Industrial Espionage: The Cyberspace War

Dimitrius F. Rivera
Master in Computer Science
Dr. Sandra Fonseca
Electric and Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

***Abstract* —** *As you may know, the World Wide Web has become an essential part of our everyday lives. Electronic communications, storage systems and computer networks in general have given us the freedom to do things we never thought possible. However, with these new forms of communication and technology come newer and more elaborate ways of property theft and sabotage. In this paper we will look at the long history of Industrial Espionage, its current world leading offenders, and common hacking tools, techniques and attack sequences used by infiltrators. We will also cover appropriate defensive techniques or countermeasures, and go over domestic and international laws and penalties that apply to those that are caught. In the end, understanding the history of Industrial Espionage, knowing the tools, techniques and attack sequences, and learning what countermeasures to use against attackers will give us the necessary knowledge we need to protect our networks against cyber espionage threats.*

***Key terms* —** *Cyber Espionage, Cyber Warfare, Industrial Espionage, Malicious Software.*

INTRODUCTION

Cyber war skips battlefield. Systems that people rely upon, from banks to air defense radars, are accessible from cyberspace and can be quickly taken over or knocked out without first defeating a country's traditional defense [1]. This quote may seem a little over the top since we will not be discussing National Security issues in this paper, however, it is indeed a good analogy to use when talking Industrial Espionage in this Internet warzone we now live in.

So how can Industrial Espionage be associated to the many horrors of war? Before we can answer this question we must first understand the intricacies of Industrial Espionage and what is gained by using such a practice. A widely used definition can be found on the Investopedia website which states that Industrial Espionage is, the theft of trade secrets by the removal, copying or recording of confidential or valuable information in a company for use by a competitor [2].

Now that we have defined Industrial Espionage we understand that just like in war there needs to be a reason or an objective for a country or an outside entity to want to start a war. In the corporate world that objective can be enormous caches of valuable data consisting of any or all of the following:

- Marketing Plans
- Trade Secrets
- Client lists
- Personnel records
- Production processes
- Customer billing information
- Company blueprints for new technologies
- Personnel records
- Confidential financial data

As you can see it is no secret that companies have numerous amounts of data available at any given moment and obtaining that data is the ultimate goal of the infiltrator. With that said, we need to understand what weapons, in this case tools, our enemies will be using to get what they want. The following list depicts the tools an attacker could use when trying to infiltrate a specific company's infrastructure:

- Social Engineering
- GUI intrusion tools
- Email propagation of malicious code
- Wide-scale use of worms
- Automated probes and scans

- Rogue Access Points (APs)
- Network sniffers
- Packet spoofing
- Session-hijacking
- Cyber threats & bullying

The above list depicts only a fragment of the vast arsenal of cyber weaponry readily available to those looking to exploit corporate data. As we can see, these tools not only include software and hardware, but also contain techniques such as Social Engineering which can also be used as a cunning tool to gain access to a company network.

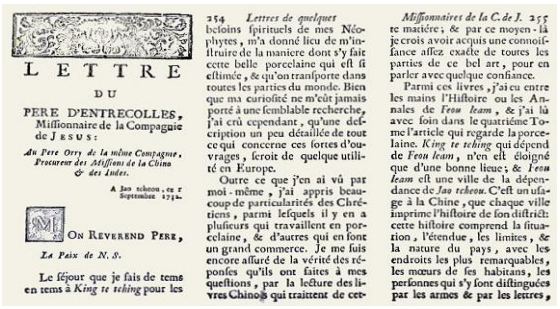
What else would you say is another key element in the cyberspace war? Every good General knows that one of the most important elements when devising a wartime strategy is the stage where the war will take place - the battlefield. In our case the battlefield is nothing other than; Cyberspace, the Internet, or as many of us have come to know by its familiar cliché "the cloud".

With the above mentioned, we have only began to touch on the subject of Industrial Espionage. Further along we will dive deeper into the history of Industrial Espionage, who is currently doing the spying, how it is being done, real-world examples, countermeasures that can be taken, and the fines and penalties if caught.

THE HISTORY OF INDUSTRIAL ESPIONAGE

Industrial Espionage has been around for centuries. One of the first documented cases of Industrial Espionage came at the hands of French priest Francois Xavier d'Entrecolles. In 1712 Francois, also working as a missionary at the time, stole the Chinese manufacturers' system of making porcelain and then wrote letters that revealed the secret to European manufactures (Figure 1 shows one of Francois' many letters).

Later the French would be accused of Industrial Espionage during the Industrial Revolution. Apprentices were placed in English factories and trades persons enticed abroad in order to get hold of new technology. This led to the first legislation against corporate espionage being passed. It was also the start of a long and ongoing battle to secure trade secrets and intellectual properties [3].



LETTRE

DU

PERE D'ENTRECOLLES,

Missionnaire de la Compagnie de JESUS:

Au Pere Orry de la même Compagnie, Procureur des Missions de la Chine & des Indes.

A Jao tcheou, ce 1 Septembre 1712.

MON REVEREND PERE,

La Paix de N. S.

Le séjour que je fais de tems en tems à *King te tching* pour les

254 *Lettres de quelques*

besoins spirituels de mes Néophytes, m'a donné lieu de m'instruire de la maniere dont s'y fait cette belle porcelaine qui est si estimée, & qu'on transporte dans toutes les parties du monde. Bien que ma curiosité ne m'eût jamais porté à une semblable recherche, j'ai crû cependant, qu'une description un peu détaillée de tout ce qui concerne ces sortes d'ouvrages, seroit de quelque utilité en Europe.

Outre ce que j'en ai vû par moi-même, j'ai appris beaucoup de particularités des Chrétiens, parmi lesquels il y en a plusieurs qui travaillent en porcelaine, & d'autres qui en font un grand commerce. Je me suis encore assuré de la vérité des réponses qu'ils ont faites à mes questions, par la lecture des livres Chinois qui traitent de cet-

Missionnaires de la C. de J. 255

te matiére; & par ce moyen-là je crois avoir acquis une connoissance assez exacte de toutes les parties de ce bel art, pour en parler avec quelque confiance.

Parmi ces livres, j'ai eu entre les mains l'Histoire ou les Annales de *Feou leam*, & j'ai lû avec soin dans le quatriéme Tome l'article qui regarde la porcelaine. *King te tching* qui dépend de *Feou leam*, n'en est éloigné que d'une bonne lieue; & *Feou leam* est une ville de la dépendance de *Jao tcheou*. C'est un usage à la Chine, que chaque ville imprime l'histoire de son district: cette histoire comprend la situation, l'étendue, les limites, & la nature du pays, avec les endroits les plus remarquables, les mœurs de ses habitans, les personnes qui s'y sont distinguées par les armes & par les lettres,

Figure 1
Letter Revealing Secret of Chinese Porcelain System

As we have learned piracy was a big deal even in those days. Knowing the amount of economical gain a country, or companies, could achieve the American government decided it wasn't going to just sit around while others benefited, thus they began to encourage such piracy. Encouragement came in many forms and even from influential personnel during the founding of the United States. Alexander Hamilton, one of the founding fathers of the United States, and most notably the chief staff aide of George Washington, was one of these promoters of piracy whom in his 1791 "Report on Manufactures" called on the country to reward those who brought us improvements and secrets of extraordinary value from elsewhere [4].

With the increase of Industrial spies infiltrating companies abroad to export machines and personnel that could work those machines came strict laws. Great Britain became the frontrunner when it came to laws against the export of machines, and even banned skilled workers from emigrating. Anyone who violated the ban could lose their property and be found guilty of treason. This leads us to mention , "The efforts of Thomas Digges, America's most effective industrial spy, got him repeatedly jailed by the Brits—and praised by George Washington for his "activity and zeal." Of course Britain wasn't excluded from piracy themselves. In the nineteenth century Britain's East India Company sent a botanist to China to steal the technique for processing tea leaves and a collection

of tea plants. By doing so, this allowed the British to grow tea in India, thus breaking China's dominion on the market.

Fate would have it that China, once the principal target of outsiders, is now the biggest offender of Industrial piracy and the U.S. the main advocate for enforcing intellectual-property rules. Today many would use the word 'karma' to describe this shift in illicitly appropriating innovations. In other words, the U.S. sees China as they once saw us; a threat to the nation's economical, scientific and technological advancements.

Early Wiretaps

In the mid-1800s the invention of the telephone opened the doors of communication to a point were humanity never thought possible. Unfortunately it also opened the doors to intruders who throughout history have used all sorts of methods to spy on their targets. Phone lines, which were invented as the primary voice transport method that interconnected phones over short and great distances, were now being used to do such spying.

For many countries expanding this technology became a primary goal eventually overshadowing security concerns that may have been brought up due to the ease of accessibility to the noticeable phone lines. This security flaw led to what is known as wiretapping as the obvious choice for those trying to gather data. *Wiretapping* is the monitoring of conversations by a third party and didn't become a bigger issue until after 9/11. There are also two types of wiretapping: Passive wiretapping and Active wiretapping.

- Passive – collecting information to gain knowledge.
- Active – Attempting to alter the information.

The following figure shows wiretapping to be a very simple task (see Figure 2). All that is needed is access to the phone-wire and alligator clips to attach to the red and green wires, a speaker, telephone or a tape recorder.

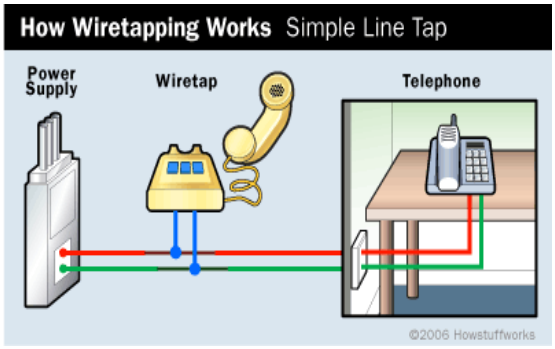


Figure 2
How Wiretapping Works

Modern Wiretaps

With the invention of computers, cellphones and the Internet wiretapping is no longer restricted to the familiar two-wire land based telephone line. Modern wiretaps tap into other forms of electronic communication, such as faxes, e-mails, and data transfers. Today wiretaps fall into one of the following four categories:

- Hardwired Wiretaps
- Soft Wiretap
- Recording Wiretap
- Transmit Wiretap

As technology has progressed we also see how wiretaps have changed to meet the times we live in. Unfortunately only having to worry about the occasional peeping Tom has long gone. Now we also have to worry about skilled cyber divisions that have been setup by competitors, and even are very own government.

Even though world government's use wiretaps as a means to prevent crimes and gather information on any upcoming threats it is still seen as an invasion of privacy to many. This is where many companies decide to use newer technologies (such as Voice over IP or VOIP combined with encryption technologies); in order to keep their secrets safe from outside entities.

As we discussed, the history of Industrial Espionage goes back many years, and although the objective is the same, the methods to gain access to data have changed dramatically. Such change is seen in the evolution of wiretaps which has evolved into many new forms. However, the one thing that

remains constant is the infiltrators goals. They are looking for profitability from someone else's' creativity, and they will lie, use deceit, or do just about any evil to obtain it.

Although much progress has been made in the last few years there are still many gray areas which need polishing and other areas where we haven't even scratched the surface. Making sure company assets are protected is indeed a huge obstacle that the global community must work together to tackle. After all, without appropriate laws and policies we are just allowing the perpetuator to steal the pie from the windowsill without even giving them a slap on the hand.

LEADING PERPETUATORS

The U.S. government accused the Chinese of being the world's "most active and persistent" perpetrators of economic spying, an unusual move designed to spur stronger U.S. and international action to combat rampant industrial espionage threatening U.S. economic growth [5]. The above statement comes from an article published by the Wall Street Journal back in 2011. The same article pulls information from the U.S. intelligence report published the same year. The report concludes that China and Russia are "the most aggressive collectors" of U.S. economic information and technology.

The Chinese Cyber-Crime Network

Sophisticated state-sponsored Chinese cyber espionage groups have also risen during the last few years. One of these groups dubbed Axiom has been known to go after intelligence benefiting Chinese domestic and international policies – an approach which combines commercial cyber espionage, foreign intelligence and counter-intelligence with monitoring of dissidents.

Axiom's work, the FBI stated in an industry alert, is more sophisticated than that of Unit 61398, a People's Liberation Army hacker group that was highlighted in a cybersecurity report last year. Axiom's activities appear to be supported by a nation state to steal trade secrets and to target dissidents, pro-democracy organizations and governments, said Peter LaMontagne, chief executive of Novetta Solutions, a Northern Virginia cybersecurity firm that heads the coalition. These are the most sophisticated cyber espionage tactics we've seen out of China [6].

Axiom malicious software has been detected on over 43,000 computers around the world belonging to government agencies, journalists, telecommunications and energy firms and even pro-democracy groups.

Russia Cyber Espionage Capabilities Now under the Microscope

Although cyber espionage has been linked more closely with the Chinese during the last few years the U.S. is now putting Russia's cyber espionage under the microscope. It is known that China has economic objectives, but Russia wants to show the world they are strong politically. Russia also wants to sell gas to Western Europe and oil to other nations, and is looking for advantages in those areas.

The below report by Recorded Future, a web intelligence company comprised with deep expertise in areas such as intelligence and security, show just how much Russia's cyber espionage has improved during the last few years:

From espionage, cyber warfare, and tracking regional geopolitical foes, Russia continues to build a cyber-capability with the potential to impact organizations worldwide. The scope of Russian cyber operations has only recently been discovered by cybersecurity firms. In contrast, Chinese cyber operations have been known for over a decade due to their sloppy operational procedures and direct attribution. Russia however, continues to lead the way in stealthier malware and operations making their efforts harder to identify and analyze [7].

FireEye, another global security firm, says that it is difficult to distinguish Russian government attacks from Russian hackers. Tom Kellerman, chief cybersecurity office at Trend Micro, states that, you only exist as a significant Russian

cybercriminal if you abide by three rules. You are not allowed to hack anything within the sovereign boundary; if you find anything of interest to the regime you share it; and when called upon for 'patriotic activities,' you do so. In exchange you get 'untouchable status.' [8]

According to The New York Times, FireEye is one of several global security firms that have connected the Russian government to cyber espionage and as mentioned before they are mostly interested in gaining advantages in the Energy sector. SurfWatch Labs, yet another cyber-risk intelligence solution organization, confirms just this in their most recent report which clearly shows that the Materials and Energy sector have seen the highest percent (59% and 47% respectively) of the cyber espionage attacks throughout 2014 so far.

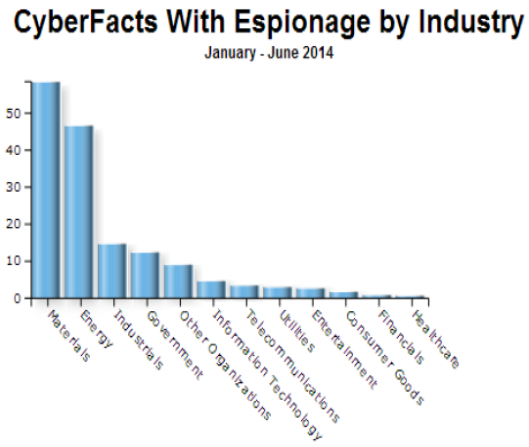


Figure 4
Espionage by Industry

As illustrated in Figure 4, the majority of the cyber espionage attacks in 2014 were aimed at gaining data on Materials. These attacks are aimed at attaining valuable company data such as company processes, plans and any other strategic information that can be used to gain an unfair advantage.

SurfWatch goes on to list the top trending targets related to espionage (see Figure 5) during the first six months of 2014. One of the important things to notice is the U.S. government being one of the most targeted. Many believe that the severity and complexity in which the U.S. has been targeted has indeed increased and may be directly related to the recent Edward Snowden revelations. This may have caused other nation states to increase or change their attacks.

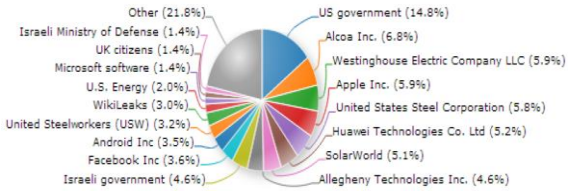


Figure 5
Top Trending Targets

Another import factor to mention is The Internet of Things (IoT), or the weakness in integrating the Internet into the business process, which has shown us that as the number of connected devices continues to grow so do the security implications for all devices connected. This can mean that as more devices are connected to a company network the more abundant poorly protected devices will be for infiltrators.

U.S. a Hypocrite on Cyber Espionage?

Cyber Risk and Security firms and cyber espionage analysts alike have shown that although many foreign countries participate in cyber espionage, China has been the most aggressive country in collecting foreign economic secrets – or is it? One of the many childhood sayings taught to us by our parents is that when you point a finger there are three fingers pointing right back at you. This simple childhood lesson can also be used as an analogy to describe the United States' double standard on cyber espionage. So the question remains… how much cyber spying does the U.S. do? To put it simple – a lot and we have been doing it for years!

Prior to Snowden's revelations about the U.S. government's extensive online surveillance programs the virtuosos of the U.S. intelligence community, the Office of Tailored Access Operations (TAO) has been breaking into China's computers and telecommunications systems for 15 years. With 600 techies (backed up by hundreds more support staff) working around the clock on

rotating shifts, TAO does everything from stealing passwords, data and text messages to analyzing foreign communication infrastructure for weaknesses that could be exploited by actual cyberweapons [9].

The TAO has also generated some of the best and most reliable intelligence information about what is going on in China and in countries around the world. TAO, a subdivision of the NSA, is known to be extraordinarily sensitive of its operations, thus even few NSA officials have complete access to information about TAO.

According to NSA officials, TAO's mission is a simple one. Collect intelligence on foreign targets by hacking into their systems, cracking passwords, compromising the security systems protecting the targeted computer, stealing data stored on computer hard drives, and then copying messages and data traffic passing with the targeted email and text-messaging systems. This technical term for the before mentioned practice is known as computer network exploitation (CNE).

Although the U.S. does collect foreign info there is little evidence that the U.S. steals secrets for the benefit of private industry. Many believe that the U.S. does not engage in such activity for both moral and practical reasons. However the case may be, whether the cybersnooping is for legitimate national security concerns or to fuel a nation's economy, it's like comparing apples to oranges. The fact of the matter is that cyber espionage is happening from both foreign soil and our very own backyard - even if it's not for economic gain.

Honorable 'Cyber-Spy' Mentions

China, Russia and the United States may be the lead players when it comes to cyber-espionage, but with the commonness of the Internet reaching more corners of the globe we have seen additional players enter the arena. A 2012 report from the U.S. Department of Defenses' Defense Security Service (DSS) says that with fewer than 20% of all reported attempts, was the Near East, which is identified as a region comprising of countries like Iran, Israel, Libya and Saudi Arabia. Entities based in Europe accounted for about 15% of the attempted attacks. With the revelations that came out of the Snowden leak, along with China's intricate Cyber Espionage network, and Russia positioning itself as a force to be reckoned with we are sure to see changes on who the victims and victimizers will be in 2015.

CYBER SPY TOOLS, TECHNIQUES AND ATTACK SEQUENCE

As we have come to learn in cyber espionage warfare attackers use many tools and techniques, but without a doubt the most successful method has been malware propagation. History and experience show that cyber espionage related malware attacks typically occur in the following sequence:

- Waterholing/Spear Phishing Initial foothold
- Second Stage Download & Tools

This order of succession may vary; however, this is the most common sequence of events associated with these attacks. Examples of this type of attack campaigns reported recently include Aurora, Ghostnet, Elderwood, VOHO, Facebook and Red October [10].

Watering Hole Technique

The watering hole, which plays off the tactic in which predatory animals stalk food by waiting at a popular watering hole, is where an attacker compromises a website that is of interest to the target and installs some sort of exploit system that will infect visiting machines with their malware of choice. A recent RSA intelligence report goes on to say that, this method is less surgical than others, but the wide net that is cast often can snag targets of opportunity that can be later exploited for further gain [10].

Spear Phishing (Social Engineering Technique)

Spear Phishing is a social engineering technique used by attackers where they disguise themselves as an individual or business that you know. They are out for the same things; passwords, account numbers, and the financial information on

your computer. Typically a “spear phisher” tries to gain some information from the target before sending the initial phishing email. They may collect information about the victim by searching the Internet. For example, they may scan social networking sites to view your friends list and even view a recent post.

Regin Malware - The New Stuxnet?

Symantec researchers discovered "the new Stuxnet", but it has been in operation since at least 2006. Obviously a highly advanced spying tool, better than the best malware out there. If you look at the times the code was put together it is clear that this is built in the UK with perhaps some help from the NSA [11]. The above is describing the recent discovery of Regin malware which has been compared, due to a few similarities, to the famous Stuxnet virus.

Stuxnet is a highly complicated computer worm discovered back in June 2010. It was developed to attack industrial programmable logic controllers. It is reported that Stuxnet ruined almost one-fifth of Iran’s nuclear centrifuges making it the very first known example of a cyber-weapon used to destroy physical infrastructure.

Stuxnet has three modules:

- A *worm* that executes all routines related to the main payload of the attack.
- A *link file* that automatically executes the propagated copies of the worm
- A *rookit* component responsible for hiding all malicious files and processes.

Regin is a highly encrypted piece of malware that hides its final form, similar to Stuxnet, from anyone looking to find it unless they have access to all five stages of the malware’s unpacking (see Figure 6). For this reason, Regin has had a 100% success rate in avoiding detectability. Another reason could be that it is still not clear how users become infected with Regin in the first place. Symantec reported that there is only one case of how a computer became infected with Regin, which was through Yahoo’s Messenger program. This goes to show that there is highly advanced malware out there that is undetectable, which is very bad news for companies trying to protect their networks and most valuable jewels.

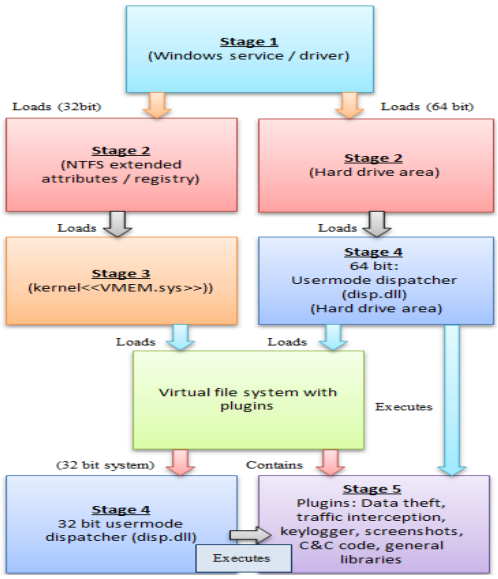


Figure 6
Multi-Stage Unpacking of Regin Malware

Unfortunately Regin is but one of the many types of malware used in the cyber espionage arsenal. Other types of malware have been known to use different code routines, and even attack cross-platform software. However with malware the preferred delivery method is usually the same; email, phishing, vulnerability exploits and port attacks.

Non-Malware Related Spy Tools

As mentioned malware is far in the lead when it comes to spy tools used by attackers but other honorable mentions are as follows:

Camouflaged USB drives – USB drives can be disguised, thus difficult to spot by the average security guard. They can also be mailed to a person or to them self at their place of work.

Wi-Fi Phishing – Since attackers know that corporate networks are being secured to the very last port Access Point (AP) cloning has become a tool for the attacker to bypass the corporate network altogether and attack the wireless client. An attacker simply downloads free software to their

PDA or laptop and impersonates any legitimate wireless hotspot AP. Once the user is connect the spy uses a "man in the middle" technique from which information is collected.

Software tools and Gadgets – There are countless devices and software one can download to assist in obtaining corporate and personal data. The majority of them can either be downloaded for free or bought online. A few items that are in existence during the creation of this paper are:

- Dish microphones used to filter out background noise to hear a conversation up to 300 yards away.
- Track-sticks which can be attached to cars to give out real-time GPS movement information.
- X-Ray envelope spray that allows the user to view the contents of a sealed envelope.

OPERATION TROY (DARK SEOUL) EXAMPLE

Tens of thousands of computers made to malfunction, the banking industry disrupted television companies unable to broadcast; all of these seem like titles to a megahit Sci-Fi movie, but on March 20th, 2013 to South Korea this was a dreadful reality. A reality coined "Dark Seoul" that virtually shut down three South Korea television stations and banks affiliated with ATMs and mobile payment systems.

Later it was known that Dark Seoul wasn't just some overnight malware infection, but part of a bigger whole named Operation Troy. McAfee confirmed this in a detailed analysis which indeed found that the cyber-attacks on Seoul, South Korea were actually the conclusion of a covert espionage campaign going back as far as 2009.

McAfee goes on to show the following key points of 2013's attack timeline (see Figure 7):

1. The remote-access Trojan was compiled January 26, 2013.
2. The component to wipe the master boot record (MBR) of numerous systems was compiled January 31.
3. An initial victim within the organization was spear-phished with the remote-access Trojan. This likely occurred before March 20, and possibly weeks prior to the attack.
4. The dropper was compiled March 20, hours before the attack occurred.
5. The dropper was distributed to systems across the victim organizations, and within minutes of execution the MBRs were wiped. This occurred around 2:00 pm Seoul time on March 20.

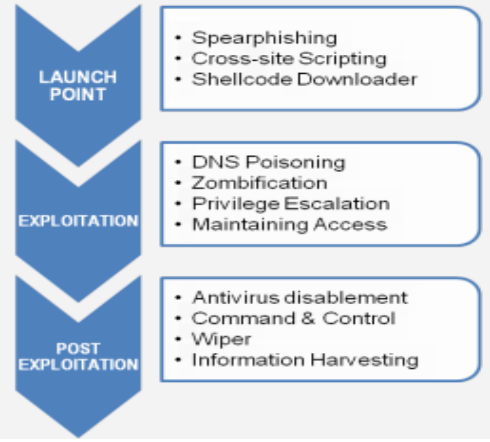


Figure 7
Dark Seoul Attack Vector

It is important to point out that there are countless cyber tools on the black market and other tools are being invented daily. There are also many techniques and attack sequences that have not even been discovered. With this said, what can companies do to protect their prized possessions? Is it even possible? The answer is yes, but it is not a simple one.

CYBER ESPIONAGE COUNTERMEASURES

With all that we now know there are indeed some defensive techniques, or countermeasures, that can be taken. For instance, using the Troy Operation as an example, the majority of computers compromised during the Seoul attack could have been prevented by having antivirus software up-to-date, making sure Windows security protection was enabled, and avoiding opening suspicious emails. The problem becomes more complicated with

Advanced Persistent Threats, or APTs, which cannot be prevented by using the measures above as a one-size-fits-all solution.

Since a company's internal workings, which can include network configurations, devices, etc., are unique each company needs to establish a comprehensive security policy tailored to their very own needs. This security policy should be relevant to today's threats and be sure to build on a sound understanding of the current threat landscape.

This individualized security policy should include the following:

Risk assessment, or risk evaluation, that includes:

- Establishing an attack response plan.
- Defining day-to-day security procedures.
- Implementing a mechanism for updating procedures – to keep up with the times.
- Regularly performing audits of IT security provisions.

Education of personnel about IT security risks which include:

- Precautions that employees can take in order to improve security.
- Current security risks and how cybercriminals may try to steal information and passwords.
- The costs to the business if attacked.
- Your company's security policy – and how they can meet its requirements.

Operating System strategies that include:

- Using newer OS's due to better security updates.
- Using 64-bit versions since they tend to be more resilient to cyber attacks.

A comprehensive IT security solution that includes:

- Patch management
- Vulnerability assessment
- Application controls
- Device controls – to help manage what devices are allowed to be connected to systems/networks.
- Web controls – which help manage, restrict and audit access to web resources

Mobile security which includes:

- A policy on not to Bring Your Own Device (BYOD) to the workplace.
- Using up-to-date Wi-Fi security procedures.

Companies should also be open-minded to innovative technologies and include multifactor authentication of computer access controls. In addition to the above countermeasures 'encryption technologies' also play a huge part in protecting private data. However, as pointed out recently by a secret US cybersecurity report, encryption technologies are not being implemented fast enough. This is indeed worrisome since encryption makes it possible for documents and messages to be unreadable to people who do not have the appropriate cryptographic key.

CYBER LAWS AND PENALTIES

Although many countries now have laws to deal with crime in cyber space it seems that we are still far off from seeing an international framework being implemented. The reason for this is that no government regards cyber espionage as a prohibited use of force. Persons caught of being spies can be punished, but international law contains protections for spies captured covered by diplomatic immunity. For instance, The United States could not prosecute a Chinese diplomat caught engaging in economic cyber espionage unless China waived the immunity and, absent a waiver, could only declare the Chinese national persona non grata, triggering that person's return to China [12].

Another strategy proposed by experts is to impose trade sanctions on countries engaged in cyber espionage and justify the sanctions under national security exceptions in World Trade Organization (WTO) agreements. However, as of this moment, WTO cases have not involved accusations against government sponsored espionage.

Other proposals focus on using U.S. laws and new strategies rather than international law. For example, the Obama administration's new strategy contains a five step approach:

- Focus diplomatic efforts to protect trade secrets overseas;
- Promote voluntary best practices by private industry to protect trade secrets;
- Enhance domestic law enforcement operations;
- Improve domestic legislation; and
- Public awareness and stakeholder outreach.

On a domestic-level the new strategy seeks to improve legal frameworks and to aim for stronger enforcement of existing laws and remedies for trade secret owners. At an international-level it seems the focus is to use formal cooperative agreements or arrangements with foreign governments.

CONCLUSION

Cyber espionage cannot be wished away, and though legislation helps, it will not eliminate the problem. It is up to individual companies to defend themselves against persistent threats to their private data and intellectual property. An adequate defense should include a company-tailored security policy that is relevant to today's threats and builds on a sound understanding of the current threat landscape. By doing so, enterprises will arm themselves with the protection they need to keep advanced persistent threats at bay, protect their data and keep their reputations intact.

REFERENCES

[1] Clarke, R. A., "Cyber War", *HarperCollinsPublishers* [Online]. January 18, 2015. Retrieved from: http://www.harpercollins.com/web-sampler/9780061992391.

[2] "Industrial Espionage", *Investopedia* [Online]. January 18, 2015. Retrieved from: http://www.investopedia.com/terms/i/industrial-espionage.asp.

[3] Ewen, J., "Corporate Espionage: Driving the Cyber Security Job Market", *JobSecurity* [Online]. January 18, 2015. Retrieved from: http://www.jobsecurity.co.uk/blog/corporate-espionage/.

[4] Surowiecki, J., "Spy vs. Spy", *The New Yorker* [Online]. June 9, 2014. Retrieved from: http://www.newyorker.com/magazine/2014/06/09/spy-vs-spy-3.

[5] Gorman, S., "China Singled Out for Cyberspying", *The Wall Street Journal* [Online]. November 4, 2011. Retrieved from: http://www.wsj.com/articles/SB10001424052970203716204577015540198801540

[6] Nakashima, E., "Researchers Identify Sophisticated Chinese Cyberespionage Group", *The Washington Post* [Online]. October 28, 2014. Retrieved from: http://www.washingtonpost.com/world/national-security/researchers-identify-sophisticated-chinese-cyberespionage-group/2014/10/27/de30bc9a-5e00-11e4-8b9e-2ccdac31a031_story.html.

[7] "Breaking the Code on Russian Malware", *Recorded Future* [Online]. November 20, 2014. Retrieved from: https://www.recordedfuture.com/russian-malware-analysis/

[8] Perlroth, N., "Online Security Experts Link More Breaches to Russian Government", *The New York Times* [Online]. October 28, 2014. Retrieved from: http://www.nytimes.com/2014/10/29/technology/russian-government-linked-to-more-cybersecurity-breaches.html

[9] Davidson, J., "China Accuses U.S. of Hypocrisy on Cyberattacks", *Time* [Online]. July 1, 2013. Retrieved from: http://world.time.com/2013/07/01/china-accuses-u-s-of-hypocrisy-on-cyberattacks/.

[10] Cox, A., "The Cyber Espionage Blueprint", *RSA FirstWatch*, The Security Division of EMC, Hopkinton, MA, Rep. Dragon WP 0713, 2013.

[11] Sjouwerman, S., "The New Stuxnet Discovered Called Regin How Does it Work?", *Knowbe4*. [Online]. November 24, 2014. Retrieved from: http://blog.knowbe4.com/bid/400453/The-New-Stuxnet-Discovered-Called-Regin-How-Does-It-Work.

[12] Fidler, D. P., "Economic Cyber Espionage and International Law", *ASIL*, Univ. Indiana [Online]. Vol. No. 17. March 20, 2013. Retrieved from: http://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving.