Written Testimony of
Richard Domingues Boscovich
Assistant General Counsel, Digital Crimes Unit
Microsoft Corporation

Before the
Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism

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

July 15, 2014

Chairman Whitehouse, Ranking Member Graham, and members of the Subcommittee, thank you for the opportunity to discuss Microsoft Corporation's approach to detecting and fighting botnets. We also thank you for your leadership in focusing attention to this complicated, but important topic. My name is Richard Domingues Boscovich, and I am Assistant General Counsel in Microsoft's Digital Crimes Unit.

Before joining Microsoft in 2008, I was an Assistant United States Attorney in the Southern District of Florida for 17 years, and served as director of that District's Computer Hacking and Intellectual Property Unit. I have witnessed the evolution of cybercrime since the infancy of the Internet, and botnets are among the most malicious online threats that I have ever seen. Botnets are groups of computers remotely controlled by hackers without their owners' knowledge or consent. Botnets infect millions of computers at a time and enable criminal enterprises to invade the privacy of unsuspecting victims and steal their identities and money.

To understand the devastating impact of botnets, we can look at how they affected one victim. Consider Eunice Power, a chef in the United Kingdom, who turned on her laptop one day to find a warning that she could not access her files unless she paid ransom to cybercriminals within 72 hours. When she failed to meet the deadline, all of her photos, financial account information, and other data were permanently deleted. As she later told a reporter, "[i]f someone had robbed my house it would have been easier."

Indeed, botnets conduct the digital equivalent of home invasions, on a massive scale. Botnet operators quietly hijack webcams to spy on people in their homes, and later sell explicit photographs of the unsuspecting victims on the black market. They use malicious software to log every keystroke that users enter on their computers—including credit card numbers, Social Security numbers, work documents, and personal emails. They send deceptive emails designed to appear as though they were sent by banks that convince consumers to disclose financial account information.

Botnets are exponentially more damaging—and efficient—than traditional computer viruses. Because a botnet gets stronger as it infects more computers, a single botnet allows a cybercriminal to commit tens of billions of illegal acts in a single day. For example, the Citadel family of botnets caused more than a half-billion dollars in economic damage worldwide before Microsoft helped disrupt it last year.

For more than a decade, Microsoft has partnered with other companies and global law enforcement agencies to battle such malicious cybercriminals. I am happy to be joined today by representatives of Symantec and the FBI, who are among our key partners in this battle and who have helped us disrupt some of the world's most malicious botnet operations. Today, I will tell you about Microsoft's approach to combatting botnets by disrupting their economic infrastructure, the legal and technical tactics that we use to identify and take down botnets, our approach to protecting consumer privacy while fighting botnets, the outstanding results that have come from our public-private partnerships, and lessons learned along the way.

Botnet Prevention Requires Cooperation between Law Enforcement and the Private Sector

We do not—and cannot—fight botnets alone. As the title of this hearing suggests, fighting botnets requires efforts from both the private *and* public sector. We routinely work with other companies and domestic and international law enforcement agencies to dismantle botnets that have caused billions of dollars in worldwide economic damage. In addition to the FBI and Symantec, we regularly work with a wide range of academics from institutions that include the Universities of California at Berkeley, Santa Cruz, and San Diego as well as the University of Washington. Industry partners include CSIS.DK, FireEye, F-Secure, Kaspersky, and Kyryus. Our joint efforts demonstrate that public-private partnerships are highly effective at combatting cybercrime. Moreover, we believe that public-private partnerships are essential to addressing the increasingly complex problems presented by cybercrime; no single individual or entity can tackle these problems alone.

To that end, we monitor evolving cybercrime threats and work closely with law enforcement on a number of initiatives to help devise and execute strategies that disrupt cybercrime threats targeting Microsoft technology, people, businesses, and critical infrastructure. Microsoft also supports governments and law enforcement by providing them with technical training, investigative and forensic assistance, and the continued development of new tools to combat cybercrime. Once Microsoft discovers a botnet and disrupts its network infrastructure, it works with Internet Service Providers (ISPs) and Computer Emergency Response Teams (CERTs) to rescue and clean computers from the control of the botnets.

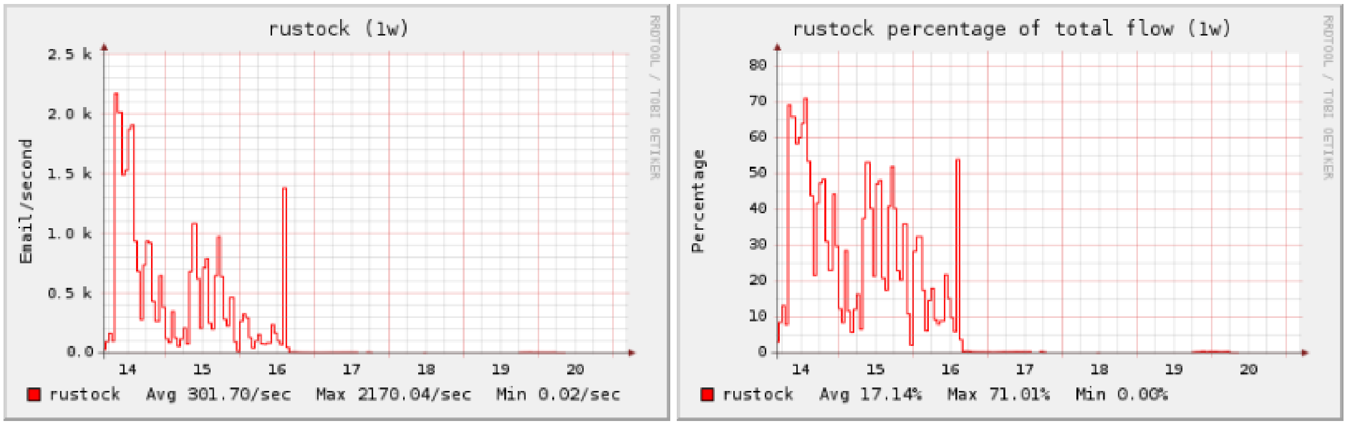
Microsoft's anti-botnet program uses the civil litigation system. We believe that civil litigation remedies, including injunctions, are appropriate and effective tools for stopping the harms caused by those who use criminal botnets to violate commercial and intellectual property laws. We also believe there is a vital role for law enforcement in this fight. While Microsoft clearly does not have access to criminal enforcement tools, we work to partner with law enforcement wherever appropriate. We also try to carefully structure our operations to ensure that we complement the efforts of law enforcement and avoid unintentionally interfering with criminal investigations or prosecutions.

Our public-private partnerships have led to significant successes. We helped to disrupt 11 botnets tied to criminal organizations committing consumer, financial, and advertising fraud, which led to the disruption of widespread criminal enterprises and the cleanup of millions of infected computers.

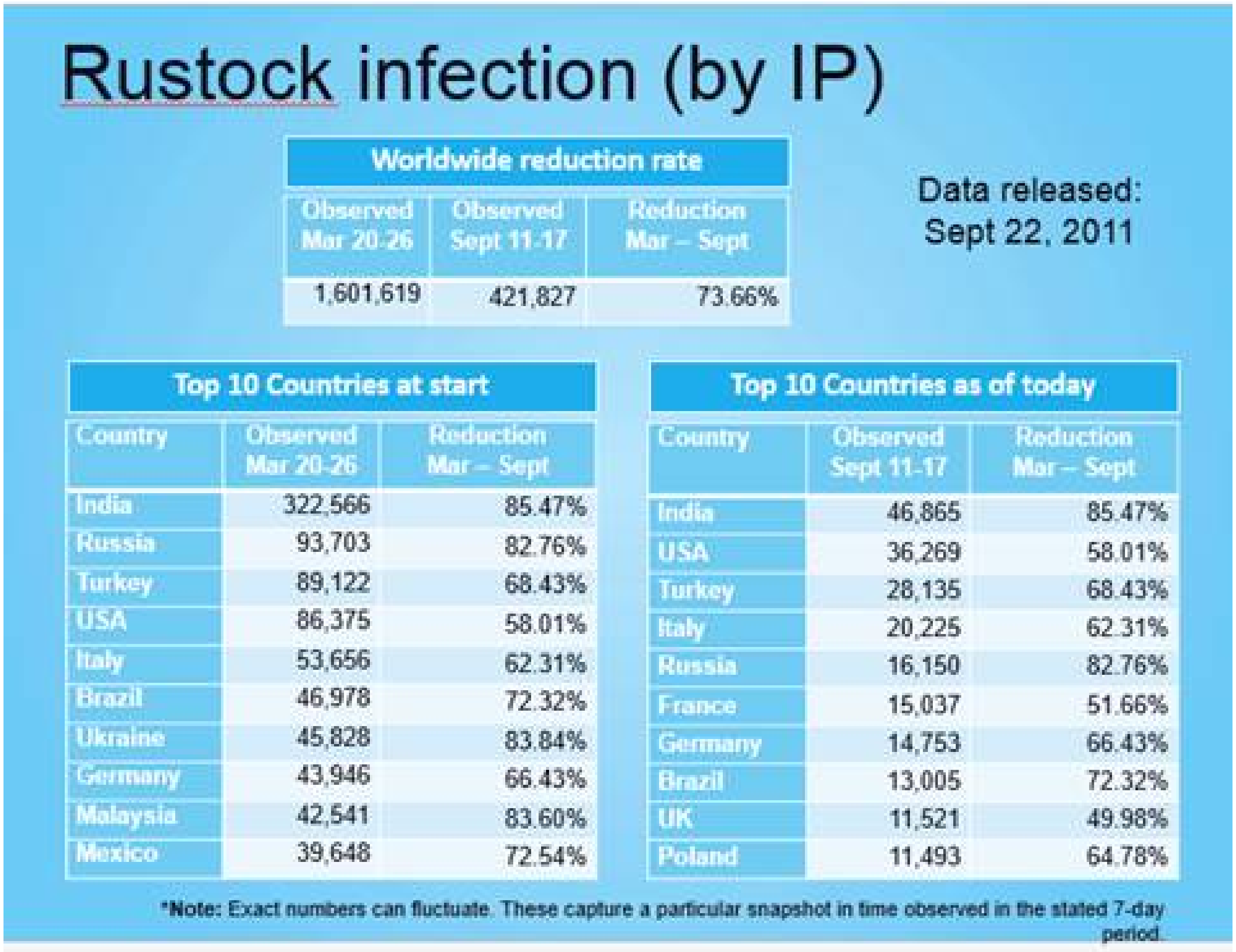
Consider the March 17, 2011 shut-down of the Rustock botnet, which at one time was responsible for approximately half of the world's spam. Microsoft worked with Pfizer, whose drugs often were the subject of Rustock spam, security experts at the University of Washington, and other law enforcement and governmental authorities, including Dutch law enforcement agencies, to dismantle this global botnet. Alex Lanstein, Senior Engineer at network security provider FireEye, said that Microsoft "did a public service" by coordinating the legal efforts to obtain control of the botnet.

The following chart shows the change in spam flow from the Rustock botnet during the week of the shut-down:

Week of Rustock Shutdown



Source: http://cbl.abuseat.org/rustock.html (visited July 11, 2014).



Rustock infection (by IP)

Data released:
Sept 22, 2011

Worldwide reduction rate		
Observed Mar 20-26	Observed Sept 11-17	Reduction Mar – Sept
1,601,619	421,827	73.66%

Top 10 Countries at start

Country	Observed Mar 20-26	Reduction Mar – Sept
India	322,566	85.47%
Russia	93,703	82.76%
Turkey	89,122	68.43%
USA	86,375	58.01%
Italy	53,656	62.31%
Brazil	46,978	72.32%
Ukraine	45,828	83.84%
Germany	43,946	66.43%
Malaysia	42,541	83.60%
Mexico	39,648	72.54%

Top 10 Countries as of today

Country	Observed Sept 11-17	Reduction Mar – Sept
India	46,865	85.47%
USA	36,269	58.01%
Turkey	28,135	68.43%
Italy	20,225	62.31%
Russia	16,150	82.76%
France	15,037	51.66%
Germany	14,753	66.43%
Brazil	13,005	72.32%
UK	11,521	49.98%
Poland	11,493	64.78%

*Note: Exact numbers can fluctuate. These capture a particular snapshot in time observed in the stated 7-day period.

Source: Microsoft

Similarly, last month, Microsoft and the FBI worked together to disrupt the GameOver Zeus botnet, which stole passwords via peer-to-peer technology, making it particularly difficult to track. Microsoft provided the FBI with technical analysis of the peer-to-peer network and developed a cleaning solution, as the FBI and Justice Department took control of the domains and filed criminal charges against the Russian hacker who led the botnet. As one reporter observed in an article about the disruption, "the biggest champion of the day may be collaboration between the feds and the private sector." It was this particular botnet that led to the theft of personal information that I described earlier in my testimony.

Disrupting Botnets' Economic Infrastructure

Microsoft's philosophy to fighting botnets is simple: we aim for their wallets. We disrupt botnets by undermining cybercriminals' ability to profit from malicious attacks.

At bottom, cybercriminals operate botnets to make money. Botnets are businesses, albeit illegal ones. Botnets are particularly attractive tools for criminals because they are cheap and effective. They have a relatively low cost of entry, the marginal cost to maintain them is low, and the potential profits grow exponentially as more computers are infected.

Microsoft has seen botnets take many forms and use a wide range of tools. But a common theme among all of them is the desire to generate a profit for the botnet operators. Consider the "business models" of the most malicious botnets:

- **Zeus** botnets, a family of financial botnets that were responsible for identity theft, caused more than $70 million in financial losses, and infected more than 13 million PCs worldwide.

- **Bamital** botnet, which hijacked people's search results, taking them to potentially dangerous websites that could install malware, steal personal information, or fraudulently charge businesses for "clicks" on online advertisements. More than 8 million computers had been attacked by Bamital in the two years prior to its takedown.

- **Nitol** botnet, which used more than 500 different strains of malware to potentially target millions of innocent people and steal their personal information, including financial account data. It was discovered as part of a Microsoft study on unsecured supply chains, which found that 20 percent of PCs purchased for analysis in China from unsecure supply chains were infected with malware.

- **Rustock** botnet, which was reported to be among the world's largest "spambots," could send up to 30 billion spam email messages per day. It infected nearly 2.5 million computers worldwide.

I am proud to report that Microsoft, in partnership with other companies and law enforcement agencies worldwide, has disrupted all of these botnets—and others—and as a result has dramatically increased their costs of "doing business." By disrupting their infrastructure, we impact the bottom-line cost-benefit equation for cybercriminals. In doing so, we seek not only to protect users from the existing botnets, but to alter the financial analysis for criminals to the point that they are discouraged from establishing new botnets.

Protecting Consumers

Microsoft draws on our deep technical and legal expertise to develop carefully planned and executed operations that disrupt botnets pursuant to court-approved procedures.

Microsoft's Digital Crimes Unit ("DCU") is a team of more than 100 technical, legal and business experts that uses creative techniques and Microsoft technology to fight cybercrime and improve cybersecurity. The DCU proactively helps Microsoft customers stay ahead of new and evolving threats and challenges. Through robust partnerships and a recognition that no one company can fight cybercrime alone, DCU plays offense against online threats.

Microsoft's work in this area dates back more than a decade. In 2003, Microsoft formed a joint legal and technical team to address cybercrime, known as the Internet Safety and Enforcement Team ("ISET"), as part of Microsoft's Trustworthy Computing initiative. In 2008, ISET evolved to become the DCU, to better align with how Microsoft was tackling the evolution of cybercrime. Last year, Microsoft opened its Cybercrime Center, combining our legal and technical expertise with cutting-edge tools and technology to mark a new era in the fight against cybercrime.

The DCU uses a combination of legal and technical tactics to help fight cybercrime. In general terms, Microsoft asks a court for permission to sever the command-and-control structures of the most destructive botnets, breaking communication lines to either the domains or Internet protocol (IP) addresses that cybercriminals use to control the botnet.

Once the court grants permission and Microsoft severs the connection between a cybercriminal and an infected computer, traffic generated by infected computers is either disabled or routed to domains controlled by Microsoft. This process, known as "sinkholing," helps Microsoft collect valuable evidence and intelligence used to help notify victims that their computers are infected, as well as clean computers to remove the malicious software. These disruptions significantly impact cybercriminals' operations and infrastructure, assists victims in regaining control of infected computers and furthers investigations against cybercriminals responsible for the threat. As we execute these court orders, we work hard to avoid disrupting legitimate Internet traffic and, where necessary, we will take steps during or after implementation of a court order to achieve that goal.

As one example, in May 2013, Microsoft worked closely with the FBI to disrupt a massive cybercrime ring associated with the Citadel botnet. As part of those efforts, Microsoft asked the United States District Court in the Western District of North Carolina to grant an emergency temporary restraining order, seizure order, and an order to show cause for preliminary injunction, to help disrupt the botnet. Microsoft argued the botnet violated a number of state and federal laws, including the Computer Fraud and Abuse Act (18 U.S.C. §1030), the CAN-SPAM Act (15 U.S.C. §7704), the Electronic Communications Privacy Act (18 U.S.C. §2701), the Lanham Act (15 U.S.C. §§ 1114), the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962), and the North Carolina Computer Trespass law (N.C. Gen. Stat. §14-458), as well as the common law torts of conversion, unjust enrichment, and nuisance.

Microsoft supported this request with evidence of how the Citadel botnet worked, and of the harm it caused to infected computers. In authorizing that request, the court: (1) enjoined the operators of the Citadel botnets from continuing to operate those botnets, (2) required domain registries to redirect a list of currently-registered domain names to secure servers, (3) required domain registries to transfer a list of currently-unregistered domain names into Microsoft's control, so they could not be used for the botnet, (4) required ISPs to log all attempts to communicate with specific IP addresses associated with the botnet, and provide documentation to Microsoft showing the persons who operate those IP addresses, (5) authorized Microsoft to cause all Citadel-infected computers attempting to connect to Citadel servers to connect instead to Microsoft servers, and install a curative file that stops the harmful acts of the botnet, and (6) authorized Microsoft to alert end-users when an infected computer attempted to connect to any Internet site, and direct them to a Microsoft or antivirus site to download curative files.

The court's order authorized Microsoft to disrupt more than 1,400 Citadel botnets that were responsible for more than half a billion dollars in losses to persons and businesses worldwide. At the same time, the FBI took coordinated separate steps related to the investigation, marking the first time that law enforcement and the private sector worked together in this way to execute a civil seizure warrant as part of a botnet disruption operation.

Transparency and Privacy are Core Values of Our Anti-Botnet Operations

Obtaining control of botnet domains is only the first step in preventing the spread of botnets and remediating the harm that they have caused. Once Microsoft receives information about a botnet, Microsoft disseminates this data to partners so that infected computers can be cleaned. Microsoft has worked in cooperation with numerous ISPs and CERTs around the world to help notify affected customers and connect them with tools to clean their devices.

Broad distribution of this information is crucial to remediating the harm that the botnets have caused, and preventing the botnets from growing. Microsoft makes information about botnets available to ISPs and CERTs through our Cyber Threat Intelligence Program ("C-TIP"). That service allows ISPs and CERTs to receive updated threat data related to infected computers in their specific country or network approximately every 30 seconds.

Last year, Microsoft and the Secretary of State of Telecommunications and Information Society of Spain announced an important agreement under which the Spanish CERT, INTECO, became one of the first organizations to receive data from the C-TIP cloud service. All the information is uploaded directly to each organization's private cloud through Windows Azure. INTECO joined the Luxembourg CERTs, CIRCL and gov CERT, as early adopters of this program. By participating in this system, organizations have almost instant access to threat data generated from previous as well as future operations conducted by the Microsoft Active Response for Security program.

The cloud-based C-TIP program represents an evolution in such information-sharing. In 2010, the original C-TIP program began sending regular emails to participating ISPs and CERTs with threat intelligence for their customers and regions. As of 2013, 44 organizations in 38 countries received these threat intelligence emails, and momentum is building for the program. The new cloud-based program dramatically increases our ability to clean computers and help us keep up with the fast-paced and ever-changing cybercrime landscape. It also gives us another advantage: cybercriminals rely on infected computers to exponentially leverage their ability to commit their crimes. If we are able to take those resources away from them, they will have to spend time and money trying to find new victims, thereby making these criminal enterprises less lucrative and appealing in the first place.

Privacy also is a fundamental value in Microsoft's anti-botnet operations. When we execute a botnet operation, we operate within the bounds of the court order. We never look at the underlying communications sent by infected computers. Instead, Microsoft only accesses the IP address used by the infected computer, so that we can help the ISPs and CERTs notify the user of the infection and assist in the remediation. We work with ISPs so they can alert their customers directly.

In addition, Microsoft makes resources available online so that consumers can help avoid becoming victims in the first place or clean infected computers. Individuals and businesses worldwide should exercise safe practices, such as running up-to-date, legitimate software. Additionally, people should use protections like firewalls and anti-virus/anti-malware programs and exercise caution when surfing the internet or clicking on ads or email attachments, as they could be malicious. More information on how to stay safe online can be found at http://www.microsoft.com/protect. People worried that their computers might be infected with malware, can obtain free information and malware cleaning tools from Microsoft at: http://support.microsoft.com/botnets.

Improving Laws to Battle Botnets

Microsoft welcomes the Subcommittee's strong interest in this growing threat, and appreciates your efforts to provide us with more tools to fight botnets. In particular, Microsoft believes that changes to two existing laws could go a long way toward battling botnets.

First, Microsoft supports amending the Computer Fraud and Abuse Act (CFAA), which long has allowed the government and private individuals to hold computer hackers responsible for unauthorized access to computers. Unfortunately, the law was enacted in 1986, long before we envisioned the command structure of botnets. In many cases, the botnet operator develops a system that enables *others* to conduct the actual hacking. Although some botnet operators have been convicted under the CFAA, we agree with the Department of Justice that the statute would be a more effective tool if it explicitly covered trafficking in access to botnets. Microsoft also agrees with the Department of Justice that Congress should amend Section 1030(a)(6) of the CFAA to eliminate the requirement of proof of intent to defraud, which in some botnet cases is difficult to demonstrate.

Finally, Microsoft agrees with the Department of Justice that Congress should amend the Access Device Fraud statute, which allows prosecutors to bring charges against the perpetrators of phishing and other credit card fraud schemes. The amendment should apply the statute to offenders in foreign countries who directly and significantly harm individuals and financial institutions in the United States. This change would provide both additional methods to disrupt phishing botnets that originate in other countries.

✧ ✧ ✧

In summary, Microsoft’s participation in public-private partnerships has resulted in the disruption and shut-down of some of the most malicious threats to public trust and security on the Internet. But our work is never done, as cybercriminals develop new and more sophisticated methods to profit from the online chaos that they create. The criminals will continue to evolve and develop more sophisticated tools. So will Microsoft. We remain firmly committed to working with other companies and law enforcement to disrupt botnets and make the Internet a more trusted and secure environment for everyone.