TESTIMONY OF RODNEY JOFFE
SENIOR VICE PRESIDENT AND SENIOR TECHNOLOGIST
NEUSTAR, INC.

on

Network Threats and Policy Challenges

before the

Committee on Energy and Commerce
Subcommittee on Communications, Technology and the Internet
UNITED STATES HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

May 1, 2009

TESTIMONY OF RODNEY JOFFE

SENIOR VICE PRESIDENT AND SENIOR TECHNOLOGIST, NEUSTAR,INC.

Good afternoon, Representative Weiner and members of the subcommittee. My name is Rodney Joffe, and I am the Senior Vice President and Senior Technologist for NeuStar, Inc. NeuStar is a neutral provider of clearinghouse services to the telecommunications industry.

I joined NeuStar in 2006 when we acquired UltraDNS, a company I founded and chaired, and which is the largest provider of DNS services in the world. DNS stands for the domain name system. When a user types in a webname, such as CSPAN.com, DNS is the mechanism that converts the webname CSPAN.com into an IP address, or the numbers that computer networks actually understand, and which are then used to route requests to go to the CSPAN.com web page for example.

Prior to founding UltraDNS, I was Vice President and Chief Technology Officer for GTE Internetworking Business Services, a position I filled as result of GTE's acquisition of Genuity, another of the companies that I founded. At the time of the acquisition, Genuity was one of the largest Internet Service Providers in the world. I also sit on the board of a small number of other technology companies primarily focused in the area of Internet cyber security threats and serve as a member of the ICANN Security and Stability Advisory Committee.

In 2008, I participated in Cyberstorm II, a cybersecurity exercise run by the Department of Homeland Security with participation by four other nations and about 40 private companies from many different sectors. My role was to develop and run the DNS portion of the exercise. While I am not free to discuss the exercise in detail, I can tell you that it was very illuminating to many companies to see just how dependent their operations were on the successful resolution of their DNS and the proper workings of the Internet for the core of their operations.

I am also one of the founders of an unofficial organization known publicly as the Conficker Working Group, established in response to the outbreak and spread of the Conficker Internet worm which first surfaced last year but became much more powerful and threatening in early March of this year. At that time, I briefed a number of Congressional Members, their committee staffs, military and federal law enforcement executives, and industry leaders on the specific threats from Conficker. Conficker represents the state-of-the-art in terms of large scale, malicious Internet and computer malware. Currently, almost 4 million computers around the world are infected with one of its versions. Our experience in coping with Conficker also provides some examples of the holes and gaps in our readiness to defend against and respond to cyber crime and cyber terrorism. I appreciate the opportunity to appear before you today and to bring these examples and facts to your attention.

Everyone understands that cyberspace has no geographic or political borders. Cyberspace is a single place that has not yet been able to properly develop the natural borders that exist in the real world, borders that you would find for example between states and countries. We don't yet have an effective mechanism to police any of those. So when cybercriminals operate, they have the advantage of being able to use this lack of maturity and are able to ignore the laws and rules that exist in the real world.

In a nutshell, we're still developing the systems and mechanisms that will allow us to conduct ourselves appropriately no matter who we are on the Internet. We are still finding our way. It was only a short while ago that the Internet first came into existence. The security systems that were put in place at the time were never meant for, and could not possibly have envisioned, today's world where nearly every critical piece of infrastructure is tied to the global Internet. And so I really appreciate the opportunity to provide input to the committee, as you look for ways to enhance the security and stability of the Internet from the very real cyber challenges and threats we face today.

The motives for Internet attacks can generally be broken down into one of three categories. The first and oldest reason for Internet attacks is that of ego or bragging rights. In general, and historically, the perpetrators behind these attacks are young, immature and intent on showing their prowess for computer programming, with little or no regard for the damage that they cause in their attacks. Their attacks include website defacements, DDOS attacks and disabling of computers or deletion of files. Probably the most public case was that of the hijacking of Comcast's domain name and website in May of 2008.[1]

The second category, now the most common, is for financial gain. Inevitably the hobbyist "miscreants" discover that they can make money doing what they do. In this category, the attacks are committed by individuals as well as organized crime gangs and are manifested in large spam email campaigns, extortion schemes, and the interception and illegal use of computer data – most commonly bank and credit card information. The most public examples of these have been the Russian Business Network[2], and the McColo Corporation[3], one of the most prolific spam outfits. It is important to note in these cases that while some of the facilities were in the US, the principals in these criminal cases operated from Eastern Europe.

The third category and arguably the most worrying, is cyberterrorism, or activities sponsored by nation-states. This category can be further split into two sub-groups: actors who seek to steal national assets and those who would seek the complete destruction or disruption of a country. Over the last two years, there have been at least three public attacks, reportedly nation-state sponsored,

[1] Mills, Elinor "Teens Await After Comcast Attacks." 30 May, 2008. CNET News. http://news.cnet.com/8301-10784_3-9956165-7.html

[2] Krebs, Brian "Russian Business Network: Down but Not Out." 7 Nov., 2007.
The Washington Post.
http://voices.washingtonpost.com/securityfix/2007/11/russian_business_network_down.html

[3] Krebs, Brian "A Closer Look at McColo." 13 Nov., 2008.
The Washington Post.
http://voices.washingtonpost.com/securityfix/2008/11/the_badness_that_was_mccolo.html

against countries including Estonia, Georgia, and Kyrgyzstan[4], although we now believe that the Estonian and Georgian attacks were carried out for financial rather than political motives. Additionally, there may have been attacks against SCADA (Supervisory Control and Data Acquisition) systems[5]. In New Orleans in January 2008, Tom Donahue from the CIA released information regarding some of these attacks in other countries. There have also been a number of reports of power-generators similar to those used in large US cities being destroyed physically as a result of a cyberattack. The Wall Street Journal reported on April 8 of this year that a federal audit of critical infrastructure facilities in the power industry had been compromised with software that would allow the attackers to disable key elements of the national power grid at will. The sources, identified as “current and former national-security officials” claimed the software was inserted by “cyberspies” from “China, Russia and other countries”[6].

It is important to understand that the lines between the three categories have become blurred. The juvenile defacers slip just as easily into the role of cybercriminal and cyberterrorist, as do the cyberterrorists slip into the role of cybercriminal.

I’d like to provide some detail around a sampling of real-world events that I’ve personally been involved in as a way of providing context for some of the challenges and opportunities.

NeuStar operates the core directory that enables data to be correctly routed on the Internet for about 15 million domain names. The technology that enables this capability is DNS, or domain name system. Humans recognize and are able to work with common words and names, however computers only understand numbers and in the case of the Internet, IP addresses, or Internet Protocol addresses. So the DNS, simply put, is the directory that converts names to IP addresses and vice versa. For example, a user enters www.house.gov into an Internet browser and the DNS converts that to the IP address 204.141.87.18. The computing devices are then able to route the user's request to the House's web server.

NeuStar provides this core directory service for the .biz top-level-domain, as well as for 18 other top level domains, including a number of country-code or cc-TLDS. These include .us for the United States, .ca for Canada, .uk for the United Kingdom, .au for Australia, .jp for Japan, and .nz for New Zealand, amongst others. We also provide the directory service for anyone attempting to reach many of the Fortune 500 or eCommerce 2000 companies. All in all, we serve about 4,000 corporations and government departments around the world, and more than 15 million domain names.

[4] Goodin, Dan “DDoS Attack Boots Kyrgyzstan From Net.” 28 Jan., 2009.
The Register. http://www.theregister.co.uk/2009/01/28/kyrgyzstan_knocked_offline/

[5] Greenberg, Andy. “Hackers Cut Cities’ Power.” 18 Jan. 2008.
Forbes. http://www.forbes.com/2008/01/18/cyber-attack-utilities-tech-intel-cx_ag_0118attack.html

[6] Gorman, Siobhan “Electricity Grid in US Penetrated by Spies.” 8 April, 2009.
The Wall Street Journal. http://online.wsj.com/article/SB123914805204099085.html

The most common kind of attack is called a DOS attack, or Denial of Service attack, whereby an attacker attempts to disrupt the ability of an organization to operate normally on the Internet. In most cases, this kind of attack employs the use of multiple (often tens or hundreds of thousand of machines, and sometimes millions) in a coordinated manner, and in these cases, the attack is classified as a Distributed Denial of Service, or DDOS attack. The attacker takes command of these machines, known as a botnet, and orders the machines to try to reach a specific site. The result is that a website is hit by millions of packets per second in an attempt to overwhelm the site and take it down. While it would require fewer than 10,000 strategically located compromised machines to effectively disable a sizeable portion of the US Internet, these attacks generally involve hundreds of thousands of machines because botnets are easily built. Cybercriminals see them as disposable resources which are easily replaced and at no real cost to the criminals.

In the second kind of attack, the cybercriminals attempt to destroy the computer systems of the victims by overriding data, deleting files, or permanently modifying information.

A third kind of attack revolves around data exfiltration, where cybercriminals attempt to gain access to computer systems either manually or through automated means using viruses, worms or trojans. They then use that malicious software to extract data from their unknowing victim’s systems and transfer that data back to the criminals for their own use or blackmarket sale to others. Bank account or credit card information is a frequent target.

There are also a number of lesser-known yet still dangerous kinds of malicious behavior that exist in cyberspace: defacement of websites, where content is replaced, and redirection, where users believe they are directed to one website but are redirected to another website instead. One of the ways this is achieved is through something called DNS cache poisoning, where local copies of the directory are modified by cybercriminals to deceive users. An example of this would be where the customers of a bank are re-directed to a fake bank website that looks identical to their normal banking website, and where the customers then unknowingly provide the criminals with their personal information and banking credentials.

These are but some of the successful threats that we have to cope with today in the Internet security world.

It is important to note that while most people may not be aware of any of these kinds of attacks actually occurring, they are very real. Often, the security industry, through hard work, coordination, knowledge and frequently, pure luck, are able to mitigate the effects before end users notice them. In most cases, these attacks never come to public notice. However, just a few minutes of effort with Google, searching for the terms “DNS and DDoS”, and “cache poisoning”, and “keystroke logging” will bring thousands of links to reports of successful breaches of Internet defenses. I’ll focus on some events that have occurred or have been identified publicly in the last month.

In the first attack, on April 1st, 2009, Register.com, one of the major Internet domain name registrars, was attacked by the use of a DNS DDoS. In this attack, the attackers caused tens of thousands of compromised computers to flood the DNS or directory servers of the victim with bogus DNS requests, effectively rendering the directory servers unusable. In this particular case, hundreds of thousands of organizations became unreachable because Register.com provided the DNS service for their domains. This attack lasted a number of hours, but the effects lingered for a few days.

A second event occurred on April 12th that is far more insidious for average Internet users. The DNS servers of a large Brazilian ISP, Virtua, were compromised and their cache, or their local temporarily stored domain name and address directory, was “poisoned”. The entry for one of Brazil’s major banks, Bradesco, was modified by re-directing users to a fake website that was an exact copy of the Bradesco site, but was controlled by cybercriminals. This poisoned entry remained in place for five hours before Virtua and Bradesco noticed the problem and corrected it. According to an official statement from Bradesco, approximately “only 1% of their customers” were affected and potentially re-directed to this malicious site. Unfortunately, 1% of their customers are almost 150,000 individuals and this represents potentially huge monetary losses. Similar cache poisoning events have been occurring for years, and the only complete defense is the implementation of the DNSSEC protocol. However, absent significant effort and support, this solution is unlikely to be available to the general public until 2011 at the earliest.

The third event and perhaps the most visible, in my opinion, is one of the most dangerous botnets ever created. It is based on the Conficker worm which as of today has almost 4 million participating computers. The owners of these computers are unaware that their computers are no longer under their control and a significant number of these computers have been identified as being located inside critical infrastructure networks.

The Conficker worm has the ability of executing many different types of attacks. Modern malware is nothing if not multi-talented; the machines could be used for keystroke logging and data exfiltration or used as a giant online search engine. The botnet could be instructed to search computers local hard drives, as well as all of the systems they are connected to, for any documents or drawings that contain the word “electrical”, “secret” or “bank account”. They could also be instructed as a group to launch a denial of service attack against any website such as whitehouse.gov or the largest bank in the United States.

As a sobering side-note, over the last three weeks, in collaboration with a researcher from Georgia Tech in Atlanta who is involved with the Conficker Working group, I have identified at least 300 critical medical devices from a single manufacturer that have been infected with Conficker. These devices are used in large hospitals, and allow doctors to view and manipulate high-intensity scans (MRI, CT Scans etc), and are often found in or near ICU facilities, connected to local area networks that include other critical medical devices.

Worse, after we notified the manufacturer and identified and contacted the hospitals involved, both in the US and abroad, we were told that because of regulatory requirements, 90 days notice was required before these systems could be modified to remove the infections and vulnerabilities. We have since identified thousands of infected computers and devices in almost all parts of critical infrastructure that are infected with Conficker. We are working with industry groups and ISACs to remediate these machines. However it is clear that in some cases, there is a disconnect between government rules meant to protect consumers, and today's cyber threats which sometimes results in delaying and hindering the ability to fix problems, such as in the case with the medical devices.

The news is not all grim, however. There are potential solutions, or at the very least, pathways to defending against these attacks. NeuStar, for example, has developed an interim technology (which can be put in place immediately well before DNSSEC is fully deployed), known as Cache Defender, to provide protection against cache poisoning of the 15 million domains that we are responsible for. Other providers are working on similar innovative solutions.

Based on my long experience in operating large networks connected to the Internet, I believe that one of the most important areas for Congress to concentrate on is in improving the collaboration and communication between the public and the private sectors in dealing with these attacks. The Department of Homeland Security operates US CERT, which as part of its mission acts as a liaison between the public and private sectors. It is a start, but in my view, it is woefully underfunded and understaffed for the enormous task put before it. Ideally, I would like to see a much more focused collaborative effort between the public and private sector--a two way street, where we reach back and forth to help one another. While a lot of US CERT's focus is properly placed on protecting our national infrastructure and our Federal networks and resources, our economy also depends on a multitude of small companies. I would like to see the private partnership role expanded to include not only the major communications and IT companies, but smaller companies as well.

In summary, we face enormous escalating threats from all parts of cyberspace, both to our economy, and to the safety and well-being of our citizens. Furthermore, beyond the obvious and perennial calls for additional resources and funding, we need to concentrate on improving the collaboration between industry and government, and across government departments. It is an enormous task, but one well worth the effort.

Chairman Weiner and members of the committee, thank you for giving me the opportunity to testify on such an important subject.