Prepared Testimony and
Statement for the Record of

Adam Bromwich
Vice President, Security Technology and Response
Symantec Corporation

Hearing on

"Emerging Cyber Threats to the United States"

Before the

United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

February 25, 2016

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Committee, my name is Adam Bromwich and I am the Vice President of Symantec's Security Technology and Response (STAR) team. I lead a global team of engineers, researchers, and analysts who develop our security technologies, attack intelligence, and security content. My team is on the front lines of cybersecurity, identifying the latest attack patterns and campaigns, deploying protection to our customers around the clock from research centers across the globe, and working closely with law enforcement agencies to track cybercriminal groups. Prior to this role, I led the development and launch of our Insight reputation technology, a fundamentally new protection approach that leverages big data analytics and anonymous software adoption patterns from over 50 million endpoints to automatically compute safety ratings for virtually every software file and web site on the Internet. I also served as Director of Advanced Concepts, an incubator group within Symantec Research Labs, where I developed new products including the Norton Online Family child safety software. I received my Bachelor of Arts degree from Princeton University and an MBA from Yale University.

Symantec protects much of the world's information, and is the largest security software company in the world with 33 years of experience developing cybersecurity 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 cyber threat data in the world through our Global Intelligence Network, which is comprised of hundreds of millions of attack sensors recording hundreds of thousands of events per second, and more than 1,000 dedicated security engineers and analysts. We maintain nine Security Response Centers and six Security Operations Centers around the globe. Every day we scan 30 percent of the world's enterprise email traffic, and process more than 1.8 billion web requests. All of these resources combined allow us to capture worldwide security data that give our analysts a unique view of the entire cyber threat landscape.

The title of today's hearing is instructive, and I am glad to see a focus on "emerging" threats. More than perhaps any other security discipline, cybersecurity is not static. Attackers are always innovating and threats evolve quickly. Just the same, defenses cannot be static. In my testimony today, I will discuss:

- The current and emerging threat environment;
- Cutting edge technologies to counter the latest threats;
- How we work with the government to improve cybersecurity and stop criminals; and
- How we partner with our industry colleagues to counter cyber attacks.

I. The Current Cyber Threat Landscape

Many of the recent headlines about cyber attacks have focused on data breaches in government and across the spectrum of industries. Indeed, the volume of recent thefts of personally identifiable information (PII) is unprecedented – over just the past three years alone, the number of identities exposed through breaches surpassed *one billion*. Yet while the focus on data breaches and the identities put at risk is certainly warranted, we also must not lose sight of the other types of cyber attacks that are equally concerning and can have damaging consequences. There are a wide set of tools available to the cyber attacker, and the incidents 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 the Internet and their government.

While many assume that breaches are the result of sophisticated malware or a well-resourced state actor, the reality is much more troubling. According to a 2015 report from the Online Trust Alliance, 90 percent of recent breaches could have been prevented if organizations implemented basic cybersecurity best practices.[1] Moreover, some breaches are actually second generation activity – criminals leverage previously stolen personal information to compromise an individual's account.

The attackers run the gamut and include highly organized criminal enterprises, disgruntled employees, 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 (traditional spycraft or economic) 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 often offer their skills to the highest bidder. Attribution has always been difficult in cyberspace, 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]

DDoS attacks have grown larger year over year, 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 a few years ago even some of the Nation's biggest financial institutions initially suffered outages when they were victims of a DDoS campaign. In addition to increasing in volume, the attacks are getting more sophisticated and vary the methods used, which makes them harder to mitigate.

The purpose of most attacks is to disrupt, not to destroy. However, some sophisticated attackers will use a DDoS attack to distract an organization's security team while the criminals unleash a more sophisticated attack. For instance, organized crime groups have been known to initiate 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.

[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/

Targeted Attacks

Targeted attacks are increasingly common. Some are directed at a company's servers and systems, where attackers search for unpatched vulnerabilities on websites or undefended connections to the Internet. But many rely on social engineering, conning people into clicking on a link, opening a file, or taking some other action that will allow an attacker to compromise their device. The attack can be targeted at almost any level, even at an entire sector of the economy or a group of similar organizations or companies. Attacks also can target a particular company or a unit within a 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 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 target 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 the attackers.

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." 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 falsely claiming to be from major security companies (including Symantec), and if a user clicks on 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 who fall for the scam 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.

First widely seen in 2007, scareware began to diminish in 2011 after users became alerted to the scams and they became much less effective. Criminals next turned to "ransomware," which 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." The criminals claim that the victim's device will be unlocked once the "fine" is paid, but in reality the device frequently remains locked. 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.

Criminals have now moved beyond even ransomware and are 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 files will be erased. And unlike scareware and ransomware, there is often no 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. Last year one police department in Maine paid a ransom in order to regain control of its data.[3] The police chief said "[w]e needed our programs to get back online."[4] A more recent example is the compromise of the systems at Hollywood Presbyterian Hospital. Over a 10-day period, staff was forced to use pen and paper until the hospital paid the criminals a $17,000 ransom for the decryption key needed to unlock their computers. Some medical devices were reportedly off-line, wait times increased at the emergency room, and some patients were directed to other hospitals.

Emerging Threats

Attackers are constantly looking for new devices to compromise and new vectors to use to attack them, and the enormous growth of connected devices, commonly referred to as the Internet of Things or IoT, is significantly expanding the available attack surface. Last summer the remote compromise of a Jeep by a pair of security researchers received a great deal of attention, and with good reason.[5] The video of the reporter driving on the highway while unable to control the car as traffic rushed past was frightening and powerful. Receiving less attention, but equally concerning, are several alerts about vulnerabilities in drug infusion pumps that the Department of Homeland Security's Industrial Control System Computer Emergency Response Team issued over the past year.[6]

These are just two examples of vulnerabilities in connected devices, and how the explosive growth of such connections can lead to physical harm. The potential for scams and other financial fraud is just as great. We need to be prepared for ransomware targeted at a smartwatch – or a connected thermostat, refrigerator, or automobile. Criminals know that most consumers would pay a few hundred dollars in blackmail to regain control of a $50,000 vehicle that was rendered unusable by a piece of targeted malware.

Yet while the devices that could be compromised are new, many of the underlying reasons they are susceptible to attack are not. In fact, many of the new connected devices are not being built with security as a core design principle, and too many of the deployed devices are not protected or updated. Last year we released a report titled "Insecurity in the Internet of Things"[7] that analyzed 50 "smart home" devices. The findings were shocking: among other security issues, none of the devices enforced strong passwords, followed appropriate authentication protocols, or protected accounts against brute-force attacks. Almost 20 percent of the mobile apps used to control the tested IoT devices did not

---

[3] Stephanie Mlot, "Maine Police Pay Ransomware Demand in Bitcoin," *PCmag*, April 14, 2015, http://www.pcmag.com/article2/0,2817,2481356,00.asp

[4] *Id.*

[5] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway – With Me in It," *Wired*, July 21, 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[6] *See, e.g.*, https://ics-cert.us-cert.gov/advisories/ICSA-15-337-02 (January 21, 2016); https://ics-cert.us-cert.gov/advisories/ICSA-15-125-01B (June 10, 2015).

[7] https://www.symantec.com/content/dam/symantec/docs/white-papers/insecurity-in-the-internet-of-things.pdf

encrypt communications to the cloud – which means they were transmitting data in clear text across the Internet.

All of these potential weaknesses are already well known to the security industry, yet known mitigation techniques are often neglected on these devices. These findings were consistent with those of a previous report we issued in 2014, which examined security in health and fitness tracking devices, many of which transmitted data (including passwords) in clear text and failed to conduct proper authentication before connecting with outside devices or systems.[8] These devices *can* be protected, and they can be built with that in mind, but that needs to start at the design stage to lay the groundwork for strong security over the life of the device.

Another worrisome trend is the increase in destructive malware such as the one used against Sony in 2014. In the past attackers were focused on stealing data, holding it ransom, or conducting espionage. But the Sony malware did much more – it completely erased hard drives and rendered computers unusable.[9] While still the minority of attacks, we expect to see more of them in the future. This only further highlights the need for organizations to be proactive about security and to utilize modern tools to protect their systems and contain any intrusion.

Methods Attackers Use to Compromise Systems

All of the attacks outlined above started with a common factor – a compromised device. From this one device, 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 leading up to 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.

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 or software. 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.

[8] https://www.symantec.com/content/dam/symantec/docs/white-papers/how-safe-is-your-quantified-self.pdf
[9] Sean Gallagher, "Inside the "wiper" malware that brought Sony Pictures to its knees," *Ars Technica* , December 3, 2014, http://arstechnica.com/security/2014/12/inside-the-wiper-malware-that-brought-sony-pictures-to-its-knees/

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 come from a friend's social media feed (or appear to) and rarely stop to question 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. 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.

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 infect visitors or redirect them to a malicious site. 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.[10] 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.

II. Modern Security Tools

Attacks are getting more sophisticated, but so too are security tools. Security still starts with basic measures such as strong passwords or multi-factor authentication and up-to-date patch management. But while these steps may stop many older, simpler attacks, they will be little more than a speed bump for even a moderately sophisticated attacker.

Real protection requires a modern security suite that is being fully utilized. To block advanced threats and zero day attacks, sophisticated machine learning and advanced exploit prevention technologies are necessary. These approaches are able to use automation to train a system to identify an attack, even one that has never been seen before. It is also increasingly critical to use big data analytics to evaluate global software patterns to create real-time intelligence. Today these analytics are able to identify and block entirely new attacks by evaluating how they are distributed and their relationships with other devices and other files.

Data protection is equally important, and a comprehensive security program includes data loss prevention (DLP) tools that index, track, and control the access to and movement of huge volumes of data across an organization. Perhaps most importantly, DLP tools will prevent that data from moving outside an organization. Organizations should also use encryption technology on particularly sensitive data, which renders it unreadable to anyone who does not have the specific cryptologic key.

Device-specific protections are also important. For example, in the retail world, there are tools that can be applied to point of sale systems that will virtually lock down the system and only allow it to perform those limited functions that are absolutely necessary for completing a sales transaction. In the IoT world, there are authentication, encryption, and endpoint protection tools that are designed to run on

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

small and low power devices. These tools can protect everything from a connected vehicle to the small sensors built into a bridge or that monitor critical machinery.

In short, good security does not happen by accident – it requires planning and continued attention. But criminals will always be evolving, and security must as well.

III. Public-Private Partnerships to Enhance Cybersecurity

Every day we hear about the impact of cybercrime, but we do not often hear about the many successes that law enforcement and the private sector have had in stopping these crimes and bringing these criminals to justice. Recently, we have seen a string of successful arrests and prosecutions of some of the most notorious cyber criminals in the world. In July 2015, a New York judge sentenced Alexander Yucel, the creator of the "Black Shades" Trojan to five years in prison and the forfeiture of $200,000. Yucel was swept up by the Federal Bureau of Investigation (FBI) and Europol last year along with dozens of other individuals in the US and abroad. Symantec worked closely with the FBI in this coordinated takedown effort, sharing information that allowed the agency to track down those suspected of involvement. And in June 2015, Ercan "Segate" Findikoglu, the man who prosecutors say orchestrated one of the biggest cyber bank heists in American history was extradited to the US to stand trial for stealing more than $55 million by hacking bank computers and withdrawing millions in cash from ATMs.

In fact, over the last few years we have had a number of successful takedown operations against prominent financial fraud botnets. In June of 2014, the FBI, the United Kingdom (UK) National Crime Agency, and a number of international law enforcement agencies mounted a major operation against the financial fraud botnet Gameover Zeus and the ransomware network Cryptolocker. Gameover Zeus was the largest financial fraud botnet in operation in 2014 and is often described as one of the most technically sophisticated variants of the ubiquitous Zeus malware. Symantec provided technical insights into the operation and impact of both Gameover Zeus and Cryptolocker, and worked with a broad industry coalition and the FBI during this case. As a result, authorities were able to seize a large portion of the infrastructure used by the cybercriminals behind both threats.

And in February of 2015, a Europol-led operation struck against the Ramnit botnet and seized its servers and infrastructure. Ramnit facilitated a vast cybercrime operation, harvesting banking credentials and other personal credentials from its victims. The group was in operation for at least five years and in that time evolved into a major criminal operation, infecting more than 3.2 million computers. These law enforcement operations and others have knocked out or severely curtailed the operations of some of the most prominent financial fraud groups in the world. In fact, the number of bots declined by 18 percent in 2014 compared to the previous year. In large measure, this decline is because the FBI, the Europol European Cybercrime Centre (EC3), and other international law enforcement agencies, working with Symantec and other technology companies, disrupted and shut them down.

Because cyberspace is a domain without borders, where crimes are often committed at a great distance, every device in the US is a potential border entry point, making investigation and prosecution of cybercrimes a difficult task. This reality makes international engagement on cybersecurity essential. For example, Symantec partnered with AMERIPOL and the Organization of American States to publish a report that provides the most comprehensive snapshot to date of cybersecurity threats in the Latin America and Caribbean region. The goal was to raise awareness of cybercrime issues and promote the importance of cybersecurity throughout the region as a national and economic security imperative.

Similarly, Symantec is partnering with the African Union to develop a report looking at the cybersecurity threats and trends in Africa. That report will be published later this year.

Symantec also maintains relationships in the US and around the world with international cyber response organizations and law enforcement entities including INTERPOL, EUROPOL, and dozens of national Computer Emergency Response Teams (CERTs) and police forces, by sharing the latest technological trends, the evolution of the threat landscape, and the techniques that cyber criminals use to launch attacks. Our latest partnership, signed in December 2015, is with the North Atlantic Treaty Organization (NATO), and is focused on boosting two-way threat information sharing.

IV. Private Sector Partnerships to Enhance Cybersecurity – the Cyber Threat Alliance

In 2014, Symantec, Fortinet, Intel Security, and Palo Alto Networks formed the Cyber Threat Alliance (CTA) to work together to share threat information. The goal was to better distribute detailed information about advanced attacks and thereby raise the situational awareness of CTA members and improve overall protection for our customers. Since the founding of the CTA, several contributing members have joined, including Barracuda Networks, Reversing Labs, Zscaler, and ElevenPaths (part of Telefonica). Prior industry sharing efforts were often limited to the exchange of malware samples, and the CTA sought to change that. Over the past two years the CTA has consistently shared more actionable threat intelligence such as information on zero day vulnerabilities, command and control server information, mobile threats, and indicators of compromise related to advanced threats. By raising the industry's collective intelligence through these new data exchanges, CTA members have delivered greater security for individual customers and organizations. In short, the CTA is not about one vendor trying to gain advantage — we are all contributing and sharing with the community.

It is important to note that we have done this while maintaining the privacy of all our customer data and in full compliance with our companies' respective privacy policies. At Symantec, we take very seriously our obligation to protect our customers' privacy and maintain the confidentiality of the data they choose to share with us, and our analysts are rigorous in ensuring that all shared data is anonymized. In the digital world, security and privacy are intertwined, and the CTA is operational proof that the two can complement each other.

The CTA has worked because there are minimum contribution requirements for all members. Each must share at least 1,000 samples of new Portable Executable (PE) malware per day that were not otherwise seen over the preceding 48 hours. Further, they must provide one or more additional sets of data relating either to mobile malware samples, command and control servers, or vulnerabilities. Member company analysts meet every month to exchange information and plan joint reports, and the company CEOs meet quarterly. When the group decides to work on a research paper, company analysts work together more frequently – often several times a week just before publication.

The CTA's recent research paper on the Cryptowall ransomware trojan is a good example of what high-impact information sharing can bring. Each member shared their Indicators of Compromise (IOCs) around a particular threat, filling in intelligence gaps and allowing an expanded understanding of the criminal networks and their methods of operation. In addition to the research paper, the effort led to more comprehensive protection for all of our customers.

Efforts like the Cryptowall paper, of course, require significant resources from the member companies. And while members work together on research, they also compete in the marketplace. But the CTA has shown that with the proper planning and due care for company-specific considerations, even competitors can come together and raise the security level for all Internet users.

Conclusion

The cyber threat landscape is always evolving – but so too are new security technologies. Cyber criminals will always seek new ways to compromise computers, but that does not mean they are always winning. In fact, we see attackers trying new techniques such as zero-day exploits because protection has become difficult to evade. These criminals did not invest the time and resources to develop new attack methods because they wanted too, they did it because they had too – because consumers were spotting their scams and security tools were blocking them. With cybersecurity, the old adage is true – there is no destination, just a journey. By driving up the cost of doing business for criminals we can make their journey all the more difficult and less lucrative. Symantec appreciates the Committee's ongoing interest in cybersecurity, and we look forward to continuing to work with you in the future.