State Sponsored Cyber Hacking and Espionage

Daniel Nguyen

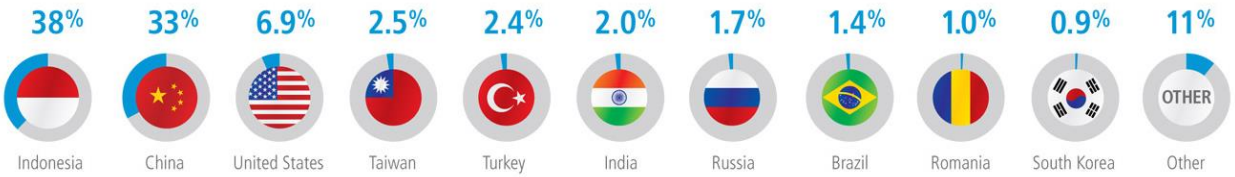
ICTN 4040

APRIL 13, 2015

State sponsored cyber hacking and espionage has come up in the news more often in the past couple of years. With ever increasing amount of classified information that is stored in databases and personal computers, the amount of state sponsored hackings and cyber espionage will increase dramatically. The objective of this term paper is to describe what state sponsored cyber hacking and espionage is and how it is being used in the world today. Some examples would be stealing classified information from militaries to use as their own, agendas such as hacking film producers if they release a certain movie, and the use of wiretapping and stealing personal data.

State sponsored cyber hacking and espionage uses funding and support provided by governments, sometimes anonymously and without acknowledgement. The goals are to gather intelligence, steal technology and designs, steal personal information, to sabotage, or to vandalize. Countries and people are affected negatively by cyber hacking and espionage. It costs the United States alone thousands of jobs and billions of dollars in damages a year. Stolen trade secrets and designs make the company less competitive when competing manufacturers duplicate items and sells them. People also have personal and sensitive information taken from them, such as social security numbers, bank account numbers and records, and personal emails. With the constant security threats facing the consumer, more money is spent to prevent and defend against such attacks. Companies have to hire information security professionals to harden their networks and block them from malicious attacks and data breaches.

Many countries participate in state sponsored cyber hacking and espionage. When it comes to the percentage of the number attacks in the second quarter of 2013, Indonesia comes in first place with 38%. It is a surprise to many who believe it was China that lead all countries in cyber-attacks, but they come in second place at 33%. The United States comes in at 6.9%, Taiwan at 2.5%, Turkey at 2.4%, India at 2% and Russia at 1.7%. These numbers will only increase with the amount of data being stored in the cloud and as more countries are capable in cyber hacking and espionage.



One example of stolen technology from state sponsored cyber hacking and espionage is the new United States air force F-35 Lightning II 5th generation fighter jet and China's new J-31 fighter jet. The two airplanes look nearly identical with design and technical specifications very similar. It was later revealed that a data breach occurred in which technology and designs were obtained from Lockheed Martin and its contractors. Edward Snow, the infamous NSA leaker, revealed that China had large scale espionage programs trying to learn the secrets of the Australian version of the F-35. As much as 50 terabytes of data and information was copied or taken. "U.S. National Security Agency whistleblower Edward Snowden said Chinese spies stole a huge volume of data related to Lockheed's F-35 Joint Strike Fighter, the Australian Associated

Press reported, and military experts say Beijing likely used the information to help develop its latest generation of fighters." (IBT)

Some of the recent major campaigns in the world include Shady RAT, Red October, APT1, Flame, PRISM, DarkSeoul, Sony Pictures, and Stuxnet. Even though malware attacks and data breaches seem to occur almost daily, these attacks were some of the most prominent in the modern day of cyber-attacks and surveillance.

Shady RAT (Remote Access Trojan) hack, was first discovered by McAfee. The attack used spear-phishing techniques to gain access. E-mails that appear to be legitimate are sent to employees of an organization, and then in turn those infected attachments contain exploit code that compromises the system. Typically these are zero-day attacks in which anti-viral and anti-malware programs cannot detect because the signatures are not of previous types of viruses and malware. With employee computers now compromised, the hackers can install RAT software and it allows them to monitor their system long-term. They can collect credentials, probe the network, and the exfiltration of data for exploitation or own use.

The Red October attack was first discovered by Kaspersky and the malware targeted governments and political groups in January 2013. The majority of the attacks and infections were found in Russia and Kazakhstan. One sign that it was a state sponsored attack was that it included a "resurrection module" which tricked the users to think that it had been removed from their system. "Attackers created unique, highly flexible malware to steal data and

geopolitical intelligence from target victims' computer systems, mobile phones and enterprise network equipment.” (V3)

The APT1 attack was first discovered by Mandiant in February 2013. The APT1 malware systematically stole hundreds of terabytes of data from at least 141 organizations. When traced to the source of the attacks, it was discovered that it was linked to a Chinese military unit based in Shanghai. Further evidence included that in over 97% of the 1,905 attacks that Mandiant observed, it was connecting to the same unit that was linked to the Chinese military. APT1 also used IP addresses registered in Shanghai and systems were set to simplified Chinese language. “From our unique vantage point responding to victims, we tracked APT1 back to four large networks in Shanghai, two of which are allocated directly to the Pudong New Area.” (Mandiant)

The Flame malware attack centered on Iran in May 2012. The malware was spread through an infected USB drive that was used on company computers. Some of the key objectives of the malware was to monitor the network, disk scanning, screen capturing, recording sounds from the built in microphones. Kaspersky discovered that the malware had MD5 hash and filenames that appeared only on customer machines from Middle Eastern nations. “"Flame can easily be described as one of the most complex threats ever discovered. It's big and incredibly sophisticated. It pretty much redefines the notion of cyberwar and cyber-espionage," Kaspersky researcher Alexander Gostev said at the time.” (V3)

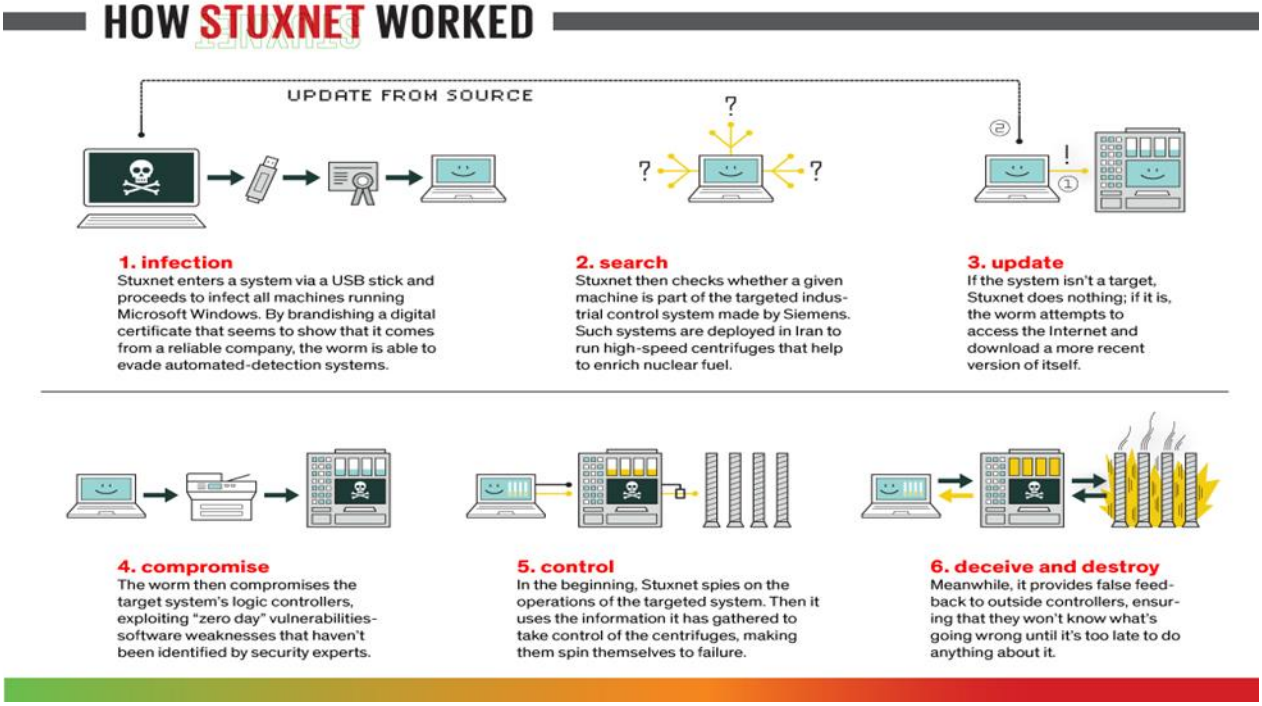
The PRISM surveillance program was both used by the National Security Agency and the United Kingdom's GCHQ. The purpose was to provide mass surveillance for data gathering of web users and governments. Phones of world leaders were tapped and bugged to monitor them. Encryption keys were broken to ensure that national security would be kept safe. One of the positives of this PRISM surveillance program was that it foiled an Islamic plot to attack New York City's subway system. It asks the question of whether people favor this type of mass surveillance program in the name of national security or do they covet their privacy more than anything.

DarkSeoul was a malware attack that occurred on the 63rd anniversary of the Korean War. It was designed to be setoff precisely at 2PM on March 20, 2013. It was believed that the hacker group under the alias of the DarkSeoul gang was working on behalf of the North Korean government. The malware affected television stations and banks. "The attackers left a calling card a day after the attacks in the form of a web pop-up message claiming that the NewRomanic Cyber Army Team was responsible and had leaked private information from several banks and media companies." (McAfee)

The Sony Pictures attacked occurred on November 24, 2013. Employee computers were locked out with a glowing red skeletons appearing on screens claiming that GOP, Guardians of Peace, were responsible for the attack. Speculation was that North Korea had some involvement in this attack because of the many protests and objections they brought to the UN. The movie depicts the life and gruesome death of their dictator Kim Jong Un. The FBI came out

with results that North Korea did indeed hack into Sony Pictures, stole and vandalized their systems. In response to the attacks of an American company, President Obama said he would "respond proportionately" to the attacks of Sony Pictures. On December 22, 2013, North Korea's internet is knocked out or greatly limited for several days. The name of the malware was later called "Destover".

Stuxnet was a malware that was introduced by an infected USB drive. It is spread through Microsoft Windows and targets Siemens industrial control systems, specifically PLCs, or Programmable Logic Controllers. The Stuxnet malware in this case targeted centrifuge equipment being used to refine uranium at Iran's nuclear facilities. The goal of the malware was to spin the centrifuges at a higher than normal speed so that it would lose control and destroy itself. While this occurred, computers reported that all systems and controls were behaving normally. Stuxnet reportedly destroyed 1/5th of Iran's centrifuges, effectively limiting their ability to create nuclear fuel for power plants or weapons. "It will be remembered as the opening act of cyber warfare, especially when viewed in the context of the Duqu and Flame malware which is outside the scope of this paper." (Langner)



In today's world more countries are turning to cyber warfare to accomplish their goals. State sponsored cyber hacking and espionage is on the rise, leading to more security risks for companies and individuals. The growing amount of data and activity on the internet will only further increase the number of attacks and espionage. A company can put a lot of resources into stopping these kinds of attacks, but there will always be vulnerabilities. A user should adhere to the safe practices when storing data or putting personal information in public places because people never know where their information might end up or how it will be used.

References

Aperovitch Dmitri, “Revealed: Operation Shady RAT” McAfee, 2011 *
http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

Langner Ralph, “To Kill a Centrifuge” Langner, November 2013 *

http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

Sherstobitoff Ryan, Liba Itai, “Dissecting Operation Troy: Cyberespionage in South Korea” McAfee, 2013 *

http://www.mcafee.com/us/resources/white-papers/wp-dissecting-operation-troy.pdf

Walter Jim, “Flame Attacks”: Briefing and Indicators of Compromise” McAfee, 2012 *

http://www.mcafee.com/us/resources/white-papers/wp-mcafee-skywiper-brief-v-1-6.pdf

Mandiant: APT1 Exposing one of China’s espionage units *

http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Wikipedia: PRISM (surveillance program)

http://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29

Pagliery, J. (2015, March 16). Ex-NSA director: China has hacked "every major corporation" in US. Retrieved April 10, 2015, from http://money.cnn.com/2015/03/13/technology/security/chinese-hack-us/

Top 10 worst state-sponsored hacking campaigns. (2014, February 21). Retrieved April 10, 2015, from http://www.v3.co.uk/v3-uk/news/2329347/top-10-worst-state-sponsored-hack-campaigns-from-prism-to-stuxnet-and-mask

Sherr, I., & Rosenblatt, S. (2014, December 20). Sony and the rise of state-sponsored hacking. Retrieved April 10, 2015, from http://www.cnet.com/news/sony-and-the-rise-of-state-sponsored-hacking/

http://assets.entrepreneur.com/article/think-china-no-1-country-hacking-think.jpg