The Hack of Sony Pictures: What We Know and What You Need to Know

trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know

A week into Sony Pictures' devastating hack attack, a series of leaked internal documents and spreadsheets containing information and data of the company's employees and senior executives have been leaked to the public. Based on initial reports, Sony shut down their entire corporate network after a threatening message, along with a skull graphic, appeared on their computer screens. The message, sent by a hacker group who call themselves "Guardians of Peace" (#GOP), warned that it

was "only the beginning," and that they will continue until their "request be met". Shortly after the news broke out about the Sony hack, there were rampant claims of the involvement of North Korea who used a certain “wiper” malware.

[More: How did the hackers drop the "warning" wallpaper into Sony's office computers? Read *An Analysis of the “Destructive” Malware Behind FBI Warnings* from the Security Intelligence Blog]

Like most breach stories, we learn more about the nature of the hack as time passes, and though the ongoing investigation provided us with a few solid details, most of the headlines around the hack have focused more on who did it rather than what was obtained. Meanwhile, researchers have determined the destructive malware that launched the attack. From a security standpoint, it's critical to record all aspects of the incident and respond urgently and accordingly. In light of the attack, we’ve rounded up important dates and events to provide an overview of what happened, what was stolen, and who the people are behind the hack.

- **November 25** - First reports of the attack on Sony Pictures network hit social media
- **November 28** – Tech news site Re/code reports that North Korea is being investigated for the attack
- **November 29** - Copies of unreleased movies, believed to be rips of DVD screeners from Sony Pictures, appear on file sharing sites
- **December 1** - Documents released, revealing salaries of Sony Pictures executives
- **December 2** - Leaked documents reveal personal information of Sony employees and other internal Sony corporate documents (more pay details, name, birth dates, social security information) to the public. FBI also releases warning about destructive malware
- **December 3** – Re/code claims that North Korea would be "officially named" behind the attacks
- **December 5** – Threatening emails sent to Sony Pictures employees; FBI confirms that they're investigating
- **December 6** – North Korea releases a statement calling the attack "righteous", but denies involvement
- **December 8** – Investigations reveal that the hackers used the high-speed network of a hotel in Bangkok, Thailand to leak confidential employee data to the Internet on Dec 2.
- **December 16** – Hackers sends threats of additional attacks, with references to Sept 11, 2001, if the movie *The Interview* was released.
- **December 17** – US officials conclude that North Korea ordered the cyber attacks on Sony Pictures' computers. Theater chains announce they will not show the film, and Sony cancels the movie's release.
- **December 19** – FBI releases an official update on their investigation, concluding that the North Korean government was responsible for the attack.

The recent attack reminds IT administrators to learn from such incidents and think ahead in terms of securing their network infrastructure. Organizations should look into the developments of the Sony attack, and learn from it to be able to defend their own networks accordingly.

[More from the Security Intelligence Blog: A look into the malware variants that could be linked to the incident, including one that disables the antivirus application]

Individuals should also be vigilant; as investigative reports of controversial attacks continue to flood the news, bad guys could use this as a social engineering lure to trick users into clicking on suspicious links in spam mails and social media posts. As such, we advise users to be careful regarding the links they click and the stories they follow online, as cybercriminals are quick to play on people's curiosity especially when it comes to major news breakouts.

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cyber Attacks, Cybercrime, Hacking, Data Breach