New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 253—NO. 82
THURSDAY, APRIL 30, 2015

INTERNATIONAL CRIMINAL LAW AND ENFORCEMENT

Expert Analysis

'Botnets' and the Battle Against Cyber Crime

By **Nicholas M. De Feis**

And **Philip C. Patterson**

In our last column, we wrote about global enforcement efforts to combat international bribery.[1] In this column, we describe efforts to combat a different but far more insidious form of international crime. This type of crime has been deemed so serious that on Feb. 24, 2015, the U.S. Department of State's Transnational Organized Crime Rewards Program offered a $3 million bounty for information leading to the arrest or conviction of one particularly egregious alleged perpetrator. An Al Qaeda mastermind? No, a 30-year-old botnet programmer.

Derived from the words "robot" and "Internet," a "botnet" is a network of software programs on different computers that allows them to be collectively controlled by a cyber criminal. The network of computers can be used to commit crimes such as identity theft, denial of service attacks, computer ransoming and massive spam campaigns. Botnets know no borders other than software compatibility. They are designed to spread to computers without revealing their existence. They cause at least hundreds of millions of dollars in economic harm every year, not to mention the inestimable personal harm caused to individual victims of identity theft.

Indeed, a study released earlier this month based on interviews of more than 500 U.S. corporations demonstrated that a third of the corporations were hit by multiple cyber attacks per year, with a third of the corporations losing $100,000 in revenue per hour during an attack.[2] Corporations are also increasingly becoming targets of class action lawsuits based on data breaches that expose sensitive customer information.

As we increasingly rely on computers, the threat from botnets will only increase, exposing law firms and corporations to pernicious hacking and litigation over cyber attacks. Right now, a global arms race is occurring between cyber criminals on the one side and corporations, software security firms and law enforcement agencies on the other side. This arms race will continue as long as we continue to rely on computers, which is to say, probably forever.

The Real Zombie Outbreak

Popular culture is full of TV shows and films depicting pandemics that create legions of zombies, but the real zombie outbreak is happening right now on computers across the world as a result of botnets. Botnets basically turn computers into robots that carry out tasks based on commands sent over the Internet. Originally, botnets were legitimate networks performing intended functions, and they are still used for legitimate purposes. But their effectiveness for illegitimate purposes and increasing use by cyber criminals has changed the term "botnet" into a pejorative.

Botnet computer programs are typically spread by "malware," which is a term that combines the words "malicious" and "software." The malware is the means by which a botnet makes it onto a person's computer. The malware is typically either picked up from websites or travels by email from one computer to another. The botnet then forces the infected computer to secretly act as a robot, or "bot," and perform functions in response to commands sent by the cyber criminal. Infected computers are frequently referred to as "zombies," because they mindlessly carry out the botnet's tasks, with the resulting group of infected computers referred to as a "zombie army."

Dangers of Botnets

One of the most common botnet tasks is forcing a computer's email software to send out the cyber criminal's spam emails. The spam typically consists of advertising, perhaps for a security that is about to be used in a pump and dump stock fraud or for a website where one can illegally purchase prescription drugs. The first known botnet was identified by Internet service provider Earthlink in 2001, and infected so many computers that it was determined to be responsible for over 10 percent of Earthlink's total email traffic.

The botnet was revealed when Earthlink sued an individual named Kahn C. Smith and 50 John Does in the Northern

NICHOLAS M. DE FEIS, *a former federal prosecutor, is a partner at De Feis O'Connell & Rose.* PHILIP C. PATTERSON *is counsel to the firm.*

District of Georgia alleging that they were responsible for sending 1.25 billion junk emails through Earthlink accounts.[3] Although Earthlink won a $25 million judgment against Smith, cyber hackers were undeterred as the volume of botnet spam has only increased since then. In 2014, experts estimated that about 90 percent of all email traffic is spam, most of which is generated by zombie computers.[4]

Botnets are also used to generate fake Internet traffic. This is a serious concern for corporations because the cost of online advertising is determined in part by how many people actually see the ads.[5] Botnets can force computers to visit sites and thus generate fake web traffic. Fake traffic is difficult to distinguish from real traffic, and has been estimated to cause damages of up to $6 billion per year in the United States alone.[6]

Another nasty botnet task is forcing the host computer to encrypt all the user's files on the computer, and then offering to de-encrypt them only if the user makes a payment to the cyber criminal over the Internet. The botnet thus holds the computer—including any personal or work-related files on the computer—as a hostage for ransom.

One of the most dramatic uses of a botnet is for distributed denial-of-service (DDoS) attacks, where the infected computers are directed to bombard an Internet site with a massive number of requests at the same time. The goal is to overload the website and even cause it to crash. These attacks can be motivated by economics, politics or simply vandalism.

One of the largest such DDoS attacks targeted the websites of Bank of America, JPMorgan Chase, Wells Fargo, U.S. Bank and PNC Bank in September 2012.[7] The attackers used a botnet to connect thousands of servers and force them to bombard the banks' websites with Internet traffic. Although the botnet did not steal any sensitive information from the banks, the websites were so overloaded that customers had difficulty logging into their bank accounts. An Islamist group claimed responsibility for the attacks, while some U.S. officials asserted that the government of Iran was responsible.[8] The true source of the attacks was never confirmed.

Law enforcement agencies in the United States have had some success in prosecuting perpetrators of DDoS attacks. The U.S. Attorney's Office for the Northern District of California and the Federal Bureau of Investigation have investigated and charged a number of individuals involved in the hacker group Anonymous for DDoS attacks carried out against online pay service PayPal. Fourteen individuals eventually pleaded guilty to charges of intentionally damaging a protected computer in violation of 18 U.S.C. §1030(a)(5).[9]

Derived from the words "robot" and "Internet," a "botnet" is a network of software programs on different computers that allows them to be collectively controlled by a cyber criminal.

The worst use of a botnet is to quietly monitor the actions of computer users and in the process steal sensitive information such as Social Security numbers or account passwords. Consider for a moment the amount of sensitive information that you store on your computer, send by email, and enter into websites in the form of usernames and passwords. If a botnet is present on your computer, all that information can be quietly gathered and transmitted to a cyber criminal at another location.

Perhaps most troubling of all, botnets are not necessarily used by their creators. A so-called "bot herder" or "bot master" can sell the botnet to others, or even lease access to it for a limited period of time. Platforms exist on the Internet where one can rent or lease access to armies of zombie computers, to be used for whatever purpose the buyer desires. Purchasing a botnet can cost as little as a few hundred dollars, and renting access to thousands of infected computers for a few hours can cost as little as a few dollars.[10]

Global Enforcement Efforts

The best example of how seriously law enforcement agencies worldwide are taking the threat of botnets is the global effort to combat the Gameover Zeus botnet (GOZ). On June 2, 2014, the U.S. Department of Justice announced the existence of "Operation Tovar," a multinational effort to disrupt GOZ. Believed to be the most sophisticated and successful botnet ever, GOZ first appeared in September 2011 as the latest version of the "Zeus" malware, which appeared in 2007. The alleged mastermind behind it is 30-year-old Russian national Evgeniy Bogachev, although other individuals in Russia and the Ukraine are also believed to be involved.

GOZ spreads through various means, including "phishing," which generally describes emails that are designed to appear routine but which actually are intended to trick computer users into downloading software that records sensitive information such as Social Security numbers or online account login information. Once recipients are led to click on a link within the email, the link may cause the user's computer to download malware containing a botnet such as GOZ. Once inside the user's computer, the botnet typically lies dormant until it is activated. It may even automatically delete the malware that delivered it to help avoid detection. At some point, the cyber criminal controlling the botnet sends out communications that activate it on infected computers and the botnet then begins forcing the infected computers to perform a task they otherwise would not perform.

In the case of GOZ, clicking on an email could result in the user's computer becoming part of a network that at its peak numbered between 500,000 and one million computers worldwide. A quarter of the computers infected by GOZ were located in the United States. The primary purpose of GOZ was to secretly gather bank account login information, which was then used to direct

money transfers from the bank accounts to the cyber criminals. The U.S. Federal Bureau of Investigation estimates that GOZ has caused $100 million in damages. The victims are not simply unwitting individuals, they include corporations, a bank and even an Indian tribe.

The Justice Department's investigation of GOZ and the efforts to disrupt it involved Europol, as well as law enforcement agencies from Australia, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, New Zealand, the Ukraine and the United Kingdom. Also participating were about 15 software companies, including Dell, Microsoft, McAfee and Symantec. In the United States, the enforcement effort includes indictments of Bogachev in Pittsburgh and Omaha on computer, wire and bank fraud charges, as well as a civil action in Pittsburgh naming Bogachev and four other unidentified individuals known only by their online aliases. The Justice Department also seized computer servers believed to be involved and set up a website users can visit to remove the GOZ malware from their computers.

Operation Tovar succeeded in cutting communications between the infected computers and the so-called command and control structure the cyber criminals used to operate GOZ, which gave users time to disinfect their computers (assuming they were aware of the infection). Yet, only two months after the shut-down, anti-virus software companies began announcing that "variants" of GOZ—essentially new-and-improved versions—have begun infecting computers in the United States, Ukraine and Belarus.[11]

Challenges for Authorities

The greatest challenge for authorities is simply keeping up. GOZ was back to infecting computers only months after a massive multinational effort to shut it down, and GOZ was only one of countless forms of botnets circulating across the globe. Moreover, beginning in 2012 botnets began to be discovered that operate on smartphones. Thus, as the technology of computing devices evolves, botnets will undoubtedly evolve to keep pace.[12]

> The worst use of a botnet is to quietly monitor the actions of computer users and in the process steal sensitive information such as Social Security numbers or account passwords.

Operation Tovar revealed that law enforcement agencies across the globe are taking the threat of botnets seriously. The question has also been posed, however, that if the government is watching the cyber criminals, who's watching the government? Documents leaked by former U.S. National Security Agency (NSA) contractor Edward Snowden reveal that the NSA has hijacked botnets and used them to install its own software for its own intelligence purposes.[13] The information gathered was to be shared with the "Five Eyes" intelligence alliance, comprising Australia, Canada, New Zealand, the United Kingdom, and the United States. It would seem botnets are simply too effective, and thus too tempting, for government agencies to resist.

Challenges for Law Firms

Targets of cyber attacks can also become targets of lawsuits. In the past two years, major corporations like Target Corp., Home Depot, Anthem, Inc. and Premera Blue Cross have all been named in multiple putative class actions based on data breaches that exposed customer information, with the actions consolidated as multidistrict litigations.

Law firms have also been targets. In March 2015, Bloomberg reported that 80 percent of the 100 largest law firms have been the subject of some sort of data breach.[14] State bars have responded by issuing opinions on the level of security lawyers should employ to protect client confidentiality. Almost all states have enacted data security breach notification laws.

The Securities and Exchange Commission has indicated that data breaches may constitute disclosure events, and is considering issuing regulations requiring certain disclosures.[15] Only days ago, the U.S. House of Representatives passed a long-debated and controversial bill that would allow corporations to share "cyber threat indicators" with each other and with the government through an intermediary.[16]

In short, individuals, law firms and corporations must be vigilant against cyber threats. Law firms and corporations must be aware of and adhere to local and federal standards regarding cyber security. Moreover, to avoid both the harm caused by cyber attacks and resulting litigation, they must ensure that they have a level of cyber security—both software and hardware—commensurate with their size and the nature of their work.

And the next time your IT people tell you to change your passwords frequently, listen to them.

•••••••••••••●●•••••••••••••

1. Nicholas M. De Feis and Philip C. Patterson, "Foreign Corrupt Practices: The Global Trend," NYLJ, Jan. 30, 2015.
2. "Neustar DDoS Attack Study Shows North American Companies Better Equipped for Cyber Security Issues," BusinessWire, April 20, 2015. Notably, these statistics reflect only one type of the attack, the so-called "denial of service," discussed infra.
3. *Earthlink v. Smith*, 01 CV 2099 (N.D. Ga. filed Aug. 7, 2001).
4. Messaging, Malware and Mobile Anti-Abuse Working Group, "Report #16 – 1st Quarter 2012 through 2nd Quarter 2014," Nov. 2014.
5. Susanne Vranica, "A 'Crisis' in Online Ads: One-Third of Traffic Is Bogus," WSJ, March 23, 2104.
6. See id.
7. CNNMoney, "Major banks hit with biggest cyberattacks in history," money.cnn.com, Sept. 27, 2012.
8. Ellen Nakashima, "Iran blamed for cyberattacks on U.S. banks and companies," Washington Post, Sept. 21, 2012.
9. *USA v. Collins*, 11 CR 471 (N.D. Ca. filed Dec. 3, 2012).
10. Nick Clayton, "Where to Rent a Botnet for $2 an Hour or Buy one for $700," WSJ.com, Nov. 5, 2012.
11. See Lucian Constantin, "New Gameover Zeus botnet keeps growing, especially in the U.S.," PCWorld.com, Aug. 14, 2014.
12. John E. Dunn, "Android smartphones hijacked to build first mobile botnet," Techworld.com, Jul. 5, 2012.
13. Joseph Menn, "NSA 'hijacked' criminal botnets to install spyware," Reuters, March 12, 2014.
14. Ellen Rosen, "Most Big Firms Have Had Some Hacking: Business of Law," Bloomberg, March 11, 2015.
15. Securities & Exchange Commission, Division of Corporation Finance, "CF Disclosure Guidance: Topic No. 2—Cybersecurity," Oct. 13, 2011.
16. Protecting Cyber Networks Act (PCNA) (H.R. 1560).