Hackers may have exploited Sony's weakest link: humans

December 19 2014, by Glenn Chapman

Workers remove the poster for "The Interview" from a billboard in Hollywood, California, on December 18, 2014

Hackers who forced Sony Pictures to abort release of a comedy about North Korea likely slipped past the entertainment titan's defenses by exploiting a weak spot—humans.

That suspicion prevailed on Thursday among cyber security specialists piecing together clues about an attack that led Sony to cancel the release of "The Interview," a movie about a fictional CIA plot to kill North Korean dictator Kim Jong-Un.

The attack, branded by White House officials as "a serious national security matter," was seen as vindictive or even personal, with hackers out to cause Sony extreme pain instead of being driven by the typical profit motive.

Sony workers may have been targeted with "spearphishing" attacks that sent specific workers bogus email messages that appeared to come from trustable sources, according to Usher online identity platform senior vice president Guy Levy-Yurista.

Such deceptive missives typically include web links or attached files which, if opened, result in computers being secretly infected with malicious software.

"The weakest link in any security system is always the human being," Levy-Yurista told AFP.

"My guess is that North Korea made a decision to go after Sony; started a quick spearphishing campaign aimed at Sony Pictures or other parts of the company and then gained access to the system."

Once hackers get footholds, they take advantage of security holes to seize control and data.

The malicious code that infected Sony Pictures was identified as a customized version of Destover. A similar hacker tool has been used in cyber attacks on banks in South Korea and corporations in the Middle East, including Saudi Aramco.

The virus spreads quickly, sucks up data and then destroys computer hard drives to cover its tracks.

"It literally shreds the hard drives of all those machines so they are

useless," said Levy-Yurista.

"It is quite impressive what they have done. It is also quite horrific."

Out to hurt Sony

CloudFlare principle security researcher Marc Rogers, who is chief of security at the notorious annual Def Con hacker gathering in Las Vegas, is studying leaked Sony files for insights into the attack.

Rogers found that once past the perimeter of Sony's computer system, data was scantly protected with "egregious" flaws such as unencrypted files and passwords stored in plain text.

Hackers could have pillaged financial accounts or even tried extortion, he reasoned.

"It seems clear that whoever was behind this wasn't after money, they were out to hurt Sony," Rogers told AFP.

"It feels more like an insider job to me."

A disgruntled employee could have opened a path for hackers, and then lax security inside the system let them run amok in the network, according to Rogers.

In addition to receiving threats, Sony has seen the release of a trove of embarrassing emails, scripts and other internal communications, including information about salaries and employee health records.

The mountain of stolen data indicated attackers were inside Sony's network undetected for a while, or even had physical access to machines.

Whoever attacked Sony could have used off-the-shelf hacker tools, and appeared to be savvy in ways of distributing stolen data online.

Spearphishing is a standard tactic used for targeted cyber attacks, although it remained unclear whether the ruse was used on Sony Pictures, according to Symantec security response team director Kevin Haley.

"I can pick out a name, do some social engineering in the email, entice them to an attachment or link, and it goes to malware," Haley said.

Hackers are also known to use a watering hole attack in which a website popular in an industry is broken into and rigged with code that pounces when prey visits, according to Haley.

"The idea is that the lion doesn't have to search around the jungle looking for food; it just sits at the water hole and waits," Haley said.

Film climax leaked

Sony defended its decision to cancel the release as footage leaked onto the Internet showing the film's climax was to have been a graphic close-up of the North Korean leader's fiery death.

White House spokesman Josh Earnest declined to confirm reports that North Korea had attacked the movie giant, which pulled the film after hackers invoked 9/11 in threatening attacks on cinemas.

But, in a sign US intelligence believes that the attack came from an enemy of the United States, he said: "The president considers this to be a serious national security matter."

North Korea has denied involvement in the brazen November 24 cyber

attack.