



Prepared Testimony and
Statement for the Record of

Bill Wright
Director of Government Affairs, Cybersecurity Partnerships
Symantec Corporation

Hearing on

“Cyber Crime: Modernizing our Legal Framework for the Information Age”

Before the

United States Senate
Committee on the Judiciary
Subcommittee on Crime and Terrorism

July 8, 2015

226 Dirksen Senate Office Building

Chairman Graham, Ranking Member Whitehouse, and distinguished members of the Subcommittee, thank you for the opportunity to testify today on behalf of Symantec Corporation.

My name is Bill Wright and I am the Director of Government Affairs for Cybersecurity Partnerships at Symantec. In this role, I manage a number of global relationships, working extensively with industry, non-profits, and governments to counter cybercrime and improve cybersecurity. I am also responsible for Symantec's global cybersecurity partnership program, through which we partner with governments around the world to raise awareness, mitigate threats, and share cyber threat information.

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 57 million attack sensors in 157 countries, recording thousands of events per second. We maintain 9 Security Response Centers around the globe and we process 30 percent of the world's e-mail messages and nearly two billion web requests every day. 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 on data breaches, cyber espionage and cybercrime. I am pleased that the Subcommittee is again focusing attention on how industry and government can work together to disrupt these threats. In my testimony today, I will discuss:

- The size and scope of the cyber threat landscape, including botnets;
- Successful efforts to disrupt botnets and cybercrime;
- Enhancing cybersecurity through public-private partnerships; and
- Improving laws to fight cybercriminals.

The Size and Scope of the Cyber Threat Landscape

If there is one thing that can be said about the threat landscape, and Internet security as a whole, it is that the only constant is change. The scale of theft of personally identifiable information (PII) is unprecedented – over just the past three years alone, the number of identities exposed through breaches is more than *one billion*. And this is just from known breaches, as many go unreported or undetected. Data breaches touch all parts of society around the globe, from governments and businesses to celebrities and individual households. 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 recent report from the Online Trust Alliance, 90 percent of last year's breaches could have been prevented if organizations implemented basic cybersecurity best practices.¹ The Center for Internet Security describes these best practices as basic "cyber hygiene." These include creating an inventory of authorized devices, identifying and patching software vulnerabilities in a timely manner, deploying

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

strong malware defenses, backing up all systems, and utilizing data loss prevention technology to stop the unauthorized transfer of sensitive data.²

Statistics from our 2015 Internet Security Threat Report demonstrate that the cyber threats we are facing on a day-to-day basis are growing. Last year, five out of every six large companies (2,500+ employees) were targeted with spear-phishing attacks, a 40 percent increase over the previous year. Since the beginning of this year, more than 115 million identities have already been exposed, including major breaches in our government, financial, healthcare and educational sectors.³ These breaches often expose real names, birth dates, and government ID numbers. This stolen data is often sold on the black market for other criminals to exploit (See attachment 1). In addition to their value on the black market, this personal information helps facilitate future attacks by providing cybercriminals a trove of information that can help them create highly customized phishing emails. Some breaches – such as the recent intrusions at the U.S. Office of Personnel Management – also expose other highly sensitive data. While we have not seen this data for sale on the black market yet, it may just be a matter of time.

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 dangerous 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 and trade secrets. It can ruin a company or individual's reputation or finances, and it can impact citizens' trust in the Internet and their government. In some cases, cyber attacks can cause physical damage to our critical infrastructure systems and the computers that operate them.

The attackers run the gamut from highly organized criminal enterprises, disgruntled employees, individual cybercriminals, so-called "hacktivists," and state-sponsored groups. The motivations vary – from pure financial gain, to the promotion of a political cause, to espionage (traditional spycraft or economic). These boundaries, however, are not set in stone, as criminals and even state actors might pose as hacktivists, and criminals often offer their skills for hire 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.

Attackers are Moving Faster than Defenses

Vulnerabilities have always been a big part of the security picture, where operating system and browser-related patches have been critical to keeping systems secure. However, the discovery of vulnerabilities such as Heartbleed and ShellShock, and their wide-spread prevalence across a number of operating systems, brought the topic front and center. Within four hours of the Heartbleed vulnerability becoming public, Symantec saw a surge of attackers stepping up to exploit it. Advanced attackers continue to favor zero-day vulnerabilities to silently sneak onto victims' computers, and last year we saw an all-time high of 24 used in attacks. As we observed with Heartbleed, attackers moved in to exploit these vulnerabilities much faster than vendors could create patches, and users could apply them.

² <https://www.cisecurity.org/documents/CSC-MASTER-VER5.1-10.7.2014.pdf>

³ http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

Cybercriminals Are Streamlining and Upgrading Their Techniques

With the glut of personal information on the Internet and black markets, attackers continued to breach networks with highly targeted spear-phishing attacks, which increased eight percent overall. Notably, they were more refined in their targeting than the previous year, deploying fewer emails per attack campaign. Attackers also perfected their use of watering hole attacks. Like the lion in the wild who stalks a watering hole for unsuspecting prey, cyber criminals have become adept at lying in wait on legitimate websites and using them to try to infect visitors' computers. Watering hole attacks compromise legitimate websites that their victims are likely to visit and then modify the sites so that they will surreptitiously deliver malware to targeted companies.

Further complicating organizations' ability to defend themselves was the appearance of "Trojanized" software updates. Attackers identified common software programs used by targeted organizations, hid their malware inside software updates for those programs, and then waited for their targets to download and install that software – in effect, leading companies to infect themselves when they thought they were applying protective patches. Last year, 60 percent of all targeted attacks struck small- and medium-sized organizations. These organizations often have fewer resources to invest in security, and many are still not adopting basic best practices like blocking executable files and screensaver email attachments. This puts not only the businesses, but also their business partners who are often connected via computer networks, at higher risk.

Malware Volume Increases and Becomes More Sophisticated

We also saw the use of malware grow and become more sophisticated. In fact, more than 317 million new pieces of malware were created last year, meaning nearly one million new threats were released into the wild each day. Attackers are also figuring out ways to fashion their malware to avoid detection. In 2014, up to 28 percent of all malware was "virtual machine aware." Virtual Machines (VM) have become a common security tool, as potential malware can be detected, executed and analyzed without endangering the overall system. Unfortunately, this VM-aware malware can recognize that it is on a virtual machine and lie dormant until it determines that it is safe to execute. It can even transmit false data in an attempt to confuse security researchers.

Botnets – Today and into the Future

Much of the cybercrime we see today is facilitated by malicious botnets. They allow cybercriminals to exponentially increase their distribution power and provide a potent tool for any number of crimes.

A "bot" is a type of malware that allows an attacker to take control of an infected computer. Also known as "Web robots," bots are usually part of a network of infected machines, collectively known as a "botnet." These typically are made up of victim machines that stretch across the globe and are controlled by "bot herders" or "bot masters."⁴ About half of these bots are what we would call helpful bots, such as the automated web crawlers that check to see that websites are running in good order or that index and update information for search engines. The others are malicious bots.

⁴ "Bots and Botnets – A Growing Threat," *Symantec*, <http://us.norton.com/botnet/>

Botnet Uses

The uses for malicious bots are only limited by the imagination of the criminal bot master. The most common use for botnets is still for Distributed Denial-of-Service (DDoS) attacks. DDoS attacks occur when multiple infected systems are used to overload a website with traffic and render it unable to respond to legitimate requests. 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 debit and credit card information.

Another common use for botnets is creating bitcoins, commonly known as bitcoin "mining." The mining process involves compiling information from recent bitcoin transactions and performing complex mathematical computations. Any single computer would take far too long to do the calculations to provide any value, so bot masters co-opt the processing power of thousands of hijacked computers to do so, thus "mining" valuable bitcoins for the bot master. Those bitcoins can then be used to purchase even more powerful cybercrime tools on the black market.

Cybercriminals also use botnets as launch points for attacks or to amplify their own processing power and bandwidth for various criminal activities such as spam generation, malware distribution and click fraud. Bot masters also can rent out their botnets for illegal purposes and can generate hundreds of thousands of dollars by making their botnets available to other users. Harvesting information such as passwords, credit card data, intellectual property, or other confidential information from infected computers is another common use for botnets. When this information is stored on a computer that is part of a botnet, the bot master has access to all of it – in an operational sense, they "own" that device. This information is often then sold to other criminals for fraudulent use.

Efforts to Disrupt Cybercriminals

Every day we read about the impact of cybercrime, but we do not often hear about the successes that law enforcement and the private sector have had in thwarting crime 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. Earlier this month, 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. *Black Shades* was a password-stealing Trojan designed to infect computers and spy on victims through their web cameras, steal files and account information, and log victims' key strokes. Yucel was arrested by the U.S. Federal Bureau of Investigation (FBI) and Europol last year along with dozens of other individuals in the U.S. and abroad. Symantec worked closely with the FBI in this coordinated takedown effort, sharing information that allowed the agency to track down the location of the command and control infrastructure.⁵ And just two weeks ago, Ercan "Segate" Findikoglu, the man who prosecutors say orchestrated one of the biggest cyber bank heists in American history was extradited to the U.S. to stand trial for stealing more than \$55 million by hacking bank computers and withdrawing millions in cash from ATMs.⁶

⁵ <http://www.wsj.com/articles/blackshades-leader-sentenced-to-prison-1435093984>

⁶ http://www.nytimes.com/2015/06/25/business/suspect-in-55-million-atm-scheme-is-extradited-to-us.html?_r=0

We have also seen a number of successful takedown operations against prominent financial fraud botnets. In June of 2014, the FBI, the U.K. 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 last year 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 and government coalition during this case. As a result, authorities were able to seize a large portion of the infrastructure used by the cybercriminals behind both threats.⁷

In July 2014, another law enforcement operation targeted the group behind *Shylock*, another dangerous financial fraud botnet, that was designed to intercept online banking transactions and steal victims' credentials. *Shylock* was responsible for the theft of millions of dollars from victims before the U.K.'s National Crime Agency seized the command and control servers, and the domains that *Shylock* used to communicate between infected computers.⁸

And in February of this year, an operation led by Europol struck against the *Ramnit* botnet and seized its servers and infrastructure. *Ramnit* facilitated a vast cybercrime operation, harvesting banking credentials and other personal information from their victims. The group was in operation for at least five years and in that time evolved into a major criminal operation, infecting more than three 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 European Cybercrime Centre (EC3) at Europol, and other international law enforcement agencies, working with Symantec and other technology companies, disrupted and shut them down.

Unfortunately, these successes have led to the emergence of new threats, such as the *Dyre* group. In a very short time, the *Dyre* financial fraud bot has emerged as another dangerous financial Trojan, capable of defrauding customers from a range of financial institutions spanning multiple countries. *Dyre* is capable of using several different types of man-in-the-browser (MITB) attacks against the victim's web browser to steal credentials. One such MITB attack involves scanning every web page a user visited and checking it against a list of sites that *Dyre* is pre-configured to attack. If a match is found, it redirects the victim to a fake website that looks similar to its genuine counterpart. This fake website will harvest the victim's credentials before redirecting back to the genuine website.⁹

Enhancing Cybersecurity Through Public-Private Partnerships

Preventing data theft caused by bots and protecting privacy starts with basic electronic device hygiene such as having security software installed, good patch management practices, using strong passwords, and recognizing suspicious emails. But that is just the start, because as we have seen in these high

⁷ <http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network>

⁸ <http://www.symantec.com/connect/blogs/all-glitters-no-longer-gold-shylock-trojan-gang-hit-takedown>

⁹ <http://www.symantec.com/connect/blogs/dyre-emerges-main-financial-trojan-threat>

profile botnet cases, sophisticated and well-funded attackers are persistent and highly skilled. Anti-virus software (AV) should be part of any security program and will stop known malware, but it is just one element in a broad security toolbox.

Today, even moderately sophisticated malware have unique signatures and can slip past systems that are using only AV software. Thus, strong security is layered security – in addition to basic computer hygiene and AV, consumers and organizations need comprehensive protection that includes intrusion protection, reputation-based security, behavioral-based blocking, and data loss prevention tools. These advanced tools look not just for known threats, but they can check the reputation of any file that is loaded on a computer and look for other behavior that could indicate the presence of previously unknown malware.

However, even with modern security suites, there is a risk that your device or network may become compromised. If that occurs, there are a number of things Symantec is doing to assist victims of botnets and other types of cybercrime. It is important to recognize that these are not victimless crimes; at best, owners of infected computers suffer decreased functionality, and at worst they have their identities compromised and their bank accounts raided. Part of our efforts to stop botnets, and indeed cybercrime *writ large*, is helping individual victims.

In April 2014, we partnered with the National White Collar Crime Center (NWC3) to develop an online assistance program, VictimVoice.org, that helps cybercrime victims better understand the investigation process and help prevent future attacks. We also make security tools available to the public to assist them if they are infected by a botnet. For example, we offer free software that allows victims of ransomware and botnets to remove malware from their system.¹⁰

Because cyberspace is a domain without borders, where crimes are often committed at a great distance, every device in the U.S. 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 recently 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 American 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.¹¹ Similarly, Symantec is partnering with the African Union and the U.S. Department of State to develop a report looking at the cybersecurity threats and trends in Africa. That report will be published later this year.

Symantec also maintains close relationships in the U.S. 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. Among other things, we share the latest security technology trends, threats, and the techniques that cyber criminals use to launch attacks.

Private to private partnerships have also proven to be effective in fighting cybercrime. An excellent example of the private sector banding together is the establishment of the Cyber Threat Alliance (CTA). The CTA is a group of cyber security practitioners founded in 2014 by Symantec, Fortinet, Intel Security

¹⁰ http://www.symantec.com/security_response/removaltools.jsp

¹¹ <http://www.symantec.com/page.jsp?id=cybersecurity-trends>

and Palo Alto Networks who share threat information to improve defenses against advanced cyber adversaries across member companies. By sharing detailed security information, we can improve overall protection for our customers. The bulk of information sharing before the CTA was established primarily involved sharing malware samples. The CTA builds upon this foundation to combat advanced attacks by sharing more actionable threat intelligence, including data on zero day vulnerabilities, botnet command and control server information, mobile threats, and indicators of compromise related to advanced persistent threats.¹²

A Path Forward – Improving Laws to Fight Cybercriminals

Symantec welcomes the Subcommittee’s sustained interest in fighting cybercrime, and appreciates your efforts to provide additional legal tools to fight this growing threat. We believe there are several areas that Congress could act on to help fight cybercrime and strengthen cybersecurity.

First, Symantec supports amending the Computer Fraud and Abuse Act (CFAA), which is the most important law that prosecutors rely on when taking down botnets. While the CFAA has undergone some changes over the years to keep up with changing technology and evolving threats, more changes are needed. Today, laws allow courts to issue injunctions for crimes involving fraud and illegal wiretapping. Using this law, the Department of Justice has had some notable successes in shutting down botnets. However, botnets also are used for crimes such as DDoS attacks, and for stealing sensitive corporate information. In those cases, an injunction to disrupt a botnet may not be considered by a court due to limits in the existing law. Symantec supports an amendment to the CFAA that would permit judges to issue an injunction against those operating a malicious botnet. This measure would enable authorities to act quickly when a malicious botnet is putting financial or personal information at risk.

Second, we agree with the Department of Justice’s recommendation that Congress should modify the so-called “access device fraud statute”, 18 U.S.C. § 1029, to allow prosecution of offenders based in other countries who directly and significantly harm individuals or financial institutions in the U.S. This would provide prosecutors the ability to bring charges against foreign criminals that possess or sell stolen credit card numbers, regardless of whether that individual is the one that stole the information in the first place. Prosecutors need this measure in order to pursue the entire criminal chain of individuals that profit from stolen financial information, not just those who conducted the attack.

Third, international cooperation is hampered by outdated legal mechanisms. In order for governments to share cyber information on criminal investigations and prosecutions, we must still proceed through Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory – processes first developed in the 1800s – that take far too long to address the real-time nature of cybercrime. To keep pace with 21st Century threats, the MLAT process should be overhauled and streamlined.

Fourth, intrusions into the computers and systems that run our critical infrastructure are increasing in volume and becoming more sophisticated. For instance, destructive cyberattacks against a power plant or transportation systems could cripple our economy and endanger lives. Symantec supports an amendment to the CFAA that creates a violation and enhanced penalties for criminals who knowingly cause damage to a computer that controls critical infrastructure systems.

¹² <http://cyberthreatalliance.org>

Last, we should remain vigilant against new laws and regulations that are not properly considered or vetted, no matter how well meaning their intent may be. For instance, last month the Department of Commerce published a proposed rule, stemming from the Wassenaar Arrangement, that imposes strict controls on the export of certain cybersecurity items. Our concern is that, as written, the rule is so vague that it could potentially cover a wider range of cybersecurity products and processes than the Department of Commerce had originally intended. As such, the rule could inadvertently impair security research, damage U.S. security companies, and severely impair our ability to protect our customers around the world.

Conclusion

As this subcommittee knows better than most, we still face significant challenges in our efforts to fight cybercrime and take down botnets. We have made notable progress over the last year but the attackers have evolved and continue to become more sophisticated. Today, both government and industry recognize the imperative for cooperation to fight cybercrime. No single organization can “go it alone” in the current threat landscape. The threats are too complex and the stakes are too high. Ultimately, defeating criminal networks and deterring cybercrime requires strong technical capabilities, effective countermeasures, industry collaboration and smart changes to existing laws that empower law enforcement while still protecting individual rights.

At Symantec, we are committed to improving Internet security across the globe, and will continue to work collaboratively with international industry and government partners on ways to do so. I would also like to commend this subcommittee for its leadership on this important issue. Thank you again for the opportunity to testify, and I will be happy to answer any questions you may have.

Attachment 1

PATH OF A CYBER ATTACKER

1 Attacker

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

Technical Abilities

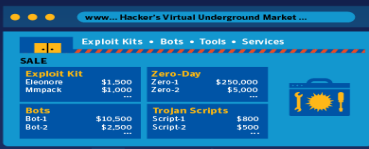
Ranges from **Novice** "Script Kiddies" (Typically youth without skill who rely on readily available code tools) to **Expert** Malware Coders

Motivations

- > Money
- > Risk vs. Reward
- > Political

2 Attacker 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."



Exploit Kits • Bots • Tools • Services			
Exploit Kit		Zero-Day	
Eleonore	\$1,500	Zero-1	\$250,000
Mimpack	\$1,000	Zero-2	\$5,000
Bots			 Trojan Scripts
Bot-1	\$10,500	Script-1	\$800
Bot-2	\$2,500	Script-2	\$500

3 Attacker Employs Tools

Attacker 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 Attacker Sells Stolen Data on Underground Market:


1,000 Stolen Email Addresses	\$.50 to \$10
Credit Card Details	\$.50 to \$20
Scans of Real Passports	\$1 to \$2
Stolen Gaming Accounts	\$10 to \$55
Custom Malware	\$12 to \$3500
1,000 Social Network Followers	\$2 to \$12
Stolen Cloud Accounts	\$7 to \$8
1 Million Verified Email Spam Mail-outs	\$.70 to \$150
Registered and Activated Russian Mobile Phone SIM Card	\$100

5 Attacker Uses Money Mule to Transfer Stolen Funds

Money Mule Shaves off small percentage for self.

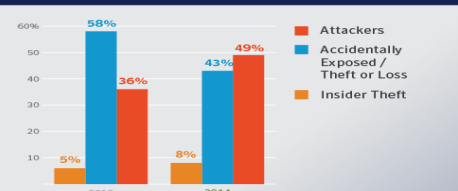


6 Attacker Now Has Laundered Money to Invest in More Powerful Hacking Tools



Top Causes of Data Breach


Source: Symantec




Year	Attackers	Accidentally Exposed / Theft or Loss	Insider Theft
2013	36%	58%	5%
2014	49%	43%	8%

Total Breaches


Source: Symantec



Year	Total Breaches
2014	312
2013	253



INTERNET SECURITY THREAT REPORT



Source: Symantec, 2015 Internet Security Threat Report, Volume 20
 Copyright © 2015 Symantec Corporation
 All rights reserved. Symantec, the Symantec logo, and the Internet Security Threat Report are registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries.

The 2015 Internet Security Threat Report (ISTR) provides an overview and analysis of the year in global threat activity. It is compiled using data from the Symantec™ Global Intelligence Network, which our global cybersecurity experts use to identify, analyze, and provide commentary on emerging trends in the threat landscape.

04/15-2130013