupt energy supplies in affected countries. Among the targets of *Dragonfly* were energy grid operators, electricity generation firms, petroleum pipeline operators, and industrial equipment providers – the majority of which were located in the U.S., Spain, France, Italy, Germany, Turkey, and Poland. Quick and detailed notification was critical in mitigating the threat.

This was not the first campaign targeted at the energy sector. In 2012, cyber attackers mounted a campaign against Saudi Arabia's national oil firm Saudi Aramco, which destroyed approximately 30,000 computers and took its network off line for days. The infected computers were rendered unusable and displayed the image of a burning American flag. Though operations were not impacted, there was speculation in the press that oil production was the ultimate target. Shortly after the Saudi Aramco attack, a Qatari producer of liquefied natural gas, RasGas, suffered a similar attack which damaged its networks

[8] Symantec, "*Security Response: Dragonfly: Western Energy Companies under Sabotage,*" June 30, 2014. http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

and took down its website. Other sectors have seen attacks too. In the manufacturing sector, the German Government recently disclosed that a cyber attack on a steel plant resulted in the failure of multiple components and, according to one report, “massive physical damage.”[9]

In the U.S. we have yet to see major destructive attacks on critical infrastructure. However, there have been widespread reports that foreign actors have sought to gain a foothold on the networks of U.S. critical infrastructure providers.[10] And we have seen the actual compromise of one water treatment facility in South Houston, Texas (fig. 5), though the attacker did not alter any controls or settings and claimed to be trying to bring attention to the vulnerabilities that exist in critical infrastructure. This particular facility was not following security best practices and was still using default passwords that were widely known. There are undoubtedly many other critical systems that are similarly exposed.

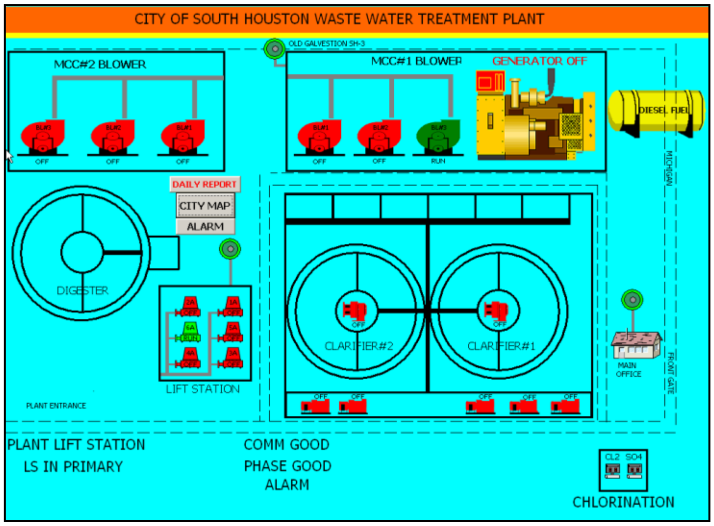


Fig. 5. Screenshot a hacker posted of the graphical user interface of the South Houston Waste Water Treatment Plant. He accessed this through use of an unchanged default user name and password.

Methods Attackers Use to Compromise Systems - Inside the Attacker’s Tool Kit

All of the attacks outlined above started with a common factor – a compromised device. From this one computer, attackers often are able to move within a system until they achieve their ultimate goal. But the threshold question is how do they get that foothold – how do they make that initial compromise that allows them to infiltrate a system?

We frequently hear about the sophistication of various attackers and about “Advance Persistent Threats” or “APTs,” but the discussion of cyber attacks – and of cyber defense – often ignores the psychology of the exploit. Most attacks rely on social engineering – in the simplest of terms, trying to trick people into doing something that they would never do if fully cognizant of their actions. For this reason, we often say that the most successful attacks are as much psychology as they are technology.

[9] SANS Industrial Control Systems (ICS), “*German Steel Mill Cyber Attack,*” December 30, 2014, Pg.1.

[10] Pierluigi Paganini, “The US energy industry is constantly under cyber attacks,” *Security* Affairs, November 14, 2014 http://securityaffairs.co/wordpress/30328/cyber-crime/cyber-attacks-energy-industry.html

Spear phishing, or customized, targeted emails containing malware, is the most common form of attack. Attackers harvest publicly available information and use it to craft an email designed to dupe a specific victim or group of victims. The goal is to get victims to open a document or click on a link to a website that will then try to infect their computers. While good security will stop most of these attacks – which often seek to exploit older, known vulnerabilities – many organizations and individuals do not have up-to-date security or properly patched operating systems. And many of these attacks are extremely well-crafted; in the case of one major attack, the spear phishing email was so convincing that even though the victim's system automatically routed it to junk mail, he retrieved it and opened it – and exposed his company to a major breach.

Social media is an increasingly valuable tool for cyber criminals in two different ways. First, it is particularly effective in direct attacks, as people tend to trust links and postings that appear to come from a friend's social media feed and rarely stop to wonder if that feed may have been compromised or spoofed. Thus, attackers target social media accounts and then use them to "like" or otherwise promote a posting that contains a malicious link. But social media is also widely used to conduct reconnaissance for spear phishing or other highly targeted attacks as it often provides just the kind of personal details that a skilled attacker can use to get a victim to let his or her guard down. The old cliché is true when it comes to cyber attacks: we have to be right 100% of the time while the attacker only has to get it right once.

Beginning in 2012, we saw the rapid growth of a new type of targeted web-based attack, known as a "watering hole" attack. Like the lion in the wild who stalks a watering hole for unsuspecting prey, cybercriminals have become adept at lying in wait on legitimate websites and using them to try to infect visitors' computers. They do so by compromising legitimate websites that their victims are likely to visit and modifying them so that they will surreptitiously try to deliver malware to every visitor. For example, one attacker targeted mobile application developers by compromising a site that was popular with them. In another case, we saw employees from 500 different companies in the same industry visit one compromised site in just 24 hours, each running the risk of infection.[11] Cybercriminals gained control of these websites through many of the same tactics described above – spear phishing and other social engineering attacks on the site managers, developers, or owners. Many of these websites were compromised through known attack vectors, meaning that good security practices could have prevented them from being compromised.

Attackers will also periodically remove malware from an infected site to avoid regular security scans that might otherwise detect the compromise. At Symantec, we constantly scan websites for vulnerabilities and our Norton Safe Web will alert customers if they are trying to connect to a site that has vulnerabilities or might try to infect their computer with malware.

Partnering to Fight Cybercrime

To assist in combating cyber threats, Symantec participates in various industry organizations and public-private partnerships with all levels of governments in the U.S. and abroad.

We share high-level cybercrime and cyber threat trends and information on a voluntary basis through a number of different fora to help protect our customers and their networks. Effective sharing of actionable information among the public and private sectors on cyber threats, vulnerabilities, and incidents is an essential component of improving cybersecurity and combatting cybercrime. In 2014, together with Palo Alto Networks, Fortinet, and McAfee we co-founded the Cyber Threat Alliance (CTA), a group of

[11] Symantec, "*Internet Security Threat Report, Volume XVIII,*" April 16, 2013, Pg. 21.

cybersecurity providers, to share threat information to improve defenses against advanced cyber adversaries. The CTA adheres to strict guidelines that protect privacy and anonymize data, while at the same time pooling a broad array of resources to fight cybercriminals.

Symantec also has a formal partnership program whereby we work with government entities around the globe to help raise awareness, mitigate threats, share cyber threat information, assist in policy development and help with training and awareness. Partnership agreements include the EUROPOL's European Cybercrime Centre (EC3), the Korean National Police Agency, AMERIPOL and the Organization of American States (OAS), among others.

Symantec also partners with a number of non-profit organizations, including the Society for the Policing of Cyberspace (POLCYB), the National Cyber-Forensics and Training Alliance (NCFTA) and InfraGard. All three organizations are excellent examples of how private industry and law enforcement can yield real world success in the areas of training, criminal investigations and threat information sharing. Through POLCYB, Symantec provides training to law enforcement around the globe. Our partnership with the NCFTA includes more than 80 other industry partners — from financial services and telecommunications to manufacturing and others — working with federal and international partners to provide real-time cyber threat intelligence to an actionable level for law enforcement to neutralize those threats.

Law enforcement and the private sector – working together – have made significant progress in recent years. Not too long ago, numerous technological, cultural and organizational barriers prevented federal agencies from coordinating with each other or with industry on the investigation and prosecution of international cybercriminals. Those barriers have largely come down, and today we see that kind of cross-agency and public-private coordination on a regular basis.

Symantec's operation to bring down the ZeroAccess botnet, one of the largest botnets in history, estimated at 1.9 million infected devices, is a good example of how effective coordination between industry and law enforcement can yield results. A key feature of the ZeroAccess botnet was that it communicates widely across all infected computers rather than from a few command and control servers out to all those infected. This "peer to peer" architecture gives the botnet a high degree of availability and redundancy since it is not possible simply to disable a few servers and bring down the botnet. Early in 2013, Symantec's engineers identified a weakness that offered a difficult, but not impossible, way to shut down the botnet. Once we began to sinkhole ZeroAccess, over half a million bots were quickly detached, and later that year Microsoft filed a civil suit against the operators of the ZeroAccess botnet. These actions appear to have put an end to the botnet and the bot masters have halted their activity. They even included the words "White Flag" in the code of one of the last updates sent to infected computers.

Another significant win came in June of last year, when the FBI and a number of international law enforcement agencies mounted a major operation against financial fraud botnet Gameover Zeus and ransomware network Cryptolocker. We worked with the FBI and a broad industry coalition during this operation, and authorities seized a large proportion of the infrastructure used by the cybercriminals behind both threats. Gameover Zeus was the largest financial fraud botnet in operation last year and is often described as one of the most technically sophisticated variants of the ubiquitous Zeus malware.

A final example is the operation that helped to bring down the Bamital botnet, a major takedown that occurred in early 2013. This effort was the culmination of a multi-year investigation conducted by a public-private partnership including Symantec, Microsoft, and law enforcement. The Bamital botnet had taken over millions of computers for criminal activities such as identity theft and advertising-related fraud, and threatened the $12.7 billion online advertising industry. This successful takedown demonstrates what can be done when private industry and law enforcement join forces to go after cybercriminal networks.

It is also important to remember the toll that cybercrime takes on its victims. Part of our effort to stop cybercrime *writ large* is to focus on individual victims. In April of last year, we partnered with the National White Collar Crime Center (NWC3) to develop an online assistance program that helps cybercrime victims better understand the investigation process and help prevent future attacks. We also make tools available to the public to assist them if their computers are part of a botnet. In addition to our Norton Security software, we do offer some free tools online that allow victims of ransomware and botnets to remove this malware from their systems (http://www.symantec.com/security_response/removaltools.jsp).

How Individuals and Organizations Can Protect Themselves

The starting point for any organization is a plan that includes both proactive security measures and reactive steps to take in the event of an attack. Strong security is layered security, and must go beyond the basics such as good computer hygiene and antivirus software. It includes comprehensive protection that includes intrusion protection, reputation-based security, behavioral-based blocking, data encryption, and data loss prevention tools. Organizations should also back up their systems regularly so that they are protected from an attack that could destroy their data. There is no such thing as 100% security, but a layered defense approach to security can significantly reduce risk and a well-thought out and regularly exercised plan can mitigate any damage that might occur.

In addition, the NIST Cyber Security Framework, developed by industry and government in 2014 and in which Symantec was an active contributor, provides a solid structure for risk management. It lays out five core cybersecurity functions (Identify, Protect, Detect, Respond and Recover) that all organizations can use to plan for managing cyber events, as well as useful references to international standards.

Good security still starts with the basics. Though criminals' tactics are constantly evolving, basic cyber hygiene is still the simplest and most cost-effective first step. Strong passwords remain the foundation of good security – on home and work devices, email, social media accounts, or whatever you use to communicate or any sites or device you log into. And these passwords must be different, because using a single password means that a breach of one account exposes all of your accounts. Using a second authentication factor (whether a smart card, biometrics, or a token with a changing numeric password) significantly increases the security of a login.

Patch management of operating systems and other software applications is also critical. Individuals and organizations should not delay installing patches, because the same patch that closes a vulnerability on one computer can be a roadmap for a criminal to exploit that vulnerability and compromise any unpatched computers. The reality is that a large percentage of computers around the world do not get patched regularly, and cyber criminals count on this. While so-called "zero days" – previously unknown critical vulnerabilities for which there is not yet a patch – get the most press, it is older, un-patched vulnerabilities that cause most systems to get compromised.

But poor or insufficiently deployed security can also lead to a breach, and a modern security suite that is being fully utilized is also essential. While most people still commonly refer to security software as "anti-virus," good security needs to be much more than that. In the past, the same piece of malware would be delivered to thousands or even millions of computers. Today, cybercriminals can take the same malware and create unlimited unique variants that can slip past basic anti-virus software. If all your security software does is check for signatures (or digital fingerprints) of known malware, you are by definition not protected against even moderately sophisticated attacks.

Modern security software does much more than look for known malware; it monitors your computer, watching for unusual internet traffic, activity, or system processes that could be indicative of malicious activity. At Symantec we also use what we call Insight and SONAR, which are reputation-based and heuristic security technologies. Insight is a reputation-based technology that uses our Global Intelligence Network to put files in context, using their age, frequency, location and more to expose emerging threats that might otherwise be missed. If a computer is trying to execute a file that we have never seen anywhere in the world and that comes from an unknown source, there is a high probability that it is malicious – and Insight will block it.

Conclusion

Citizens are increasingly aware of the cyber risk and the need to take precautions to secure their data and protect their privacy. It is important that Americans know of the risk but also understand that there are things they can do to protect themselves. Every time someone patches their computer, changes a password, or utilizes a modern security suite, he or she is making it more difficult for cybercriminals to operate. Like any other crime, cybercrime will never be completely eliminated, but it can be fought. For example, the criminals did not stop using the scareware described above because they wanted to – they quit when it stopped working, and it stopped working when the targets no longer allowed themselves to be victimized.

At all levels, both government and industry recognize the imperative for cooperation to fight cybercrime. No single company or government can “go it alone” in the current threat landscape. The threats are too complex and the stakes are too high. Ultimately, stopping cyber attacks and the criminal networks behind them requires strong technical capabilities, effective countermeasures, industry collaboration and law enforcement cooperation to be successful. At Symantec, we are committed to improving online security across the globe, and will continue to work collaboratively with international industry and government partners on ways to do so. Thank you again for the opportunity to testify, and I will be happy to answer any questions you may have.

ATTACHMENT

PATH OF A CYBERCRIMINAL

1

Hacker

A person who uses computers to gain unauthorized access to data.

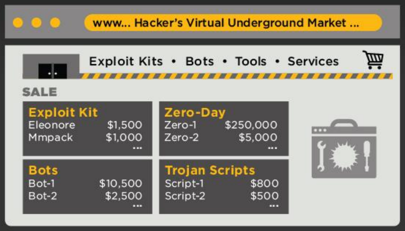
Technical Abilities

Ranges from **Novice** "Script Kiddies" (Typically youth without skill who rely on readily available code tools) **to Expert** Malware Coders

Motivations

- Money
- Risk vs. Reward
- Political

2



www... Hacker's Virtual Underground Market ...

Exploit Kits • Bots • Tools • Services

SALE

Exploit Kit	
Eleonore	$1,500
Mmpack	$1,000
	...

Zero-Day	
Zero-1	$250,000
Zero-2	$5,000
	...

Bots	
Bot-1	$10,500
Bot-2	$2,500
	...

Trojan Scripts	
Script-1	$800
Script-2	$500
	...

Hacker Shops Virtual Underground Markets

These underground markets are growing in size, complexity, are geographically spread out and are masked from the public eye with cryptographic features in the "darknet."

3 Hacker Employs Tools

Hacker uses tools to steal data such as: personal information; account information; and credit card data. Victims range from individual users to multinational companies and Governments.

4 Hacker Sells Stolen Data on Underground Market

Credit Card Information	$1.70 per unit
Bank Account Credentials	$10 to $900
E-mail Accounts	$1 to $18
Full Identities	$.67

5 Hacker Uses Money Mule to Transfer Stolen Funds

Shaving-off small percentage for self.

6

Hacker Now Has Laundered Money to Invest in More Powerful Hacking Tools

552 Million
Identities breached in 2013

$113 Billion
Direct global costs to consumers in 2013

50%
of online adults are victims of Cybercrime

26%
Average increase of cybercrime costs to companies

15 – 20%
Percentage that Cybercrime undercuts the value of the internet economy

Source from left to right: Symantec 2014 Internet Security Threat Report (ISTR); Ponemon 2013 Cost of Data Breach Study; ISTR 2014; ISTR 2014; CSIS 2014 Cybercrime Study

Infographic courtesy of Symantec.