Sony Hack

By Evan Hack

What was the Sony hack?

It was November 2014, when the entertainment company, *Sony Pictures Entertainment*, was hacked by a hacker group. The group is said to be "...working in at least some capacity with North Korea…" and in the hack they "...stole huge amounts of information off of Sony's network.". The group also "...threatened to commit acts of terrorism against movie theaters, demanding that Sony cancel the planned release of *The Interview*, a comedy about two Americans who assassinate North Korean leader Kim Jong Un.".

VanDerWerff, E. (2015, January 20). *The 2014 sony hacks, explained*. Vox. Retrieved March 1, 2022, from https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea

What was the Sony hack?

Sony then proceeded to shelf the movie. In early December, President Obama stated that “Imagine if producers and distributors and others start engaging in self-censorship because they don't want to offend the sensibilities of somebody whose sensibilities probably need to be offended.”, he then said "That's not who we are.”(VanDerWerff). After this statement the movies was released again to select theaters and online sites.

VanDerWerff, E. (2015, January 20). *The 2014 sony hacks, explained*. Vox. Retrieved March 1, 2022, from https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea

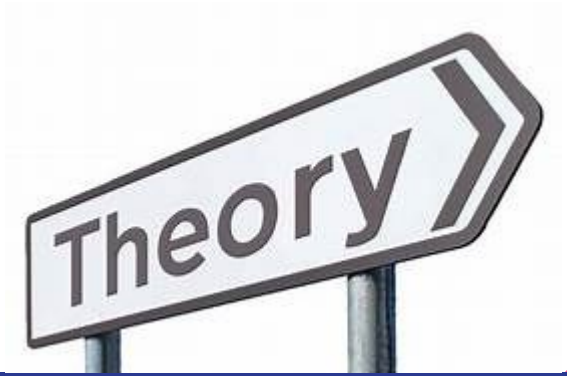
Who did it?

The hacker group responsible for the attack was called “Guardians of Peace” or “The Lazarus Group”. They are a “...a group of cyber-criminals that some security experts believe are native to, or at-least based out of, North Korea.”(Halliday), the group is said to have committed some of the largest cyber attacks in history. It is suggested that they “have been responsible for 2014’s Sony hack and they’re also believed to be connected to the theft of US$81 million from the Central Bank of Bangladesh in 2016.”.

Halliday, Fergus. (2018, March 18). *Who are the lazarus group?* PC World. Retrieved March 1, 2022, from https://www.pcworld.idg.com.au/article/635052/who-lazarus-group/

Who else could have done the hack?

It is widely theorized that the hack may have also been done by the U.S.. This is theorized because United States and North Korea were at each other's throats and through this attack the United States could make it look like an attack from North Korea; Therefore, giving the U.S. the ability to attack North Korea with an excuse as to why.



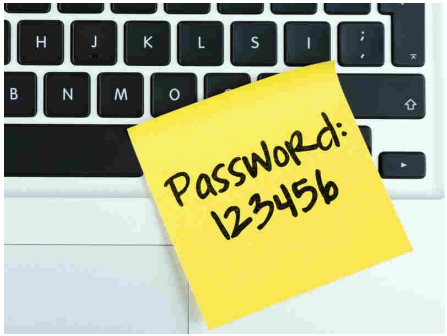
How did it happen?

It is reported that the group broke in through the Sony Entertainment network. The group hacked into one of the least protected Sony Entertainment servers and "...escalated the attack to gain access to the rest of the network."(Mazzarella). After more of an analysis of what made the attack possible, it was discovered that the network "...was not layered well enough to prevent breaches occurring in one part of their network to affect other parts of the network."(Mazzarella).

Mazzarella, J. (2015, January 6). *The sony hack; what happened, how did it happen….what did we learn?* UMass Boston IT News. Retrieved March 1, 2022, from https://blogs.umb.edu/itnews/2015/01/06/the-sony-hack/

How did it happen?

Another reason the group was able to infiltrate the company, is that they were able to decipher all of the passwords in the network, most of the passwords were “password”. Once logging in they would install malware into the network in order to damage the network.



Mazzarella, J. (2015, January 6). *The sony hack; what happened, how did it happen….what did we learn?* UMass Boston IT News. Retrieved March 1, 2022, from https://blogs.umb.edu/itnews/2015/01/06/the-sony-hack/

What was leaked?

On December first, the information leaked was a bunch of files and downloads for unreleased movies, they also leaked SSN of current and past employees of the company.

- 33,880 files were leaked
- 15,232 SSN were leaked from past and present employees.

RBS. (2014, December 5). *A breakdown and analysis of the december, 2014 sony hack*. Risk Based Security. Retrieved March 1, 2022, from https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

What was leaked?

The second wave of leaks was on December third, the items leaked included two files called “Bonus.rar” and “List.rar”. The “Bonus.rar” file contained server information, security certificates, passwords, and payment information. The “List.rar” file contained “...three files containing internal and external PC data, Linux servers, and Windows servers.”(RBS).

RBS. (2014, December 5). *A breakdown and analysis of the december, 2014 sony hack*. Risk Based Security. Retrieved March 1, 2022, from https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/

How could it have been prevented?

When it comes to security, a more multi-layered defense is needed in order help maintain a stronger security. This means that employees will need more practice with different security policies and strategies. For example "...using strong passwords and changing them per company policy, using technologies like firewall and VPN, performing periodic risk assessments to understand one's security posture – which controls are effective and which are failing."(Mazzarella).

Mazzarella, J. (2015, January 6). *The sony hack; what happened, how did it happen….what did we learn?* UMass Boston IT News. Retrieved March 1, 2022, from https://blogs.umb.edu/itnews/2015/01/06/the-sony-hack/

How else can it be prevented?

Doing penetration tests would be a great way at discovering potential breach points in the security, allowing the company to make their network more secure. Another practice that is useful is constant monitoring the network in order to catch threats before anything harmful is done.

Mazzarella, J. (2015, January 6). *The sony hack; what happened, how did it happen….what did we learn?* UMass Boston IT News. Retrieved March 1, 2022, from https://blogs.umb.edu/itnews/2015/01/06/the-sony-hack/

Sources

Halliday, Fergus. (2018, March 18). *Who are the lazarus group?* PC World. Retrieved March 1, 2022, from https://www.pcworld.idg.com.au/article/635052/who-lazarus-group/

Mazzarella, J. (2015, January 6). *The sony hack; what happened, how did it happen….what did we learn?* UMass Boston IT News. Retrieved March 1, 2022, from https://blogs.umb.edu/itnews/2015/01/06/the-sony-hack/
RBS. (2014, December 5). *A breakdown and analysis of the december, 2014 sony hack*. Risk Based Security. Retrieved March 1, 2022, from https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/
VanDerWerff, E. (2015, January 20). *The 2014 sony hacks, explained*. Vox. Retrieved March 1, 2022, from https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea