Prepared Testimony and
Statement for the Record of

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

Hearing on

"Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks"

Before the

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

July 15, 2014

226 Dirksen Senate Office Building

Chairman Whitehouse, Ranking Member Graham, and 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, Asia, and Latin America, and represent the company in key policy organizations. In this capacity, I work extensively with industry and government organizations, including serving from 2010 to 2012 as 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 also serve as a board member of the Information Technology Industry Council (ITI), the US Information Technology Office (USITO) in China, and the National Cyber Security Alliance (NCSA). 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 on massive data breaches and cyber espionage. While these are critically important issues, botnets – or networks of infected computers – are the foundation of the cyber-criminal ecosystem, and I am pleased that you again are focusing attention on how industry and government are working to disrupt them. In my testimony today, I will discuss:

- Types of botnets we are seeing and what we may see in the future;
- Efforts to disrupt botnets;
- Assistance for victims of botnets and combating cybercrime; and
- Improving government and industry cooperation.

<u>Botnets – Today and into the Future</u>

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."[1] One recent study found that over 60% of traffic on the internet today is from bots.[2] About half of these bots are what we would call helpful bots, such as the automated web crawlers

[1] http://us.norton.com/botnet/

[2] http://incapsula.com/blog/bot-traffic-report-2013.html

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, the subject of today's hearing.

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 and render it unable to respond to legitimate requests. Another recent use of DDoS attacks has been to provide cover for another, more sophisticated attack. 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 or 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. The cost to unsuspecting victims is lost productivity.

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, click fraud,[3] and data storage. 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.

Types of Botnets

The first botnets were centrally controlled – once a computer was infected, it would "call home" to a command and control (C&C) server to let the bot master know that the malware had been installed. Often, a bot master would then install additional software or otherwise solidify control over the infected device to ensure continued control over it. Much, if not all, of this activity is automated. At that point, the bot waited for further commands from its master – which could include any of the activities described above.

This centralized C&C model worked well, but had drawbacks. Though C&C servers can be hidden (and often are compromised computers themselves), they are potentially a single point of failure for a botnet. If the bot master loses control of a C&C server (or even just communications to or from the server) the whole botnet can be taken down. As a result, a growing number of botnets rely on a peer-to-peer (P2P) model, where any node in the network can act as both a client and a server. In a P2P botnet, each individual bot can distribute commands to other infected computers and as a result the network as a whole is highly resilient and resistant to takedowns.

Until now, virtually all botnets have been networks of infected laptop and desktop computers. However, in the past few years we have seen the first botnets comprised of mobile devices such as smart phones or tablets. And while the early reports of "smart" refrigerators sending spam proved to be incorrect,[4] we are seeing a major increase in compromised connected devices. As such, we fully expect that the coming "Internet of Things" will bring with it a future of "thingbots" of compromised connected devices that will range from appliances to home routers to digital video recorders – and who knows what else.

Efforts to Disrupt Botnets

Investigating and prosecuting cybercrime poses no less a challenge than does defending against cyber attacks. It is technically complex, and requires a level of expertise and training that many police agencies and prosecutors are just now beginning to develop. It is also resource intensive – the time and money required to see a case from inception through to a successful conviction is often substantial. The criminals know this, and indeed often count on it.

Despite these obstacles, 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 cyber criminals. 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 its use of P2P architecture, which gave the botnet a high degree of availability and redundancy. Since there is no central C&C server, one cannot simply disable a few servers to bring down the botnet. *ZeroAccess* was primarily designed to deliver payloads to infected computers. These payloads performed two basic functions: click fraud and Bitcoin mining, with an estimated economic impact of tens of millions of dollars lost per year. In addition, we estimated that the cost of electricity alone to operate the botnet was as much as $560,000 per day.

Early in 2013, Symantec's engineers identified a weakness that offered a difficult, but not impossible, way to disrupt the botnet. One year ago today, Symantec began to sinkhole *ZeroAccess* infections, which quickly resulted in the detachment of over half a million bots. This meant that these bots could no longer receive any commands from the bot master and were effectively unavailable to the botnet both for spreading commands and for updating or installing new revenue generation schemes.[5] Later that year Microsoft filed a civil suit in the U.S. District Court for the Western District of Texas against 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 last month, when the Federal Bureau of Investigation (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 coalition

[4] "Despite the News, Your Refrigerator is Not Yet Sending Spam," http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam

[5] "Grappling with the ZeroAccess Botnet," http://www.symantec.com/connect/blogs/grappling-zeroaccess-botnet

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.

In our view, the approach used in the *Gameover Zeus* operation was the most successful to date and should serve as a model for the future. A group of more than 30 international organizations from law enforcement, the security industry, academia, researchers, and ISPs all cooperated to identify the criminal element and technical infrastructure, develop tools, and craft messaging for users in order to collectively and aggressively disrupt this botnet. And while cyber criminals are resilient – recent reports are that a new gang is reconstituting parts of the defeated botnet – this successful model of public and private cooperation used to disrupt *Gameover Zeus* is one that can and should be repeated in the future.

A final example is the operation that helped to bring down the *Bamital* botnet, a major takedown that happened earlier this year. 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 click fraud, and threatened the $12.7 billion online advertising industry. This successful takedown is another example of what can be done when private industry and law enforcement join forces to go after cybercriminal networks.

Unfortunately, these examples highlight just how much still needs to be done. For while *ZeroAccess*, *Gameover Zeus*, and *Bamital* were successes for law enforcement and industry there are undoubtedly more – and likely larger – criminal rings operating today. The small number of successful cases such as these is not because governments do not want to pursue them, or because the criminals are not out there. The investigators and prosecutors are willing, and the private sector is eager to help. There are simply not enough resources – investigators, prosecutors, and judges – who can handle them. Put simply, as criminals migrate online, the FBI, the Secret Service, and state and local law enforcement agencies need more skilled personnel dedicated to fighting cybercrime.

Assisting Victims of Botnets and Combating Cybercrime

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

Today, even moderately sophisticated pieces of 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 call out 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) on a new online assistance program to help victims file cybercrime complaints and to better understand the overall investigation process. I would like to thank Senator Whitehouse for your participation in the launch and support of the VictimVoice (victimvoice.org) initiative. Symantec also makes software available to the public as a whole (beyond our Norton Security customers) to assist them if they are infected by a botnet. For example, we offer free cleaning tools that allow victims of botnets and ransomware to remove malware from their system.[6]

Symantec is also active in organizations working to raise awareness and provide resources to fight botnets, including the Online Trust Alliance (OTA). The OTA works with the public and private sectors to address the threats resulting from botnets, and has created a multi-stakeholder botnet taskforce to take a holistic look at the botnet problem, including prevention, detection and remediation. Last year, through OTA, we contributed to the development of comprehensive guidelines for botnet remediation.[7] These guidelines have been used widely and reflect the best practices from a broad array of industry stakeholders. The OTA's other efforts include working with law enforcement, ISPs and web hosting companies in takedown efforts, promoting best practices to reduce the distribution of bots, and aiding users to reduce their vulnerabilities.

Another effort is the Industry Botnet Group (IBG) which was formed in January 2012 and was comprised of a group of companies, trade associations, and non-profit organizations concerned about the adverse impact of botnets. Established in response to a U.S. Department of Commerce request for information on ways to combat botnets, the group developed a set of principles to thwart botnets and encouraged voluntary efforts by government, industry, and users to raise awareness and reduce the effectiveness of botnets.

To combat cybercrime more broadly, Symantec participates in a number of public-private partnerships in the U.S. and abroad. As demonstrated in the botnet cases described above, we voluntarily share high-level cybercrime and cyber threat information through a number of different fora to help protect our customers and their networks. Of course, all of this is done in keeping with both our own strict privacy policies to protect our customer data, and all applicable privacy laws.

Some of our key partners in these areas are the National Cyber-Forensics and Training Alliance (NCFTA), InfraGard, and INTERPOL. The NCFTA is a good example of how private industry and law enforcement partnerships can yield real world success. The NCTFA is a Pittsburgh-based organization that includes more than 80 industry partners – from financial services to telecommunications to manufacturing – working with federal and international law enforcement partners to provide real-time cyber threat intelligence to an actionable level in order to identify threats and actors.

InfraGard, of which Symantec serves on the National Board of Advisors, is another example of how law enforcement can partner with both private industry and individuals to share information on cyber threats. This successful partnership between the FBI and members of the private sector is focused on intrusions and vulnerabilities affecting national critical infrastructure. Comprised of a coalition of more than 55,000 private and public sector members, InfraGard promotes ongoing dialogue and timely communication between its members and the FBI.

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

[6] See http://www.symantec.com/security_response/removaltools.jsp

[7] "Anti-Botnet Remediation Best Practices, https://otalliance.org/resources/malicious-threats

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.

Symantec also maintains relationships 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. Just last week, Symantec notified and provided detailed Indicators of Compromise (IoC) to more than 40 national CERTs around the world about a new threat we named *DragonFly*.[8] An ongoing cyber espionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims, which could have caused damage or disruption to energy supplies in affected countries. Among the targets of *Dragonfly* were energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers – the majority of the victims were located in the U.S., Spain, France, Italy, Germany, Turkey, and Poland. Quick and detailed notification was critical in mitigating the threat.

Unfortunately, both here in the U.S. and around the world, there is a critical shortage of investigators, prosecutors, and judges who are adequately trained to handle complex cybercrime cases. Recognizing this need, Symantec has a number of initiatives whereby we work with law enforcement organizations and non-profit safety groups to provide training and technical expertise, and to help facilitate global cooperation. For example, through our partnership with the National Center for Justice and the Rule of Law (NCRLJ) and the U.S. National Association of Attorneys General, Symantec has aided in training prosecutors in trying cybercrime cases as well as judges who adjudicate those cases.

This training can – and should – start when young lawyers are still in school. In March 2014, we sponsored the third annual cyber moot court competition at UCLA School of Law. The competition helps students develop their legal skills and introduces them to many of the difficult legal concepts surrounding cybercrime. Thirteen law schools sent teams to compete this year, and we hope to expand this program to reach other law schools.

Symantec also partners with international advocacy organizations, including the Canada-based Society for the Policing of Cyberspace (POLCYB), to provide training workshops to law enforcement officials and policymakers around the globe. To date, we have partnered with POLCYB and other organizations to train law enforcement officials and policy makers in more than 35 countries around the world. Last month, Symantec participated in a U.S. Department of State cybercrime workshop in Gabarone, Botswana, aimed at policy makers from the Southern Africa Development Community and other African regional organizations to raise awareness of the threats and impacts of cybercrime, including botnets.

A Path Forward – Public and Private Cooperation

Because cybercrime and botnets are a borderless problem, any effort to thwart them requires cooperation and coordination – between the government and the private sector, between governments, and within the private sector itself. In the private sector, we need to know that we can work with our government partners and with our private sector counterparts to disrupt botnets without having to look over our shoulder to

[8] "Dragonfly: Western Energy Companies Under Sabotage," http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

ensure we are not running afoul of the law. To be clear, I am not talking about a blank check – what I am saying is that consistent with privacy protections and legal parameters, we need to be able to share cyber threat information and coordinate with our peers in industry and our partners in law enforcement quickly and efficiently.

Information sharing legislation that facilitates this cooperation, *while still protecting privacy*, is needed. Too often, security and privacy are portrayed as being in opposition, but in the digital world this is a false conflict because if our data is not secure, then neither is our privacy. At Symantec we have long supported civilian-led information sharing legislative proposals – and have also worked to ensure that they include requirements that an organization minimize personally identifiable information before information is shared. Improved information sharing – and corresponding legislation – is not a panacea, but it will give us another tool to help us work together by removing a barrier that may be keeping some organizations on the sidelines of the cybercrime fight.

Resources are also an issue in going after botnets and fighting cybercrime. As stated above, there are simply not enough investigators, prosecutors, and judges with the technical knowledge and experience to keep up with the growth of these types of cases. We recognize that the FBI, Secret Service, Department of Justice, and DHS have devoted significant new resources to cybercrime and cybersecurity in recent years, but the criminals are doing the same. If we want to improve cybercrime deterrence, the government needs to invest in new resources, as well as continue to grow successful partnerships with industry.

Lastly, the law governing cybercrime needs to be modernized. In the U.S., we need to look at amending laws such as the Electronic Communications Privacy Act, which was written before most Americans had heard of email or the Internet and when mobile phones were the size of bricks. This is no less true overseas, where most nations' laws also are playing catch up with the pace of innovation and technology. Another challenge today is that in order for governments to share cyber information internationally, we must still proceed through Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory – processes first developed in the 1800s – and 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.

Conclusion

As this subcommittee knows better than most, we still face significant challenges in our efforts to take down botnets and dismantle cybercrime networks. But while there is still much work to be done, we have made progress. Today, 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, defeating the threat of malicious botnets 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. Finally, 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.