the Availability Digest

www.availabilitydigest.com

Cyber Threats Surpass Terrorism

March 2013

Appearing before the Senate Select Committee on Intelligence in early March, 2013, James R. Clapper, Director of National Intelligence, testified that cyber threats have now surpassed terrorism as the top security threat facing the United States. This conclusion is documented in the United States Intelligence Community's assessment of threats to U.S. national security.[1]

The assessment noted that the world's threat environment is changing rapidly and radically. Attacks involving cyber weapons can be deniable by the perpetrators and unattributable to any source. Destruction caused by these weapons may be invisible, latent, and progressive. The fact that there has been an attack may not be immediately obvious. The effects of the attack may not be noticed until sometime after the attack has been launched and may play out over a period of time.

Cyber Threats

Our critical infrastructures, economy, and personal lives are becoming more entwined with technology and particularly with the Internet. In some cases, technology is advancing faster than our ability to understand the security implications and to mitigate potential risks.

The United States intelligence community recognizes two types of cyber threats – cyber attacks and cyber espionage.

Cyber Attacks

A cyber attack is an offensive operation intended to create disastrous physical consequences, to deny services, or to manipulate, disrupt, or delete data. Cyber attacks range from Distributed Denial of Service (DDoS) attacks, such as those launched recently against major U.S. banks, to attacks that can disable critical infrastructure.

Less sophisticated cyber warriors might deploy less sophisticated attacks for retribution or retaliation. Though these attacks are likely to cause inconvenience rather than destruction, there is the chance for unintended consequences due to unexpected system configurations or spillover to other nodes in a networked system.

[1] James R. Clapper, Worldwide Threat Assessment of the US Intelligence Community.
http://intelligence.senate.gov/130312/clapper.pdf

Cyber Espionage

Cyber espionage involves the intrusion into government and corporate IT systems for the purpose of acquiring confidential information. Such information might include classified government documents or corporate trade secrets such as patent applications in progress.[2] Most detected activity has targeted unclassified networks connected to the Internet. However, much of the nation's critical proprietary data is stored on these networks.

Today's highly networked information systems are providing opportunities for foreign intelligence services, trusted insiders, and hackers to collect sensitive U.S. corporate and national security data. The assessment notes that this may be allowing our adversaries to close the technological gap between our respective militaries.

Malware-as-a-Service

Cybercriminals are now selling tools openly on the Internet to enable easy access to critical systems. The Internet has become a source of free or low-cost malware that is easily customizable to meet every hacker's needs. Malware-as-a-Service significantly reduces the skill set needed by a cybercriminal to launch automated attacks.[3]

These hardware and software packages can give governments and cybercriminals the capability to steal, manipulate, or delete information on targeted systems. In addition, companies are selling professional-quality technologies to support cyberoperations, often branding these tools as lawful intercept or defensive security products. According to the assessment, foreign governments already use some of these tools to target U.S. systems.

Examples of Recent and Ongoing Cyber Threats

Bank DDoS Attacks

In September, 2012, a hacktivist group calling themselves the "Izz ad-Din al-Qassam Cyber Fighters" vowed to take down the online portals of several major U.S. banks if the YouTube video "The Innocence of Muslims" was not removed from the Internet. True to their word, they launched massive Distributed Denial of Service (DDoS) attacks against Bank of America, Wells Fargo, PNC Bank, JPMorgan Chase, U.S. Bank, Capital One, SunTrust Banks, and Regions Financial. Each attack took down the banks' online portals for a day or more.[4]

The attacks were massive, amounting to attack data rates of almost 100 gigabits/second. This is an order of magnitude more than standard DDoS attacks. Typically, DDoS attacks utilize infected networks of PCs (botnets) to send traffic. However, this group used hundreds of thousands of volunteer PCs as well as infected servers, each of which could generate the traffic of thousands of PCs.

The video was not removed, and in December the attacks were repeated against U.S. Bank, JPMorgan Chase, Bank of America, PNC Financial Services Group, and SunTrust Bank.[5] Recently, in early March, 2013, JPMorgan Chase was again attacked.[6] The group vows to continue these attacks until the offending video is removed from YouTube.

[2] A recent change in the patent law gives priority to the first to file, not the first to invent. If a patent application in progress can be stolen, a nefarious actor can file the patent application first and be awarded the patent.

[3] Malware as a Service, *Availability Digest*; December 2011.
http://www.availabilitydigest.com/public_articles/0612/malware.pdf

[4] Islamic Hactivists Attack U.S. Banks, *Availability Digest*; October 2012.
http://www.availabilitydigest.com/public_articles/0710/bank_attacks.pdf

[5] DDoS Attacks on U.S. Banks Continue, *Availability Digest*; January 2013.
http://www.availabilitydigest.com/public_articles/0801/more_bank_attacks.pdf

[6] Cyber attack stops access to JPMorgan Chase site, *Reuters*; March 13, 2013.

Stuxnet

The Stuxnet worm[7] is designed to attack and sabotage control systems used in power grids, pipelines, nuclear plants, railroads, and other facilities controlled by computers. Stuxnet is a very targeted piece of malware. It looks for specific industrial-control systems. When one of the right type is found, Stuxnet allows hackers to take control of the system and to manipulate it remotely without the operator knowing.

Stuxnet is ingenious. It has two major components. One intercepts valid commands being sent to the devices and replaces them with potentially dangerous commands generated automatically or by remote hackers. The other secretly records what normal operations at the facility look like and plays these back to the plant operators so that it appears to them as if the plant is operating normally.

The version of Stuxnet that was first detected targeted centrifuges that Iran was using to enrich Uranium. It caused the centrifuges to spin out-of-control at high speeds with the intent to destroy them.

The attackers have never been identified, but the virus was so complex and sophisticated that suspicion is focused on a government attacker. Though never confirmed, the suspicion is that the attackers were Israel and the United States.

Chinese Cyber Espionage

Many infections in corporate and government systems have been traced to a Chinese military facility. The Chinese deny any type of cyber activity against the United States. The attacks continue.

An interesting example occurred in October, 2012. The New York Times was preparing to expose a multibillion dollar fortune obtained through perhaps nefarious business dealings by relatives of Wen Jiabao, China's prime minister. It was then that suspected Chinese hackers infiltrated the Times' computer systems and stole the passwords of its reporters and other employees. Though the attackers could have wreaked havoc on the Times' computers, they did not. It seems their purpose was to identify Chinese citizens who may have provided information to the New York Times concerning Mr. Jiabao's business dealings.

Security expert firm Mandiant was hired by the Times and identified the attacks as similar to earlier attacks perpetrated by the Chinese military. The attacks were not made directly but rather through several computers at U.S. universities in an attempt to hide the source of the attacks.

The security experts found evidence that the hackers stole the passwords of every employee of the Times and used these passwords to gain access to the computers of 53 of the employees. The hackers evidently initiated their attack by snooping around for two weeks through back doors that they had opened in the systems until they found the domain controller that contained the user names and their passwords.

It is strongly suspected that the hackers gained access to the Times' systems through a spear-phishing attack that requires just one employee to download just one malicious email that will install malware. This malware can then siphon off oceans of data, including keystrokes, screen images, documents, microphones, and cameras.

Over the course of three months, the attackers installed 45 pieces of malware. The Times' antivirus protection found only one of them and quarantined it.

Mandiant reports that it has traced several other corporate cyber attacks to the Chinese military.

[7] Stuxnet – The World's First Cyber Weapon, *Availability Digest*; March 2011. http://www.availabilitydigest.com/public_articles/0603/stuxnet.pdf

Terrorism

According to the intelligence assessment, terrorism threats are in a transition period as the global jihadist movement becomes increasingly decentralized. The United States also is concerned about potential threats from Iran and Hezbollah.

- *Al-Qa'ida in the Arabian Peninsula (AQAP)* will continue to plan attacks on U.S. soil.
- *Al-Qa'ida-Inspired Homegrown Violent Extremists (HVE)*, though having been inspired by successes such as the 2009 attack at Fort Hood, will be involved in fewer than ten domestic plots per year.
- *Core Al-Qa'ida* has been degraded by senior personnel losses to the point that the group is probably unable to carry out complex, large-scale attacks in the West.
- *Al-Qa'ida in Iraq (AQI)*'s goals in Iraq will take precedence over U.S. plotting.
- Somalia-based *al-Shabaab* will remain focused on local and regional challenges.
- *Al-Qa'ida in the Land of the Islamic Maghreb's (AQIM)* will focus on local, U.S., and Western interests in North and West Africa.
- Nigeria-based Boko Haram will continue to aim at destabilization of the country and to advance extreme Islamic rule.
- Pakistan-based *Lashkar-e-Tayibba (LT)* will be the most problematic of the Pakistani militant groups and may evolve into a HAMAS/Hezbollah-like presence in Pakistan.
- *Iran* may be more willing to seize opportunities to attack within the United States but prefers to avoid direct confrontation as its priority is regime preservation.
- *Hezbollah* overseas terrorist activity is focused on Israel, and it is reluctant to face the U.S. outside of the Middle East.

Why Are Cyber Threats More of a Concern Than Terrorism

There are several reasons why the U.S. assessment is that cyber threats are now more worrisome than terrorism:

- The incidence of cyber threats is far greater than the incidence of terror plots, especially in the continental United States. There are literally millions of malicious probes made every day against our critical IT government and corporate infrastructures. Fortunately, few of these succeed; but the rate of system infections is significant. Those that do succeed, such as the bank DDoS attacks and the exposure of secret government documents by WikiLeaks, have caused significant damage.

  Terrorist attacks, which can result in loss of life or property, seldom succeed in the U.S. Many are thwarted by law enforcement and intelligence agencies.

- A successful cyber attack can cause a great deal more damage than a successful terrorist attack. For instance, it is unlikely that a terrorist attack could take down the entire electrical grid in the U.S. However, this is not an inconceivable result from a sophisticated cyber attack.

Fortunately, the intelligence community does not see an immediate threat to our critical infrastructure. The report states:

> "We judge that there is a remote chance of a major cyber attack against US critical infrastructure systems during the next two years that would result in long-term, wide-scale disruption of services, such as a regional power outage. The level of technical expertise and operational sophistication required for such an attack … will be out of reach for most actors during this time frame. Advanced cyber actors – such as China and Russia – are unlikely to launch such a devastating attack against the United States outside of a military conflict or crisis that they believe threatens their vital interests."

U.S. Cyber Counterattacks

Certainly, the U.S. has its own cyber counterattack strategies should it suffer a major attack. Network World reported that if the United States finds itself under a major cyber attack aimed at undermining the nation's critical information infrastructure, the Department of Defense is prepared, based on the authority of the president, to launch a cyber counterattack or an actual bombing of an attack source if the attack is determined to originate from a foreign country.[8] However, the preferred route would be to warn the source to shut down the attack before a military response is initiated.

The group responsible for analyzing the need for a cyber counterstrike is the National Cyber Response Coordination Group (NCRCG). Its three key members are the US-CERT computer-readiness team (part of the Department of Homeland Security), the Department of Justice, and the Defense Department. A big problem the group faces is how to coordinate if a significant portion of the Internet or traditional voice communications are suddenly struck down by a cyber attack.

So far, there has been no major cybersecurity event against the United States that has prompted the need for a national response. Nonetheless, the U.S. is training cyber fighters to do network warfare. It will have fighters in cyberspace.

Summary

We can see from our Never Again stories the growing predominance of cyber threats. Many of them can take our systems down for hours or days. If we are to provide continuous availability of our IT services, we must begin to extend our focus from hardware, software, human, and environmental faults to external attacks from malicious players.

Some of these attacks are intrusions intended to spy on us or to steal our data. Others, such as the DDoS attacks that hit the major U.S. banks, are intended to take down our systems. Today, these latter attacks are generally meant to exact retribution for some imagined or real grievance. Tomorrow, they may be intended to do significant harm to us for competitive or national-security reasons.

[8] U.S. cyber counterattack: Bomb 'em one way or another, *Network World*; February 8, 2007.