5-1-2013

Conceptualizing Financial Loses as a Result of Advanced Persistent Threats

Christopher Levine
Honors College, Pace University

Conceptualizing financial losses as a result of Advanced Persistent Threats

Pace University – Seidenberg School of Computing Science

One Pace Plaza, New York, NY

By Christopher Levine

Graduation date: May 15, 2013

Advisor

Dr. Darren Hayes

Abstract

Advanced Persistent Threat (APT) attacks are the biggest threat in the computing world. Currently, there is ample information available on how these attacks occur and who supports these attacks. However, there is dearth of information available that adequately describes the potentiality for financial losses. These losses are a direct result of the attacks themselves, however these attacks could only operate with the support of well-funded groups, such as nation states. Therefore, it is important to understand this relationship to conceptualize how these losses occur. In exploring the results of both Operation Aurora and Stuxnet, two famous APT attacks, it is evident that there are considerable financial losses that go along with APT attacks, thus making them a threat.

Table of Contents: **Pages**

1. Introduction

Advanced Persistent Threats more commonly shortened to APT are targeted computer attacks. These type of attacks are committed by APT groups, as APT attacks rely on human input and are not just automated pieces of code. Once the APT group has gained access to their target, attackers steal information that they desire such as trade and government secrets. However these types of attacks have also been known to be used for different purposes such as destruction of specific targets and monitoring of organizations, individuals and companies. APT attacks are successful because they specialize in remaining undetected in order to complete their objectives. They are also successful because they combine different techniques and tools in their operations which makes them hard to defend against **[1]**.No two APT attacks are the same, however there are some shared similarities in what is needed for a successful APT attack **[2]**.

1.2 Controversy over the proper definition of an APT

There are two main schools of thought on how an APT should be defined. The controversy being that one group, the "who" group, feels that an APT should describe a type of attacker; while the other group feels that the term APT should be used to describe a type of attack. Mandiant believes that the term APT should represent a specific group of attackers, they state that they "do not use this term in its diluted sense — as a generic category of threats", and they are not the only group who feel this way **[3]**. The "who" group believes that the groups behind the attack are more significant than the process undertaken. There is some merit in this definition as these type of attacks can only be committed by entities with ample resources such as nation states due to the funding and time needed to properly conduct an APT intrusion. Also the motives behind an attack are important and different APT groups have different motives

which can change how the attack operates. Ultimately the "who" group believes that by changing the definition to a type of attack lessens the severity of the phrase.

The other group believes that because APT attacks use similar techniques and objectives they should be defined as a category of attack. When you can identify these attacks based on common occurrences it seems nonsensical to worry about a particular group, when any well-funded group could commit these types of attacks **[4]**. Jeffrey Carr best summarizes this argument: "When you have multiple "who's" operating with similar or identical methods, I think it makes more sense to name the method rather than the actor"**[5]**. While it is informative to understand who are committing these attacks, in the end you defend against the attack itself and not the group committing the attack.

1.3 The importance in the choice of the words Advanced and Persistent

Understanding the word choice of both advanced and persistent are key in understanding how APT attacks differ from other attacks. These types of attacks are advanced because of many reasons. APT attacks always have a specific target and because of this the APT groups can employ reconnaissance to understand and identify weaknesses in their target. When they have identified enough weakness, the APT group are able to craft a specific attack that will exploit these found weaknesses. In exploiting these weaknesses APT attacks blend differing techniques such as spear phishing, malware, and social engineering to accomplish their goal **[2]**. Additionally these attacks often utilize zero day exploits, computer application vulnerabilities that are previously unknown of **[6]**. It is very costly and time consuming to discover these vulnerabilities and because of this attacks that utilize them are uncommon **[1]**. These attributes are very different from mass market attacks, a computer attack intended for a large audience.

Those type of attacks often use an all-encompassing technique where one specific type of malware is used on a lot of people in the belief that casting a large net will achieve you better results. Mass Market attacks do not analyze weaknesses or commonly use zero day exploits. Due to these characteristics standard computer security devices cannot defend against APT attacks **[7]**.

Persistent is used to describe these attacks because they have a specific objective and will not stop until they accomplish that objective. Unlike other forms of attacks that seek immediate financial gain, APT attacks take as much time as needed to accomplish their goal **[2]**. As these attacks often require a lot of time, they specialize in avoiding detection. It is not uncommon for these types of attacks to last for years. Mandiant stated in their 2012 MTrends report that the median number of days before an attack was discovered was 416**[3]**. Another way these attacks are persistent is that they install backdoors. These backdoors allow the attackers to come back later to steal more data and are one of the ways they remain undetected **[3]**. Mass Market attacks are not supported for years and they are not particularly stealthy. If those type of attacks encounter any difficulty they will move on to a different target, conversely APT attacks will never move to a weaker target, they will continue to persevere until they win **[8]**.

It is these two aspects of APT attacks that make them a true threat. There is a specific goal and the attackers will invest the time, resources, and energy to accomplish their mission. If the attackers are having difficulties they will continue to persist and will not move on to different targets. These attacks are led by teams of people that can exploit discovered weaknesses and adapt to any situations. APT attacks often utilize advanced technology such as zero day exploits which is uncommon in other attacks. In their perseverance, they remain hidden and will continue

to be a threat until they are discovered. These properties truly make them one of the biggest threats in informational security today.

2. The stages of an APT attack

While no two APT attacks are ever the same, there are always common recurring trends, tools, and strategy used that can identify these attacks. Mandiant describes in their initial report on APT's, seven stages which they label as the "exploitation life cycle" **[7]**. The seven stages are

1. Reconnaissance
2. Initial Intrusion into the Network
3. Establish a Backdoor into the network
4. Obtain User Credentials
5. Install Various Utilities
6. Privilege Escalation / Lateral Movement / Data Exfiltration
7. Maintain Persistence

As these attacks are identified by the common recurring trends it is essential to understand the processes in each of the individual steps. The process behind an APT attack best illustrates the complexity and sophistication behind these attacks.

2.1 Reconnaissance

Reconnaissance is indispensable as gathering information about the target is needed for a successful APT attack. In gathering this information attackers can develop the best strategy for

entering the targeted computer network **[8]**. Attackers seek to gather information on both individuals that use the targeted network and the target network itself. During the reconnaissance individuals are identified that can be exploited to provide access to the network. These individuals can range from senior leadership such as CEO's to more common employees like administrative assistants **[7]**. Data is also gathered about the computer network itself in order to understand how they can move about the network. Examples of this information are what kind of software the computers on the network use, and how the network is structured among other things. Ultimately the goal of reconnaissance is to understand and identify the weaknesses of the target that can be exploited **[8]**. The reconnaissance phase on APT attack is particular important because the information identified will be used throughout the entire process of the attack **[9]**.

2.2 Initial Intrusion into the Network

After the APT group conducting the attack has gathered the necessary information during the reconnaissance phase, they launch the initial intrusion into the network. The ultimate goal of this attack phase is to place their malware onto a targeted computer. There are a variety of ways to achieve this objective but there are some common patterns. The most common is the use of spear phishing. Spear phishing is tricking a target using email communication into believing you are someone else and then getting them to download malware that will give the attacker access to the network **[7]**. An example of spear phishing is if the APT group knew that the employees of a targeted company attended an intercompany meeting they would craft an email where they would pretend to be an executive at the other company and attach a malicious file **[7]**. Another way the attackers can gain initial access is to infect a Universal Serial Bus (USB) stick which is particularly useful in situations where the targeted computer is not connected to the internet **[8]**. The malware uploaded differs in every attack and can range from common malware to advanced

zero day exploits **[6]**. The compromised machine will then be the entrance for the attackers into the network.

2.3 Establish a backdoor into the network

Once the initial intrusion into the network is successful, the attackers need to ensure that they can renter the network as needed. To accomplish this task, the attackers need to open multiple backdoors into the network they are targeting **[7]**. Installing backdoors is crucial because of two main reasons. The first reason is if the initial infected machine is discovered and taken out of the network, the APT group will still retain the ability to enter the network as needed. Backdoors are also important for attackers as they can be used to upload further malware onto the network **[10]**. To make the process of installing backdoors easier attackers try to obtain domain administrative credentials and transfer the credentials out of the network because these credentials provide them with the power to alter the computer network as they need. With the domain administrative credentials the attackers can utilize system level privileges which makes it seem to observers and security systems that nothing is amiss **[7]**. These backdoors are both a safety net for the attackers and useful for further compromising the network. Due to these factors, APT groups seek to install as many backdoors as they can.

2.4 Obtain User Credentials

The next step for the APT group is to gather user credentials. These credentials can range from user names, passwords, and any other form of authentication. With these credentials, the attackers can find and steal the data that is located on the various computers of the network and also disguise themselves as users of the network to avoid detection **[7]**. There are multiple ways that attackers can obtain user credentials. A prominent way that APT groups obtain user

credentials is to target domain controllers **[7]**. Domain controllers are servers within a Windows network within a computer network that store user credentials **[11]**. By targeting and infecting these domain controllers, APT groups can quickly gain access to both user account names and the password hashes that are associated with those accounts **[7]**. Password Hashes are encrypted passwords, and if decrypted will provide the plaintext password allowing the hackers to authenticate themselves as that user **[12]**. This method is good for acquiring lots of credentials quickly. Attackers also gain access to credentials from machines they compromised with their malware **[7]**.

2.5 Install Various Utilities

When attackers have access to the credentials of users on the network, they then install utilities that allows them to perform systems administration tasks. Some of the tasks that are done with these utilities are installing backdoors into the network, obtaining email from servers, and list current programs that are running **[13]**. These utilities are often installed on systems without backdoors installed which means that they were installed using the user credentials **[7]**. As in the case with installing backdoors, APT groups seek to compromise as many computer systems in the network so as to protect themselves in case they are discovered. For example if one system is discovered and removed from the network, the attackers know that they have been discovered. By compromising multiple computer, the APT group will only have to change their tactics slightly if they are discovered and then they can continue with their activities **[7]**. If one door closes to them, they can just open another one and due to this installing the software needed to compromise more systems is an important step of the process.

2.6 Privilege Escalation / Lateral Movement / Data Exfiltration

The machines that are initially compromised do not typically have access to the information the APT group is seeking. Attackers have to search the network which is not difficult for them as they have the credentials and software to do so and search for their information and transfer it out of the network **[13]**. Examples of information that might be removed from the network are emails, files, and attachments, nevertheless the data removed depends on what the attacker is seeking **[7]**. The best way for the attackers to remain hidden, is to remove the data slowly so as to not arouse suspicion by generating a lot of network traffic **[13]**.The most common way the attackers stealth is maintained is by congregating the data on staging servers and then compressing and password protecting the data **[7]**. From there the APT group sends the data out of the network to a server where they can retrieve the data from safely. Afterwards it is common for the attacker to delete the compressed files so as to leave no trace behind **[7]**.

2.7 Maintain Persistence

Finally attackers maintain persistence on the network. After all of the work that goes in to gaining access, the APT group conducting the attack want to ensure that they stay undetected and can reenter the network at will. APT groups maintain persistence by hiding any evidence that a breach has occurred. When a connection into a network is made, information is recorded. To avoid being given away by this, APT's blend their network traffic into the regular network traffic **[7]**. The hackers also delete any tools, files, and software that could indicate a compromised network **[3]**. Another way that Attackers maintain persistence is by varying the skills and techniques used while on the network. In changing the techniques and software attackers provide

no suspicious activities that can be noticed **[14]**. If they believe they are detected, the attackers change techniques and shift their focus to other compromised machines that are not known to be compromised. This flexibility on the side of the hackers is what makes these attacks such a threat. If they are not detected the attackers can just keep stealing whatever information they desire without you ever knowing.

2.8 Common themes during the attack process

The steps involved with committing an APT intrusion are lengthy and complicated. Throughout the process two major themes are prevalent. The first major recurring theme is the importance of patience and planning in an attack. Throughout the attack attackers always have the next step planned. APT groups perform reconnaissance in order to better know their target, and identify weaknesses in the network so that two factors can be exploited. They also identify targets on the network themselves such as domain controllers that will allow them to accomplish their goals easier.

The other main recurring theme is the importance that stealth plays in the attack process. APT groups constantly take measures to avoid being detected such as installing backdoors, hiding network traffic, and employing valid credentials. The effect of this is that it is very hard for conventional security to work properly. Basically if you are not looking for an APT attack, you will have a difficult time in detecting one. They are only typically discovered when the APT group makes a mistake.

3. Who are behind APT attacks?

Various groups utilize APT attacks to accomplish their goals. The majority of APT groups are backed by nation states because they require a lot of financial assets to conduct and

they require a lot of dedicated time. Other groups that are not backed by nation states such as criminal groups have conducted APT attacks but the rate of this happening is not comparable to APT groups that are backed by nation states. While there is no one country backing APT attacks, there are some nations that utilize APT attacks more often than others.

3.1 People's Republic of China

The nation that commits APT attacks the most is the People's Republic of China. There have been multiple incidents in which the evidence points towards China being behind the attack. The targets that China is suspected of committing APT attacks against are spread across different industries. China seems to have two major goals of their APT attacks, gaining information about those who criticize their country and gathering information that can bolster their core industries.

On January 30th, 2013 The New York Times newspaper reported that hackers of Chinese origin have been consistently attacking the newspaper and obtaining the passwords of reporters and other employees. The New York Times stated that the attack coincides with the release of an online investigation that indicated that relatives of Wen Jiabao, China's prime minister, had accumulated a lot of money due to their business dealings. In a manner that indicates a traditional APT attack, Mandiant, who the newspaper hired to investigate, stated that the APT group behind the attack only sought to obtain information related to the investigating into the Jiabao family. Other types of hackers would have taken the opportunity to seize any information they feel could be of benefit to them or others but these attackers had a specific target. The goal of these APT attackers was to discover information on who provided information the reporter who investigated the Jiabao family **[15]**.

This has not been the first reported attack by Chinese hackers on US media. In 2012, the Wall Street Journal announced that it had been breached at its Beijing Bureau. The target of this attack was Jeremy Page, a reporter who wrote about the murder of a British businessman which was responsible for the downfall of Bo Xilai, a Chinese politician. China is sponsoring APT attacks on western media targets for two main reasons, they want to know how the outside world views them, and they want to know where is the information originating from for stories that criticize China and Chinese officials **[16]**.

The intrusions that are more prevalent for Chinese APT groups are intrusions that seek to obtain information that can help build up their industries. Mandiant noted that the targets of Chinese APT attacks were emerging industries that China self-identified in their 12 year plan **[17]**. One example, is the case of Televent Canada LTD, now Schneider Electric. They reported in 2012 that intruders stole files related to one of their big software products OASyS SCADA. This product helps energy firms merge older computer assets with newer technologies. The attack on Televent Canada LTD was later traced to a Chinese hacking team known as the comment group because the malware used was commonly utilized in other attacks by them **[18]**.

Another incident of information theft was in an attack dubbed Operation Night Dragon by McAfee. In their report on Operation Night Dragon, McAfee states that there were two groups of targets. The first group of targets were various global oil, gas and chemical companies while the other group was individuals and executives in varying countries such as Taiwan and Greece. The overall goal of the attack was to obtain confidential information from these companies and individuals. McAfee provides the evidence that points the blame towards China. In the report they state that the computers that were removing data from these networks originated from Beijing IP addresses. McAfee also noted that the times when data was stolen

correlated with the Beijing workday which leads them to conclude that the attack was conducted by people working a regular job and not amateur hackers **[19]**.

While there is countless evidence that point to China committing APT intrusions, none is more damming than Mandiant's release of their report on APT1. In their report Mandiant claims that a group they designated APT1 is under direct control of the 2nd Bureau of the People's Liberation Army and is designated as Unit 61398. Mandiant found that Unit 61398 is responsible for computer network operations. They also unearthed that the requirements to be in Unit 61398 are to possess advanced computer skills along with having strong English proficiency. In addition there are public records that indicate that in early 2007, a new building was constructed for Unit 61398 located in Shanghai, which is referred to as the Unit 61398 Center Building. The building that is located there is large enough to provide offices for a large group of individuals required to operate the APT attacks committed by this group. Finally Mandiant observed that APT1 intruders during the attack connected to their home network used IP addresses registered in Shanghai and systems set to use the Simplified Chinese language. This evidence brought together demonstrates links Unit 61398 to APT1. The unit requires English proficiency and high technical skills. Unit 61398 also has a newly built, large facility that can support the people needed for an APT attack. Lastly APT 1 connected back to their network using Shanghai based IP addresses and had their computer language set to simplified Chinese. These attributes make Unit 61398 to be the best candidate for being the APT Group, APT1. As this operates in the People's Liberation Army we can summarize that the Chinese government are behind these attacks **[17]**.

The Chinese government repeatedly denies they are behind any APT intrusions. China's Foreign Ministry spokesman Hong Lei criticized allegations that designated China as utilizing

APT attacks when he stated "To presume the source of a hacking attack based on speculation is irresponsible and unprofessional."**[16]**. Along with Hong Lei, Chinese embassy spokesman Geng Shuang also denied Chinese cyber spying when he stated that "It is irresponsible to make such an allegation without solid proof and evidence," **[16]**.

Contrary to what Chinese official's state, the evidence, and the motives suggest Chinese sponsorship of these attacks. In the intrusion of the New York Times and the Wall Street Journal, the goal was to discover who provided information that painted Chinese officials in a negative light. In the cases of Telvnet and Operation Night Dragon, the APT groups behind these attacks were looking for trade and industrial secrets that could give an advantage to Chinese industries. Lastly Mandiant was able to directly tie Unit 61398 to APT1, which has committed countless acts of cyber espionage. They are not the only nation state committing APT intrusions though.

3.2 The Russian Federation

The Russian Federation is also widely suspected of committing intrusions into networks, Russia is interested in discovering weaknesses in other countries infrastructure. In 2009 it was revealed by the Wall Street Journal that Russia had attempted to map out various U.S infrastructure systems including the electrical grid. Dennis Blair, Director of National Intelligence has gone on the record as stating that Russia could disrupt elements of the United States information infrastructure if they wanted to **[20]**.Discovering weakness in other countries infrastructure is not Russia main use of APT attacks however.

The main goal of Russian APT intrusions are acquiring trade secrets, intellectual property and technology although not at a rate that is comparable to China **[21]**. An incident that indicates Russian involvement was disclosed in January 2013 by Kaspersky labs. They revealed that it had

uncovered a multi-year espionage campaign they named Operation Red October. Kaspersky in their report detailed that a cyber-espionage campaign had been ongoing for the several years. The group behind the attack had targeted various organizations located in countries around the world but mostly in Eastern Europe, Central Asia, and Former U.S.S.R members. The main goal of the attack was to gather intelligence from these various organizations. Russia has not been directly implicated by Kaspersky as being behind these attacks as they state that the information stolen could be sold in underground markets. However they do states that the information stolen is more useful to nation states than it would be to normal thieves **[22]**.

However the data that Kaspersky provides can be extrapolated to indict Russia's involvement in these particular network incursions. They state that the malware used in the attack was created by Russian speaking operatives. The length of these intrusions themselves indicates that these attacks were most likely state sponsored for two reasons. Due to the length of the attack, the APT group behind the attack has to be able to operate free from government persecution. Along with that is the fact that a criminal group of hackers would have a hard time procuring the funds to sustain such as large attack as they would likely move on to easier targets. **[23]**. The targets themselves were also a good indicator that Russia was behind the attack as the countries targeted were within their sphere of influence as they located mostly in the region of Eastern Europe, and Central Asia" **[22]**. Finally the target categories most targeted were governments and embassies which have little financial value for private hacking groups. So while there is no explicit evidence indicating Russia, as was the case with many of the Chinese APT intrusions, the evidence that is provided is a strong indication of Russia's involvement with Operation Red October.

The United States Government has indicated that along with China, Russia is committing cyber espionage. A report published by the Office of the National Counter Intelligence Executive in 2011 indicated that Russia's intelligence services have been collecting economic information and technology from United States organizations **[24]**. Robert Bryant, another US official stated that Russia is targeting our research and developments through their intelligence services and corporations **[25]**. Despite these accusations by the United States government the Russian government has not commented on committing cyber espionage.

3.3 United States and Israel

The United States along with Israel are suspected of committing APT style attacks due to Stuxnet. Stuxnet was an advanced computer worm that targeted Siemens industrial controllers that run uranium enrichment centrifuges used at Natanz Nuclear facility in Iran. Like a normal APT attack Stuxnet had a clear target as it was designed to cause no harm to non-targeted machines **[26]**.Also indicative of an APT attack is that Stuxnet had specific objectives, which was causing Iranian Centrifuges to destroy themselves. Stuxnet was so advanced that Kaspersky labs reported that Stuxnet could only have been backed with nation state support due to its complexity **[27]**. Roel Schouwenberg who helped disseminate the Stuxnet worm at Kaspersky best summarized how complex the Stuxnet code was when he stated that "a team of 10 people would have needed at least two or three years to create it" **[26]**. While a worm traditionally would not be considered an APT attack, the complexity behind the code and how it operates is indicative of an APT.

There is plentiful evidence that links both the United States and Israel to creating the Stuxnet worm. Some of the evidence that links these two countries to Stuxnet originates from the

code itself. The Stuxnet code was designed to utilize an unprecedented total of four zero day exploits **[26]**. While this is impressive, more important is how the code only attacked its intended targets. In Iran's nuclear facilities they used the P-1 centrifuge which is used to obtain enriched uranium that can fuel both reactors and bombs. These specific centrifuges are controlled by a type of Siemens controller known as P.C.S.-7 which are operated by complex software that is difficult to understand. Whoever conducted this attack had to understand the specific of how the Siemens controller software operated in order to manipulate them into causing damages to the centrifuges **[28]**.

The only two countries that had access to this kind of information were the United States and Israel. The United States had obtained the specific type of centrifuges that Iran uses, after Libya gave up its nuclear program. The United States then studied those centrifuges to uncover their weaknesses. In conjunction with this Siemens had in the past cooperated with one of the United States laboratories to identify the vulnerabilities in their machine controllers. This indicates that the United States had the necessary knowledge on both the weaknesses in the centrifuges and the controller software to properly design this attack **[28]**.

Israel helped in the process by providing an environment where they could test the Stuxnet worm. The Dimona Complex in Israel is believed to house the same type of centrifuges that the Iranian use. In this controlled environment both governments could utilize the equipment to perfect the Stuxnet worm. Israel provided knowledge on how the centrifuges operated which helped in conjunction with what the United States knew about the centrifuges. In working together both countries had the necessary knowledge needed for this attack to be successful. Officially the United States and Israel deny their involvement in creating the Stuxnet worm the evidence of the attack implicates that it was these two countries. **[28]**

3.4 Why are APT attacks utilized more often by nation states.

APT attacks are utilized more often by nation states for two main reasons. They allow the countries to advance their interests easily and because they cannot be punished for their actions. While there might be other countries committing APT attacks, they are unknown of as of this time. China, Russia, Israel and the United States constitute the majority of APT style attacks. While all of these countries utilize APT attacks for different goals, they all are used to advance the interests of that country. As provided in the examples China uses APT attacks to strengthen their industries and their control over their people. Russia uses theirs to map out weaknesses in other countries and also to steal information that can help them strengthen their industries and give them an easy completive advantage. The United States and Israel used an APT attack to delay the nuclear program of Iran without resorting to a declaration of war.

More importantly are that these type of attacks offer the countries plausible deniability. No matter what evidence is involved the leaders of these countries can always deny they are behind these attacks. As a result of this there are almost no consequences for committing APT attacks. While other non-nation state groups could theoretically conduct an APT attack, they do not have access to the resources or immunity from prosecution needed for success. Nation states can grant their own hacker groups immunity.

4. Losses that APT's can incur

When an APT intrusion occurs and the intrusion is not detected quickly, there is a potential for the target of the attack to sustain heavy losses. These losses are unique to each individual APT intrusion. While one company might suffer heavy financial losses due to stolen intellectual property another target might sustain losses due to destruction of equipment.

However most companies do not disclose when they have been the target of an APT attack. Companies that are targeted by APT attacks do not want this information being released for a variety of reasons. The main reason is that targets of an attack do not want to broadcast that they have weaknesses in their organization. Another factor why targeted organizations do not release this information is because notifying the public on an APT attack could a company's value to decrease. Due to this factor it is difficult to find exact details about the losses incurred.

Yet the lack of clear information on these loses is concerning because the details of the losses suffered can serve to greatly illustrate the threat posed by APT attacks. Despite understanding how the process occurs and who most often commits APT style attacks, understanding the true potential of losses that can suffered is important to understand these attacks. While financial losses are to be expected there are also unreported losses due to these attacks. Understanding the losses suffered by both Google and the government of Iran due to APT attacks can help to illustrate the true potential of APT attacks.

4.1 Losses suffered by Google as a result of Operation Aurora

On January 12, 2010 Google announced on their official blog that they had been targeted by an APT group based out of China. They stated that during the attack some intellectual property that they held was stolen. As Google continued to investigate they discovered more information there was more to this attack then just stolen intellectual property. First Google discovered that they were not the only target of the attack. Other companies were targeted in this attack with one example being Adobe Systems who would reveal to the public that they were a target of this attack. **[29]**. Google also identified that the stealing of intellectual property was not the primary motive of this attack. Google identified that the APT group were attempting to

access the Gmail accounts of Chinese human rights activists although the hackers were not successful. Finally in their investigation Google learned that Gmail accounts of advocates for human rights in China based in other countries, such as the United States had been compromised **[30]**.

The results of this APT intrusion angered Google greatly. They stated in their official blog post on the incident that "These attacks and the surveillance they have uncovered… have led us to conclude that we should review the feasibility of our business operations in China" **[30]**. Google would later as a response to this decide to stop censoring Google searches on google.cn, which is Google's search domain for Chinese users and instead redirect users to google.hk, google search domain for Hong Kong which is uncensored**[31]**. This action by Google forced them to eventually abandon the Chinese search market as China would not allow an unrestricted search engine.

One could argue that Google did not have to stop censoring their web searches and that this action was independent of the initial APT intrusion. Yet Google states in its code of conduct that the idea of "don't be evil" is central to the organization. Their response was not dictated by the loss of intellectual property but rather that the hackers were attempting to discover what human rights activists both in China and outside of China were doing. Based on this knowledge they were put in a tough position due to this APT intrusion. They could either look the other way or ignore their stated morals. Their actions as a result of APT intrusion resulted in momentous losses for them.

When Google effectively abandoned the Chinese search market, they abandoned the largest online market per users in the world. China in 2010 had around 420 million internet users,

which is 109 million users more than the second largest online market, the United States**[33][34]**. This loss of a market was momentous for Google due to how they derive the majority of their profit. 96% of Googles revenue originates from their ad services Adwords, and Adsense **[35]**. Both Adwords and Adsense rely on their search engine utility with which they are famous for.

Google does not operate a search engine in mainland China, and as a result of this they have lost a huge percentage of their market share in China. Before Google left the Chinese search engine market, they held 30% of the market, second only to Baidu, a local Chinese search engine **[36]**. The Google search engine was theoretically used by 126 million people in China, as they held 30% share in the internet search market and there were 420 million internet users in China in 2010. Though using search engines are an integral part of the internet, we cannot assume that every internet user in China used a search engine and that this number could be potentially off and should serve as possibility to what the actual numbers could reflect.

In 2012, Google as the result of transferring mainland Chinese users to their Hong Kong Service lost a share of the search engine market. At the end of 2012, Google only held 12 percent of the search engine market in China **[36]**. Over two years they have lost, 18% of the online search engine market in China. Also at the end of 2012 there were 564 million internet users in China **[37]**. Using this same math as before we can summarize that the internet users in China using google is around 67 million. Despite there being more overall internet users in China, Google between 2010 and 2012 has lost around 58 million users and has effectively halved people using their search engine in China. This trend is likely to continue and as Google's main revenue relies on it advertising services which in turn relies on its search engine will limit Google's potential in the Chinese market.

Google also suffered in the short term after the revelation of the attack. On the day of the initial announcement by Google that they had been the target of an attack the stock for Google ended at $590.48. From the period of January 12, 2010 where they first revealed the attacks to March 23, 2010, where they revealed that they were going to end mainland China's google search, the stock never hit as high as the January 12, 2010 closing prices. In fact it wouldn't be until April 15, 2010 where the closing price of Google stock eclipsed the January 12, 2010 closing value at $595.30. While this drop in closing value could be attributed to other factors, the main focus of Google in the news during this time was whether or not they were going to leave the Chinese search engine market **[38]**.

The APT attack on Google forced them to confront the situation they were involved in with China. If the attackers had just been after intellectual property, then Google might have continued to conform to China's censorship requirements. The revelation that the attackers were targeting human rights activists forced them to abide by the unofficial motto "don't be evil". Google ended up losing a lot in this attack, they lost their share of the search engine market in China, which in turn caused them to lose potential revenue. In addition to the loss of the market, they suffered the effects of dropping stock values which could have hypothetically discouraged people in investing in Google. While not affected in the traditional sense by an APT intrusion in the loss of intellectual property being the main factor of losses occurred, this case is still important to understand some of the potential for losses due to APT style attacks.

4.2 Losses suffered by Iran due to Stuxnet

The Stuxnet APT attack crippled Iranian nuclear facilities. As previously mentioned Stuxnet was designed to target Siemens controllers that operated the uranium enrichment

centrifuges at the Natanz nuclear facility. When Stuxnet gained access to the controllers it then used the controllers to cause the centrifuges to spin rapidly and destroy themselves. The exact number of destroyed centrifuges is unknown as Iran nor has the International Atomic Energy Agency released this information **[39]**.It is known that Iran decommissioned 1000 centrifuges in either late 2009 or early 2010. This information along with the admission by Iran that they had been targeted by a cyber-attack suggests that this is an accurate representation of the number of centrifuges that ultimately had to be replaced due to Stuxnet. As a result of their destroyed centrifuges, Iran shut down other centrifuges in use while they discovered what was behind the attack. The destruction of the centrifuges along with the forced shut down delayed Iran's ability to produce a nuclear weapon **[40]**.

The prolonging of Iran's ability to produce a nuclear weapons will hurt them due to sanctions against them. Various countries and multinational organizations have sanctions in place against Iran due to their uranium enrichment. The United Nations has had sanctions in place against Iran as a result of this since the passing of resolution 1696 in 2006**[41]**. The United States also has sanctions as a result of Iran's uranium enrichment since the passing of the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010**[42]**. President Obama during the signing of this act stated that the goal of this sanctions was to neutralize Iran's ability to produce nuclear weapons **[43]**. These sanctions will remain in place until Iran decides to suspend their uranium enrichment.

Despite these sanctions Iran is committed to uranium enrichment with their President Mahmoud Ahmadinejad directly stating that "the Iranian nation will not yield to pressure and will not let its rights be trampled on" **[45]**. Yet these sanctions have disastrous effects on Iran's economy. Exporting oil is essential to the economy of Iran as it is the country's largest source of

revenue. The various sanctions against Iran however have negatively affected their ability to export oil and as a result has caused damage to their economy **[45]**. As a result of their diminishing ability to export oil, the value of the Iranian currency the Rial dropped to its lowest point ever in 2012 and has dropped 80% of its value since the end of 2011**[46]**. In a statement before the house foreign affairs committee in 2010, William J. Burns, Undersectary of State best outlined the biggest lose to Iran. He stated that "Iran may be losing as much as $50-60 billion overall in potential energy investments, along with the critical technology and know-how that comes with them" **[47]**. Iran is losing their ability to maintain a strong economy due to these sanctions as evidenced by the currency value dropping and their loss of investments.

As a result of the economy suffering, so are the citizens of Iran. A Gallup poll conducted from December 12, 2012 to January 10, 2013, illustrates the feelings of the people of Iran regarding the sanctions against their country. 56% of Iranian adults, the majority feel that sanctions imposed by the US and the U.N have hurt Iranians livelihoods a great deal. Another 48% felt that these sanctions hurt their personal livelihoods a great deal. The poll also asked Iranian Adults to rate the wellbeing of their lives. 31% stated that they are "suffering" which according to the Gallup poll is one of the highest in that area of the world. Countries with a similar rate of "suffering" are countries currently in the middle of a war such as Afghanistan or are experiencing severe political unrest such as Egypt and Tunisia **[48]**.

As Iran has sanctions in place due to their uranium enrichment, the delaying of their ability to produce a nuclear weapon prolongs these sanctions. These sanctions damage Iranians economy and causes suffering to their people. While Iran does not have to maintain a nuclear program they feel as if it is a right they should be allowed. The delay in their nuclear program was a result of Stuxnet. Stuxnet was not designed to prolong these sanctions, however the

destruction of the centrifuges and subsequent discovery by Iran had the result of delaying the nuclear program. It is by this logic that we can attribute the losses due to sanctions as a result of Stuxnet.

Along with the losses due to sanctions, Stuxnet is also responsible for losses occurred due to the destruction of the centrifuges. There is no source available for the actual monetary cost of an IR-1 centrifuge, the type that Iran uses to enrich uranium. The centrifuges that were destroyed accounted for 10 percent of the centrifuges at the Natanz nuclear plant. These centrifuges are hard to replace because the sanctions in place prevent certain materials and technology needed from reaching Iran **[39]**. These centrifuges were eventually replaced but the damage was already done by that point.

Stuxnet has had a huge impact on Iran and their nuclear program. Stuxnet delayed the uranium enrichment process which will delay their ability to produce nuclear weaponry. As a result sanctions that are in place will continue due to Iran's refusal to cease uranium enrichment. While the losses due to sanctions can be attributed to this refusal to cease enrichment of uranium, it is clear that they do not intend to stop. However as Stuxnet pushed back this process, the sanctions will continue to have an adverse effect on that country. Iran's economy is hurting as is the wellbeing of their people. In addition to this, the loss of the centrifuges themselves were costly as they are hard to replace as the technology nor materials are easily available to Iran.

5. Conclusion

APT attacks are the biggest threat in the computing world. These type of attacks value stealth and patience, which allows for high levels of success in compromising a target. The steps involved illustrate their complexity, and a level of planning that is not involved in other forms of computer attacks. Since these attacks are advanced they are mostly backed by nation states which provide the APT groups with the time, resources, and immunity needed for success. Therefore APT groups are able to target varying industries, organizations, and even governments without fear of possible repercussions. APT attacks are an easy way for governments to advance their own interests.

Due to these multiple factors, APT attacks can result in huge losses for their targets. Losses that generally equate to millions of dollars, or more. Aside from financial losses there are a number of other losses that can occur. Google, after Operation Aurora, was forced to confront their own morality when they discovered Chinese sponsored hackers had been targeting human rights activists. While Google could have ignored this behavior they responded in a manner in accordance with their morals. As a result, Google lost an incalculable amount of potential profit, because they lost access to the entire Chinese search engine market. Due to the Stuxnet worm, the Iranian economy suffered due to prolonged sanctions. These sanctions, in turn, hurt the entirety of the Iranian populous. Currents reports on this topic do not properly address the magnitude of these financial losses. This is most likely due to the fact that these attacks are often not disclosed to the public. The potentiality for massive financial losses, as evident in Operation Aurora and Stuxnet, should make these APT attacks of higher importance.

6. References

[1] Blue Coat Systems Inc. (2011). Blue Coat Labs Report: Advanced Persistent Threats. [Online]. Available: http://www.bluecoat.com/sites/default/files/documents/files/Advanced_Persistent_Threats.0.pdf

[2] Damballa Inc. (2010). Advanced Persistent Threats(APTs). [Online]. Available: https://www.damballa.com/downloads/r_pubs/advanced-persistent-threat.pdf

[3] Mandiant Corporation. "M-Trends 2012". Mandiant Corporation. Alexandria, VA, 2012

[4] PCI Guru, "is it 'who' or 'what' that is important?" 2012, http://pciguru.wordpress.com/2012/04/15/is-it-who-or-what-that-is-important/

[5] J. Carr, "Is The Advanced Persistent Threat A "Who" Or A "What"?" 2011, http://www.forbes.com/sites/jeffreycarr/2011/02/08/is-the-advanced-persistent-threat-a-who-or-a-what/

[6] T. Bradley, "Zero Day Exploits: Holy Grail of the Malicious Attacker" http://netsecurity.about.com/od/newsandeditorial1/a/aazeroday.htm

[7] Mandiant Corporation. "M-Trends: the advanced persistent threat". Mandiant Corporation. Alexandria, VA, 2010

[8] A.K. Sood and R.J. Enbody, "Targeted Cyber Attacks: A Superset of Advanced Persistent Threats" IEEE Security and Privacy Magazine, Volume 11, no. 1, Jan-Feb 2013

[9] Mandiant Corporation. "M-Trends 2013". Mandiant Corporation. Alexandria, VA, 2013

[10] Thrive Networks. "How Hackers use backdoors to access a network". Staples Inc. Framingham, MA, 2013.

[11] B. Posey. "Networking Basics: Part 5 - Domain Controllers", 2006, http://www.windowsnetworking.com/articles-tutorials/netgeneral/Networking-Basics-Part5.html

[12] J. McGlinn. "Password Hashing", 2007, http://phpsec.org/articles/2005/password-hashing.html

[13] Command Five Pty Ltd. (2011). Advanced Persistent Threats: A Decade in Review. [Online]. Available: http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf

[14] Mandiant Corporation. "M-Trends 2011". Mandiant Corporation. Alexandria, VA, 2013

[15] N. Perloth, "Hackers in China Attacked The Times for Last 4 Months" The New York Times, January 30, 2013. [Online]. Available: http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=1& [Accessed April 21, 2013]

[16] S. Gorman, "Chinese Hackers Hit U.S. Media" The Wall Street Journal, January 31, 2013. [Online]. Available: http://online.wsj.com/article/SB10001424127887323926104578276202952260718.html?mod=WSJ_article_comments#articleTabs%3Darticle

[17] Mandiant Corporation. "APT1: Exposing one of China's Cyber Espionage Units". Mandiant Corporation. Alexandria, VA, 2013

[18] B. Krebs, "Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent", 2012, https://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/

[19] McAfee Inc. (2011). Global Energy Cyberattacks: "Night Dragon". [Online]. Available: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

[20] S. Gorman. "Electricity Grid in U.S. Penetrated By Spies" The Wall Street Journal, April 8, 2009. [Online] Available: http://online.wsj.com/article/SB123914805204099085.html

[21] E. Nakashima. "In a world of cybertheft, U.S. names China, Russia as main culprits" The Washington Post, November 3, 2011. [Online] Available: http://www.washingtonpost.com/world/national-security/us-cyber-espionage-report-names-china-and-russia-as-main-culprits/2011/11/02/gIQAF5fRiM_story.html

[22] Kaspersky Labs (2013). "Red October" Diplomatic Cyber Attacks Investigation. [Online] Available: http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation

[23] J. Reed. "Hunting Red October: Who done it?" , 2013, http://killerapps.foreignpolicy.com/posts/2013/01/17/hunting_red_october_who_done_it

[24] Office of the National Counter Intelligence Executive. (2011). Foreign Spies Stealing US Economic secrets in Cyberspace. [Online] Available: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

[25] C. Boldeen et al. "U.S. report blasts China, Russia for cyberattacks" USA Today, November 3 2011, [Online] Available: http://usatoday30.usatoday.com/news/washington/story/2011-11-03/china-russia-cybersecurity/51065010/1

[26] D. Kushner "The Real Story of Stuxnet" (2013) http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[27] Kaspersky Labs. "Kaspersky Labs provides it's insight on the Stuxnet Worm" (2010) http://www.kaspersky.com/news?id=207576183

[28] W. Broad et al. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay" The New York Times, January 15, 2011, [Online] Available: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=3&pagewanted=all&

[29] P. Prasad. "Adobe Investigates Corporate Network Security Issue" (2010), http://blogs.adobe.com/conversations/2010/01/adobe_investigates_corporate_n.html

[30] Google Inc. "A New Approach to China" (2010), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

[31] Google Inc. "A new approach to China: an update" (2010), http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html

[32] Google Inc. "Code of Conduct" Google Investor Relations, April 2012, [Online] Available: http://investor.google.com/corporate/code-of-conduct.html

[33] Internet World Stats. "China: Internet Usage Stats and Population Report" (2010), http://www.internetworldstats.com/asia/cn.htm

[34] Internet World Stats. "United States of America: Internet Usage Stats and Broadband Usage Reports" (2010), http://www.internetworldstats.com/am/us.htm

[35] G. McFarlane. "How does Google make it's money", Investopedia, November, 2012 [Online] Available: http://www.investopedia.com/stock-analysis/2012/what-does-google-actually-make-money-from-goog1121.aspx [Accessed: 20 April, 2013].

[36] M. Lee. "Google controls too much of China's smartphone sector: ministry", Reuters, March , 2013 [Online] Available: http://www.reuters.com/article/2013/03/05/us-china-google-android-idUSBRE9240B220130305 [Accessed: 20 April, 2013]

[37] China Internet Network Information Center "Internet Statistics Basic Data", [Online] Available: http://www1.cnnic.cn/IDR/BasicData/ [Accessed 20 April, 2013].

[38] Google Finance. "Google Inc Stock Prices between 1/12/2010 – 4/15/2010" [Online] Available: https://www.google.com/finance/historical?cid=694653&startdate=Jan%2012%2C%20

2010&enddate=Mar%2023%2C%202010&num=30&ei=9GNrUejUEIfd0QG7Kw&start=0

[39] D. Albright et al. "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" Institute for Science and International Security, Dec 2010 [Online] Available: http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

[40] D. Albright et al. "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report1" Institute for Science and International Security, Feb 2011 [Online] Available: http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf

[41] United Nations Security Council. "SECURITY COUNCIL DEMANDS IRAN SUSPEND URANIUM ENRICHMENT BY 31 AUGUST, OR FACE POSSIBLE ECONOMIC, DIPLOMATIC SANCTIONS" July 2006, [Online] Available: http://www.un.org/News/Press/docs/2006/sc8792.doc.htm

[42] Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010, [Online] Available: http://thomas.loc.gov/cgi-bin/bdquery/z?d111:H.R.2194:

[43] Office of the Press Secretary, "Remarks by the President at Signing of the Iran Sanctions Act" July 2010, [Online] Available: http://www.whitehouse.gov/the-press-office/remarks-president-signing-iran-sanctions-act

[44] L. Neisloss and M. Chance, "Iran president refuses to budge" CNN, September 2006 [Online] Available: http://edition.cnn.com/2006/WORLD/meast/09/01/iran.deadline/

[45] I. Arnsdorf, "Iran Oil Exports Seen Rising by IEA Even as Sanctions Widen" Bloomberg, March 2013 [Online] Available: http://www.bloomberg.com/news/2013-03-13/iran-oil-exports-seen-rising-13-by-iea-even-as-sanctions-widen.html

[46] S. Usher "Iran's rial hits an all-time-low against the US dollar" BBC News, October 2012, [Online] Available: http://www.bbc.co.uk/news/business-19786662

[47] W. Burns "Implementing Tougher Sanctions on Iran: A Progress Report" US Department of State, [Online] Available: http://www.state.gov/p/us/rm/2010/152222.htm

[48] M. Younis "Iranians Feel Bite of Sanctions, Blame U.S., Not Own Leaders" Gallup, Feb 2013, [Online] Available: http://www.gallup.com/poll/160358/iranians-feel-bite-sanctions-blame-not-own-leaders.aspx