Assignment 2:

Operation Aurora: A Review and Analysis

Corbin Osman

INTL440 – Cyber Warfare

Beth Subero

February 11, 2024

Introduction

In our world of evolving technology, there are vulnerabilities and threats that are ever present. Some malicious actors seek to attack individuals, companies, and organizations with the hopes of obtaining personal information, confidential data, money, and access to systems and networks. Others may launch attacks to disrupt or destroy servers, networks, and devices. In recent years there have been many different types of attacks from those with malintent, and while they are unfortunate events, we have the chance to learn from them and gain a better understanding of how and why they are performed.

This paper will explore the cyberattack known as Operation Aurora. It will cover the victims of the attack, the party that launched it, and the nature of the assault. The potential motivation behind the attack and the malicious party’s desired outcome will be theorized, and the success of the attack will be reviewed. The purpose of the paper is to inform readers about a real-world attack that occurred and help them better understand the intent and motivation behind the attacker’s actions. Readers will learn how unfortunate incidents can help cybersecurity specialists prepare for future threats and vulnerabilities. In studying Operation Aurora and similar attacks, individuals are able to draw upon real-world experiences and learn how they are performed in order to better understand malicious actor's intents and attack methods and how to protect against them.

Overview of Operation Aurora

The attack known as Operation Aurora occurred over the second half of 2009 and consisted of various cyberattacks that were targeted at several different companies and organizations. The name of the attack comes from a folder named “Aurora” which was found in the source code of many of the attacks launched (Zetter 2010). Reports of the attack were not shared until the start of the following year, with Google releasing the first reports of the attack and its effects on their company (Cha and Nakashima 2010). Additional companies would later claim to have been targeted by the attackers who utilized a phishing scheme and zero-day vulnerabilities to perform the attacks.

**Known Parties Involved in Operation Aurora**

While the exact number of parties involved in Operation Aurora is unknown, there are sources which have confirmed the involvement of a few specific groups in the attack. The attack originated from China, and The Elderwood Group, also referred to at times as The Beijing Group, appeared to be the backbone party behind the many attacks that were launched (Council on Foreign Relations 2010). Factors such as the domain names and IP addresses associated with information found surrounding the attack support the claim of The Elderwood Group’s involvement in the cyberattacks. Additional sources reported on the involvement of the Chinese Politburo along with Chinese public security experts (Shane and Lehren 2010).

The Elderwood Group is known to be a cyber-espionage organization that specializes in attacking second-tier or lower security organizations. The official name of the organization is unknown, and the name “Elderwood” was given to the attacking party due to the name appearing in source code that was found associated with the attack (Clayton 2012). Individuals and parties that appear to be connected to Elderwood may consist of Chinese activists, officials, and hackers.

**Reported Victims of Operation Aurora**

In January of 2010 Google reported that it had been the target of a recent cyberattack that originated from China. They also discovered that at least twenty other companies were involved in the attack along with various email accounts of individuals (Google 2010). Google worked to notify these and other companies they suspected of having been targeted by Elderwood. Over time more companies would report that they had also been victims cyberattacks that originated from China. Among these are notable companies Yahoo, Adobe Systems, Juniper Networks, and Symantec, to name a few. Reports concluded and confirmed a minimum of thirty-four victims from various industries, with the potential of more unreported victims having been targeted (Cha and Nakashima 2010).

**Probable Motivation Behind Operation Aurora and the Desired Outcome**

Due to the large number of companies and organizations that were targeted in this assault, there are various reports on different motivations and intents behind the attacks of Operation Aurora. Google reported that one of the purposes of the attack was to access email accounts of human rights activists located in China, US, and Europe-based areas. It is unclear what type of information they were searching for in the email accounts, as Google found that the content of information contained in email communications were not targeted by the attackers (Google 2010).

Another potential motive behind the assault was to gain access to essential computer and security systems. Gary Cohen reporting for Cybersecurity Pulse states that the attackers sought access to computer systems that offered elevated privileges and access. These systems were part of second-tier defense and technology companies and organizations, and it is believed that they were targeted in order to infiltrate systems belonging to the second-tier companies. Their goal may have been to infect the devices and systems with malware and backdoors so they could gain access to systems at a later date (Cohen 2022). From the many sources and reports on the various attacks, the hackers appeared to be after intellectual property of companies, control of critical security systems and devices, and the interactions of human rights activists.

Nature of the Attack

Operation Aurora consisted of various cyberattacks during the course of the several months it occurred. The primary attack methods utilized by Elderwood were spear-phishing attacks that were aimed towards the employees of their target companies. Email communications were sent to employees that incited them to click on links contained in the message. These links would take their victims to a site that would download and begin installing malicious trojan software onto their devices (Clayton 2012). In most cases this software would work to create backdoors into the systems and networks they had infected, allowing the attackers easy access to them at a moment’s notice.

Another method employed by Elderwood was infecting websites that were commonly visited by employees of the companies they were attacking. Many well-known and regularly visited websites implement strong levels of encryption and security, so the attackers instead focused their efforts on less secure websites that were still used by employees. They knew that it was just a matter of time before employees would visit the infected sites, and when they had, malware would begin installing itself onto their devices as users interacted with the website (Clayton 2012).

Once attackers gained access to the systems and networks they had infected, their goal was to search for valuable information and data to capture. Such is a common target of cyber criminals who may seek to sell the data and information or use it for their own personal gain. As was previously mentioned, some of these attacks targeted the emails of human rights activists who were searching for potential sensitive and confidential information that they could capture. Google reports that the email accounts of individuals that were hacked likely occurred due to the users falling for phishing scams employed by the attackers (Google 2010).

**Sophistication of Operation Aurora**

Operation Aurora is well known due to its sophisticated nature and relatively rapid occurrence. Elderwood exploited zero-day vulnerabilities in web browsers such as Internet Explorer, granting them access to some accounts and systems of their targets (Zetter 2010). These vulnerabilities are often known and recognized by the companies they threatened but have yet to be patched or prevented. The attackers recognized that by exploiting these vulnerabilities and infecting second-tier security and defense companies, they would have the potential to later attack first-tier or similar companies and organizations using backdoors that they had already created.

The attacks performed by the hackers were also advanced due to their efficiency in covering their tracks. Actions online and on devices and networks often leave digital fingerprints which can be traced back to their actor, but the Elderwood Group succeeded in utilizing strong levels of encryption to avoid common detection and prevention practices. Dmitri Alperovitch of McAfee commented that the levels of encryption used by Elderwood were advanced for their time. It was also noted that the types of companies targeted outside of the defense and security industries were not prepared for the sophisticated attacks launched against them (Cohen 2022).

However, despite the advanced nature of the attacks and the efforts employed to avoid detection, key factors and information were discovered that led investigators to the source of the attack. Technical evidence found, as shared by Cohen, such as the domain names and IP addresses of the attackers traced back to The Elderwood Group. While they were able to avoid detection during the course of the attacks, evidence was gathered to conclude the involvement of Elderwood in the many cyberattacks (Cohen 2022).

Success of the Attack and Victim Responses

Many companies were targeted by The Elderwood Group and others involved in the attack, but several of the victims reported that they did not believe their sensitive information or security systems were compromised (Cha and Nakashima 2010). Of the email accounts belonging to Chinese human rights activists, Google reported that only two appeared to have been accessed by the attackers (Google 2010). Other companies would not comment on the effects or success of the attacks launched against them, so it is unclear how exactly the attacks affected all of the companies that were involved in the attack. What is known is that The Elderwood Group and other parties continue to launch attacks to date, making it important for companies and organizations to focus sufficient time and resources to creating and maintain strong security systems and practices. This allows them to protect against potential attacks from various cyber criminal groups such as The Elderwood Group.

It is unknown how each and every company responded to Operation Aurora, but a few companies shared what the had done to protect against future attacks. Google responded to the assaults by quickly making changes to their infrastructure and security systems to ensure they offered strong protection for both themselves and their users (Google 2010). Symantec, a company that specializes in developing security software, reported that they are making plans to ensure they are providing strong security and protection for their customers (Cha and Nakashima 2010). It is important for companies that experience similar attacks to consider the immediate and lasting effects that come from threats and vulnerabilities they face. Even if systems and information do not appear to be in jeopardy following an attack, companies should review their security systems and policies and look for potential changes that would strengthen their security.

Conclusion

In reviewing Operation Aurora, it is evident that many of the companies which were targeted were not prepared for the level of attack they experienced. The Elderwood Group was able to take advantage of employees through phishing attacks and exploit zero-day vulnerabilities to bypass established security protocols and systems. Whether or not the victims were negatively impacted by the attacks, there are important lessons that can be learned from this cyberattack. All companies should consider training and educating their employees on phishing attacks, focusing on what they might look like, how they are dangerous, and how to properly respond to them. Additionally, companies should focus time and resources to patching or protecting against known zero-day vulnerabilities as quickly as possible. Because of their exploitive nature it can be difficult to respond to an attack which takes advantage of zero-day vulnerabilities, so companies should be proactive instead of reactive in their responses to the threats.

Operation Aurora also presents the fact that threat actors can be large in size and that their targets may consist of multiple companies. The Elderwood Group appeared to consist of various individuals and parties, and it is likely that they had access to vast amounts of research and information surrounding the systems and networks of their targets. They were also able to launch attacks against dozens of companies and organizations, and while they might not have been successful in all of their endeavors, they were still able to infiltrate many systems and networks with relative ease. As cyberthreats continue to grow and advance in their attack patterns and methods, both cybersecurity specialists and everyday users should take the time to learn about and prepare for the potential attacks of adversarial parties. In so doing their efforts to protect against cyberattacks may be improved and heightened.

Bibliography

Cha, Ariana E., and Ellen Nakashima. “Google China Cyberattack Part of Vast Espionage Campaign”. *Washington Post*, January 14, 2010. https://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html

Clayton, M. “Stealing US Business Secrets: Experts ID Two Huge Cyber ‘Gangs’ in China”. *The Christian Science Monitor*, September 14, 2012. https://www.csmonitor.com/USA/2012/0914/Stealing-US-business-secrets-Experts-ID-two-huge-cyber-gangs-in-China

Cohen, G. “Throwback Attack: Operation Aurora signals a new wea in industrial threat”. *Industrial Cybersecurity Pulse*, December 22, 2022. https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-operation-aurora-signals-a-new-era-in-industrial-threat/

Council on Foreign Relations. “Operation Aurora”. Accessed February 08, 2024. https://www.cfr.org/cyber-operations/operation-aurora

Google. “A new approach to China”. Accessed February 08, 2024. https://googleblog.blogspot.com/2010/01/new-approach-to-china.html

Shane, Scott, and Andrew W. Lehren. “Leaked Cables Offer Raw Look at U.S. Diplomacy”. *New York Times*, November 28, 2010. https://www.nytimes.com/2010/11/29/world/29cables.html?\_r=1&hp

Zetter, K. “Google Hack Attack Was Ultra Sophisticated, New Details Show”. *Wired*, January 14, 2010. https://www.wired.com/2010/01/operation-aurora/