Alex Banning, Gage Gutmann, Davis Lee
Computer Security — CPSC 448
December 5th, 2019

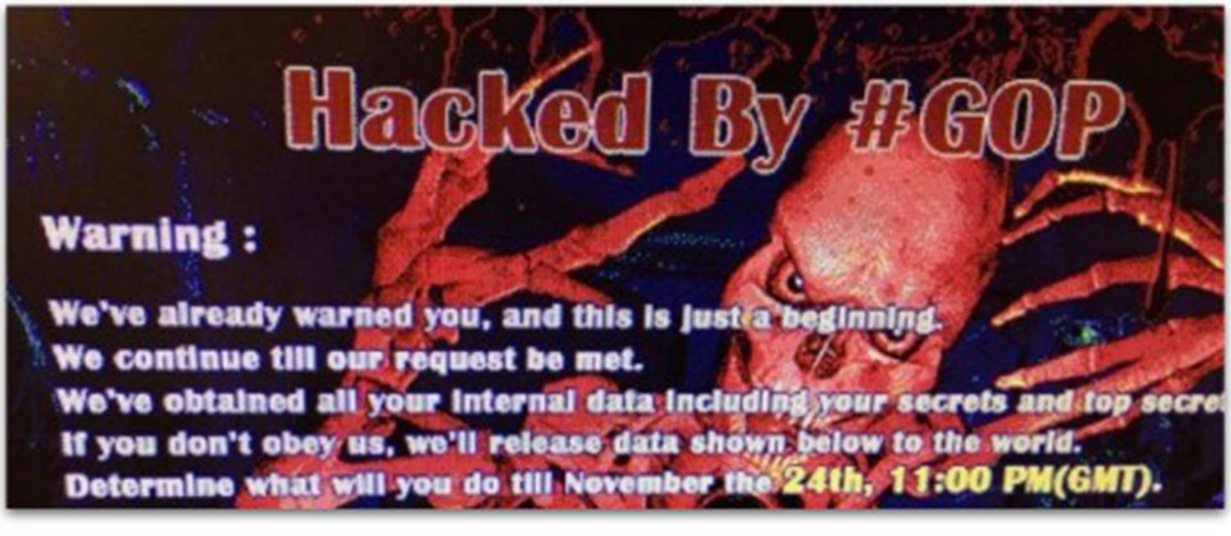
Sony Pictures Hack: When Nation-States Get Involved

(I) Introduction

Firstly, it's important to know that this attack was confirmed to have been performed by a North Korean hacking group called "Guardians of Peace." This result was directly claimed as a result of the FBI investigation that followed the attack. Secondly, shortly before the attack happened, Sony planned to release *The Interview*, a raunchy comedy in which actors Seth Rogen and James Franco are asked by the CIA to conduct a fake interview with North Korean leader Kim Jong Un. During this fake interview, the insurgents are directed to assassinate the leader by poisoning him. All of the evidence from the investigations that followed this attack point at *The Interview* being the cause of the attack. Many North Korean officials expressed disdain towards Sony for their movie and said they deserved to get hacked (RiskBasedSecurity). With that in mind, the following section will outline the events of the attack followed by how the attack was performed.

(II) The Attack

On November 24th, 2014, Sony employees logged into their computers to find a mysterious message:



Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data including your secrets and top secre
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).

Figure 1 - Message Received on Sony Computers on "Attack Day"

Simultaneously, a Reddit post was released — speculation claims the original poster of the content was a member of the Guardians of Peace — stating Sony had been hacked. The post also contained minor details of what was stolen, and the data leaks began.

Many third parties began reporting that Sony's entire network had been compromised, and panic ensued for Sony leadership, employees, and subsidiaries. Over the following two days, the GOP released private key information, the full overview of the extent of the breach, and several movies from Sony Pictures. Several of the torrent links released included big-name movies that Sony planned to release near Christmas. These were: *Annie*, *Mr. Turner*, and *To Write Love On Her Arms*. "According to several torrent tracking sites, these files have been downloaded over 100,000 times" (RiskBasedSecurity). These free downloads led to tens of millions in losses for Sony Pictures and the movie production studios involved with the films.

In the first round of major leaks, GOP released 24.87GB of compressed data files and even uploaded this data to MEGA and RapidGator through a compromised Sony server. In order to congest network traffic and stop people from downloading these files further, Sony reset their server configurations and reclaimed as many as possible to download the content back and throttle traffic on the download links. This nuisance caused so much of a traffic jam that many of the torrent service providers removed the links provided by GOP (RiskBasedSecurity). At this point, there was speculation that North Korea was involved in the attack because the malware used in the attack seemed very similar to the malware used in the Dark Seoul attack on South Korea. Because this attack now possibly involved another nation, the FBI began investigating; however, this investigation was not publicly announced until months later.

The first point of contact between Sony and the GOP after the initial message came on December 16th, 2014. At this point, Sony was still planning on releasing *The Interview*, even amidst light, vague threats from anonymous sources that it was a bad idea to go through with the release. As a response to this, the GOP sent Sony and movie theaters a terrifying message threatening violence at theaters that show the film: "The world will be full of fear. Remember the 11th of September 2001" (RiskBasedSecurity). This threat caused all of the theaters planning to release the film to cancel the premiers because they did not want to assume responsibility for any terror attacks. This was devastating news for Sony, and they decided to withhold the release of *The Interview* indefinitely.

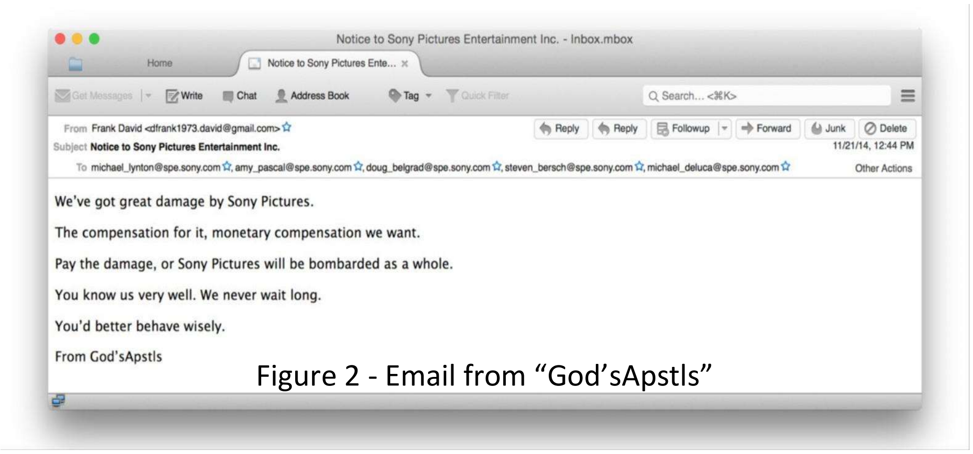
(III) The Aftermath

A few weeks after Sony pulled the release of *The Interview*, the FBI announced publicly that they had been investigating the attack and, more importantly, that they believed that North Korea was involved. This was not confirmed at this point, but the public opinion took over. Sony received *massive* amounts of backlash from the public for trying to appease the GOP. President Obama even spoke on the matter, saying Sony had not provided the White House with any information about the attack up to that point, and they had done the wrong thing by pulling the release because they were attempting to "negotiate with terrorists" (RiskBasedSecurity). This public statement really shed a poor light on Sony Pictures, and they received many threats from international and domestic sources for their actions.

In an attempt to mitigate the backlash, Sony decided to push the release of *The Interview* to Christmas again, less than a week away. Some local theaters decided to pick the movie back up in a form of protest against the North Koreans, but none of the major theaters took it back because of the short lead time and big risk associated with the release. In order to keep their sales up, Sony decided to release the movie digitally as well on YouTube and GooglePlay platforms, as well as their own Sony PlayStation Network. Within the first three days of release, *The Interview* earned over $40 million and became Sony Pictures' highest grossing film; the popularity of the movie would continue to grow through the next several months.

(IV) How the Attack Happened

Shortly before the day of the attack, Sony received an email from the hacking group known as "God'sApstls" (Franceschi-Bicchierai, Vice):



From Frank David <dfrank1973.david@gmail.com>
Subject Notice to Sony Pictures Entertainment Inc.
11/21/14, 12:44 PM
To michael_lynton@spe.sony.com, amy_pascal@spe.sony.com, doug_belgrad@spe.sony.com, steven_bersch@spe.sony.com, michael_deluca@spe.sony.com

We've got great damage by Sony Pictures.

The compensation for it, monetary compensation we want.

Pay the damage, or Sony Pictures will be bombarded as a whole.

You know us very well. We never wait long.

You'd better behave wisely.

From God'sApstls

Figure 2 - Email from "God'sApstls"

Sony ignored this email, but they would soon find out the depth of this threat. Through various email conversations between the members of GOP and several independent journalists, the following details were discovered about the Sony attack.

- People affiliated with the GOP infiltrated a Sony campus through lax physical security.
- The infiltrators planted the malware responsible for gaining monitoring capabilities, access to the Sony network, and ultimate control over Sony data by gaining physical access to Sony network devices.
- The GOP hackers had full control of Sony data for nearly a year before announcing their presence on “Attack Day.”
- The GOP’s motivation for attacking was the offensive nature of *The Interview*.

Beyond the simple fact that the GOP primarily gained access due to lax physical security, Sony also failed to follow good cyber security practices. Much of the sensitive information stored on Sony’s network was unencrypted, including *full* employee SSNs, network and employee passwords, credit card information, and personal details of employees and clients of Sony. Furthermore, Sony’s password policy was extremely lax, and led to many of the password-protected network restrictions being breached by GOP quite easily.

(V) Countermeasures

Sony didn’t have very good security practices when they were hit with this attack. If they had implemented changes beforehand, it might have prevented or slowed the GOP’s attack. They needed to better mediate their network, as well as log and monitor all server activity. Their passwords were another weakness, as the ones that were discovered were not nearly strong enough. Their database could’ve been designed better, and their server and network needed to be hardened. Better training their employees about security including tailgating and phishing attempts could have prevented them from getting the GOP from getting into the system in the first place.

After the attack, Sony updated their password policies, retrained employees to better corporate cyber hygiene, and hardened their network configurations. However, if we can guess anything from Sony’s hack history, these countermeasures likely aren’t enough to mitigate future attacks.

(VI) Confidentiality, Integrity, and Availability

Looking at how the attack compromised those affected, it mainly affected Sony’s data and the people who work there. Confidentiality was broken as worker profiles were leaked to the public over time. Integrity was lost when the GOP made their first move, deleting the information on worker’s computers. This also affected availability, as the computers were compromised, and the network had to be quarantined.

(VII) The Numbers and The Significance

The results of this breach are as follows:

- 47,000 unique, unencrypted stolen SSNs
- Over $200 million in total losses
    - Repairing network devices and Sony computers
    - Restoring lost data
    - Mitigating lost records
    - Providing personal protection for Sony leadership and Sony clients
- At least four days of Sony network downtime
    - Including PlayStation Network, Sony Entertainment, and third parties that rely on Sony network services

This Sony breach goes on to show the importance of encryption. If it was implemented, the attackers wouldn't have been able to compromise as many machines as they did because they used the data they were collecting to access other parts of the network. They also wouldn't have found out that some of the security certificates were just "password" (UMass Boston). It also shows how security in design is important because the system that was used didn't have complete mediation and as such the attackers were able to access the entire network by simply accessing a single weak section of it. Finally, physical security can't be underestimated. Network security can only mitigate so much, if someone walks in and gets access physically, they can still cause serious damage to computers and systems.

(VIII) Surprises with This Attack

The amount of data that Sony stored on their servers in plaintext was astounding. They stored employee details such as names, emails, passwords, and social security numbers (SSNs) in plaintext (RiskBasedSecurity). The fact that the SSN's were also full not just the ending 4 digits was also a big surprise because there was no need for this level of information being stored and unencrypted as it is such a valuable piece of information, above even passwords. The other surprise was just the sheer scale that Sony was able to get hacked. They are such a big company that it is hard to justify how lax their infrastructure security was, they definitely had the money to work on it, to have the tools available to them to prevent or mitigate such an attack as this. Lastly, Sony has been hacked before, not only that they have been hacked multiple times in the previous decade. Especially with the most recent incident with the PlayStation Network breach in 2011 Sony should have done more to update their security practices.

(IX) Conclusion

Overall, this attack is most astonishing because it displays just how sophisticated and coordinated cyber-attacks can be when they are sponsored by nation-states. In this example, it was very likely that GOP was funded and trained by North Korean government officials, and it is intimidating that even a country with as few public resources as North Korea has the technology available to pull off these large-scale attacks; possibly more intimidating is the fact that nation-states may not have the technical savvy to pull off attacks like this on their own, but the resources to utilize other nations that do.

Additionally, this example is a great case of a nation-state attacking a large company as a form of an attack on the American economy and public state. The GOP very successfully caused serious damage to Sony Pictures, and they instilled fear in the American public by threatening violence. Although the attack resolved with no violence, the attack itself was extremely successful, and we will likely see an increase in state-sponsored attacks on large companies because of the effectiveness of a coordinated attack.

Sources

https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

https://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12

http://blogs.umb.edu/itnews/2015/01/06/the-sony-hack/

https://www.vice.com/en_us/article/bmvn3m/sony-hack-cyberweapons-report

https://privacyrights.org/data-breaches/sony-pictures

http://nymag.com/intelligencer/2014/12/sonys-very-very-expensive-hack.html

https://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg

----