Department of Justice

STATEMENT OF

JOSEPH DEMAREST
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ENTITLED

"TAKING DOWN BOTNETS: PUBLIC AND PRIVATE EFFORTS TO DISRUPT AND DISMANTLE CYBERCRIMINAL NETWORKS"

PRESENTED

JULY 15, 2014

Statement of
Joseph Demarest
Assistant Director
Cyber Division
Federal Bureau of Investigation

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

At a Hearing Entitled
"Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks"

Presented
July 15, 2014

Good morning Senator Whitehouse. I thank you for holding this hearing today, and I look forward to discussing the progress the FBI has made on campaigns to disrupt and disable significant botnets.

As you well know, we face cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. They seek our state secrets, our trade secrets, our technology, and our ideas – things of incredible value to all of us. They may seek to strike our critical infrastructure and our economy. The threat is so dire that cyber security has topped the Director of National Intelligence list of global threats for the second consecutive year.

Cyber criminal threats post very real risks to the economic security and privacy of the United States and its citizens. The use of botnets is on the rise. Industry experts estimate that botnets attacks have resulted in the overall loss of millions of dollars from financial institutions and other major U.S. businesses. They also affect universities, hospitals, defense contractors, government, and even private citizens.The "weapons" of a cyber criminal are tools, like botnets, which are created with malicious software that is readily available for purchase on the Internet. Criminals distribute malicious software, also known as malware, that can turn a computer into a "bot." When this occurs, a computer can perform automated tasks over the Internet, without any direction from its rightful user. A network of these infected computers—numbering in the hundreds of thousands or even millions—is called a botnet (robot network), and each computer becomes connected to a command-and-control server operated by the criminal.

Once the botnet is in place, it can be used in distributed denial of service (DDoS) attacks, proxy and spam services, malware distribution, and other organized criminal activity. Botnets can also be used for covert intelligence collection, and terrorists or state-sponsored actors could use a botnet to attack Internet-connected critical infrastructure. And, they can be used as weapons in ideology campaigns against their target to instigate fear, intimidation, or public embarrassment.

A botnet typically operates without obvious visible evidence and can remain operational for years.

Our personal computers can become part of a botnet—it only takes one wrong click for a home user to download malicious code. For example, you might get an unsolicited e-mail promoting a dating website or a work-at-home arrangement or an e-mail that appears to come from your bank containing a seemingly harmless link. You could be sent a link by a friend asking you to view a great video, which was actually sent because your friend's computer is already infected. You could see a link on a webpage that seems to be soliciting donations for a recent tragedy. And you might even visit a fraudulent website—or a legitimate one that's been compromised—and download video, pictures, or a document containing malicious code.

Once the malware is on your computer, it's hard to detect. In addition to your computer being commanded to link up with other compromised computers to facilitate criminal activity, the bot can also collect and send out your personal identifiable information—like credit card numbers, banking information, and passwords—to the criminals running it. Those criminals will take advantage of the information themselves or offer it for sale on cyber criminal forums.

The impact of this global cyber threat has been significant. According to industry estimates, botnets have caused over $9 billion dollars in losses to U.S. victims and over $110 billion in losses globally. Approximately 500 million computers are infected globally each year, translating into 18 victims per second.

The FBI, with its law enforcement and private sector partners, has had success in taking down a number of large botnets. But our work is never done, and by combining the resources of government and the private sector, and with the support of the public, we will continue to improve cyber security by identifying and catching those who threaten it.

FBI's Cyber Criminal Strategy

Due to the complicated nature of today's cyber criminal threat, the FBI has developed a strategy to systematically identify cyber criminal enterprises and individuals involved in the development, distribution, facilitation, and support of complex criminal schemes impacting U.S. systems. This complete strategy involves a holistic look at the entire cyber underground ecosystem and all facilitators of a computer intrusion.

The FBI's overall goal is to remove, reduce, and prevent cyber crime by attacking the threat through the identification of the most significant cyber criminal actors. Our success can only be attained through coordination of our overall cyber criminal strategy amongst all FBI Cyber Division's existing and emerging entities.

Just last month, the FBI Cyber Division evolved to create a threat-model approach to address the most significant domestic and international cyber threats. The FBI cyber criminal strategy

consists of the newly established Major Cyber Crimes Unit, which serves as the primary headquarters unit addressing the cyber criminal threat by providing strategic and field office operational support; the Cyber Initiative and Resource Fusion Unit (CIRFU) which supports the National Cyber Forensics and Training Alliance (NCFTA) and is comprised of representatives from industry, academia, and the FBI; and the Internet Crime Complaint Center (IC3) which has a vital role in the identification of cyber fraud-related threats. All of these entities work together to enhance and support field office operations by developing and maintaining long-term strategies to infiltrate cyber criminal networks, provide tactical support, and develop intelligence collection opportunities against predicated targets.

The FBI cyber criminal strategy also includes working closely with our international partners to develop a holistic assessment of the threat posed by cyber criminals and organizations to partner countries. Through this collaborative process, the FBI hopes to launch aggressive and comprehensive mitigation strategies through joint investigations and operational partnerships with law enforcement partners, private industry, and academia.

These important components of the FBI cyber criminal strategy coordinate efforts with the National Cyber Investigative Joint Task Force (NCIJTF), which is intended to be the focal point for all U.S. government agencies to coordinate, integrate, and share domestic cyber threat information specific to national security investigations.

FBI Efforts to Combat Botnets

Through the NCIJTF, and in alliance with its U.S. government (USG) partners, international partners, and private sector stakeholders, the FBI has worked collaboratively in developing a multi-pronged effort aimed at defeating the world's most dangerous botnets.

Over the past several years, the FBI's efforts to combat these significant cyber threats have caused the disruption and dismantlement of numerous botnets including Butterfly Bot, Rove Digital, Coreflood, ZeroAccess, and Gameover Zeus, resulting in numerous arrests, extraditions, and convictions.

Operation Clean Slate

In April 2013, the FBI initiated an aggressive approach to disrupt and dismantle the most significant botnets threatening the U.S. economy and our national security. This initiative, named Operation Clean Slate, is spearheaded by the FBI's NCIJTF. It is a comprehensive, public/private effort engineered to eliminate the most significant botnets jeopardizing U.S. interests by targeting the criminal coders who create them. This initiative incorporates all facets of the USG, international partners, major Internet service providers, the U.S financial sector, and other private sector cyber stakeholders.

Operation Clean Slate has three objectives: (1) to degrade or disrupt the actor's ability to exfiltrate sensitive information from U.S. networks through arrests, by deploying a technical

solution to interrupt the botnet, and by working with private sector partners to update security software that detects and damages the bot's malware; (2) to increase the actor's cost of business by causing wasted time debugging failures, or forcing an actor to write new code for new botnet attacks; and (3) to seed uncertainty in the actor's cyber activity by causing concern about potential or actual law enforcement action.

The FBI Cyber Division ranked the Citadel Botnet as the highest priority under the Operation Clean Slate initiative. In June 2013, the FBI, in coordination with its partners, disrupted the Citadel Botnet which had facilitated unauthorized access to computers of individuals and financial institutions to steal online banking credentials, credit card information, and other personally identifiable information. Citadel was responsible for the loss of over a half billion dollars. Over 1,000 Citadel domains were seized, accounting for more than 11 million victim computers worldwide.

In separate but coordinated operations, the FBI, Microsoft, and financial services industry leaders successfully disrupted more than 1,000 botnets built on Citadel malware in a massive global cyber crime operation that is estimated by the financial services industry to have been responsible for over half a billion dollars in financial fraud. Microsoft exercised its independent civil authorities in this matter. The company then coordinated with the FBI and other private parties. The FBI provided information to foreign law enforcement counterparts so that they could also take voluntary action on botnet infrastructure located outside of the United States. The FBI also obtained and served court-authorized search warrants domestically related to the botnets.

Building on the success of the disruption of Citadel, in December 2013, the FBI and Europol, together with Microsoft and other industry partners, disrupted the ZeroAccess botnet. ZeroAccess was responsible for infecting more than two million computers, specifically targeting search results on Google, Bing, and Yahoo search engines and is estimated to have cost online advertisers $2.7 million each month.

Recent Successes

Other recent FBI successes in combating the botnet threat include domestic and international investigative efforts which have resulted in indictments, arrests, and extraditions. Examples include:

- In April 2011, the FBI executed criminal seizure warrants to disable an international botnet consisting of hundreds of thousands of computers infected with a malicious software program known as Coreflood. Coreflood allowed infected computers to be controlled remotely for the purpose of stealing private personal and financial information from unsuspecting computer users, including users on corporate computer networks, and used that information to steal funds.

- In November 2011, a two-year FBI investigation called Operation Ghost Click resulted in the dismantlement of an international cyber ring that infected millions of computers worldwide with a virus that enabled the thieves to manipulate the multi-billion-dollar Internet advertising industry. In November 2013, three Estonian nationals were extradited to the United States to face charges related these crimes.

- In December 2012, the FBI disrupted an international organized cyber crime ring related to Butterfly Botnet,which stole computer users' credit card, bank account, and other personally identifiable information. Butterfly Botnet compromised more than 11 million computer systems and resulted in over $850 million in losses. The FBI, along with international law enforcement partners, executed numerous search warrants, conducted interviews, and arrested 10 individuals from Bosnia and Herzegovina, Croatia, Macedonia, New Zealand, Peru, the United Kingdom, and the United States.

- In April 2014, the FBI's investigative efforts resulted in the indictments of nine alleged members of a wide-ranging racketeering enterprise and conspiracy who infected thousands of business computers with malicious software known as "Zeus," which is malware that captured passwords, account numbers, and other information necessary to log into online banking accounts. The conspirators allegedly used the information captured by "Zeus" to steal millions of dollars from account-holding victims' bank accounts.

- In May 2014, the FBI announced the indictments of a Swedish national and a U.S. citizen believed to be the co-developers of a particularly insidious computer malware known as Blackshades. This software was sold and distributed to thousands of people in more than 100 countries and has been used to infect more than half a million computers worldwide. Also charged and arrested in the United States was an individual who helped market and sell the malware, and two Blackshades users who bought the malware and then unleashed it upon unsuspecting computer users, surreptitiously installing it on their hardware. At least 40 FBI field offices conducted approximately 100 interviews, executed more than 100 e-mail and physical search warrants, and seized more than 1,900 domains used by Blackshades users to control victims' computers, and at least 18 other countries were involved in executing more than 90 arrests and more than 300 searches.

- In June 2014, the FBI announced a multinational effort to disrupt the GameOver Zeus botnet, the most sophisticated botnet that the FBI and its allies had ever attempted to disrupt. GameOver Zeus is believed to be responsible for the theft of millions of dollars from businesses and consumers in the U.S. and around the world. This effort to disrupt it involved impressive cooperation with the private sector and international law enforcement. GameOver Zeus is an extremely sophisticated type of malware designed specifically to steal banking and other credentials from the computers it infects. In the case of GameOver Zeus, its primary purpose is to capture banking credentials from infected computers, then use those credentials to initiate or re-direct wire transfers to

accounts overseas that are controlled by the criminals. Losses attributable to GameOver Zeus are estimated to be more than $100 million.

Way Forward

The FBI is proud of these successes, but we recognize that we must constantly strive to be more efficient and effective. Just as our adversaries continue to evolve, so, too, must the FBI. We live in a time of sophisticated cyber criminal threats - threats that most often impact our private citizens.

Much like with the FBI's other investigative priorities where we focus on the impacting the leaders of a criminal enterprise or terrorist organization, we are focusing on the major cyber actors behind the botnets. The FBI must also continue to develop and deploy creative solutions in order to defeat today's complex cyber threat actors. This includes R&D addressing how to identify and shut down botnets faster than they are created and used. We also strive to build better relationships in order to overcome the obstacles that prevent us from collaborating and sharing information.

We remain focused on defending the United States against these threats, and we welcome opportunities like the one today to discuss these efforts. We are grateful for the Committee's support, and we look forward to working with you as we continue to forge aggressive campaigns against botnets.