Sexually Explicit Material Used as Lures in Recent Cyber Attacks

trendmicro.com/vinfo/us/security/news/cyber-attacks/sexually-explicit-material-used-as-lures-in-cyber-attacks

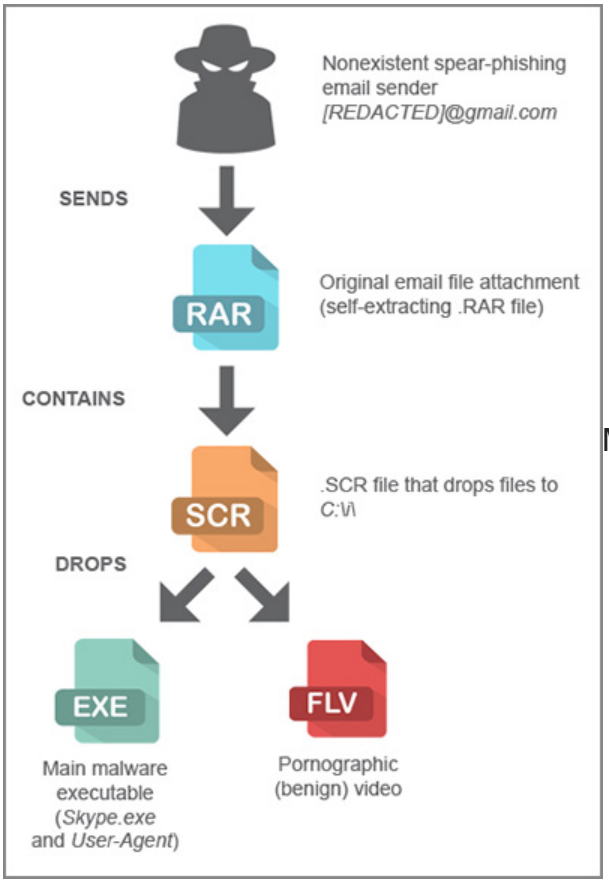
Sex sells. Cybercriminals know this and readily use it as lures, as we have seen in past spam runs that used fake YouTube links or promised photos of naked celebrities.

This month, actors of Operation Arid Viper and members of the Yanbian Gang jumped on the sexually explicit content bandwagon, using them in separate attacks that target respective victims in Israel and Kuwait, and South Korea.

Operation Arid Viper attacked five Israeli-based organizations in the government, transport, infrastructure, military, and academic industries, and one organization in Kuwait using spear-phishing emails that dropped a pornographic video on a victim's computer.

“It targeted professionals who might be receiving very inappropriate content at work and so would hesitate to report the incident,” declares Trend Micro threat researchers in a recent report of the Arid Viper discovery.

[Read: How Operation Arid Viper Used Sexually Explicit Content]



Meanwhile, fake versions of popular porn apps were among the many lures that the Yanbian Gang used to infect millions of Android™ mobile banking customers in South Korea.

Mobile banking customers unknowingly downloaded malware apps, which mobile threat researcher Simon Huang described to come "in the guise of popular porn apps with lewd icons and names and eye-catching descriptions like 'sexy women photos' and 'porn movies.' ”

"They hardly ever deliver on their promise though when run. All they do, in fact, is steal and upload victims’ mobile banking credentials to C&C servers," adds Huang.

When mobile users in South Korea download the apps—either through links sent via SMS or from infected mobile downloads—their mobile phone numbers, account names and number, and login credentials are automatically sent over to the Yanbian Gang members.

[Read: Fake Porn Apps Used in South Korean Banking App Scam]

Battling Malicious Clicks and Urges

Threat actors rely on an element of shame from professionals who received the pornographic video, care of Operation Arid Viper, to keep them from reporting the incident to their IT departments. This gives attackers a longer window to use the malware to get whatever information they can from the system. "These victims' failure to act on the threat could have then allowed the main malware to remain undiscovered. The attackers used a distinct and likely successful strategy previously unseen when it came to avoiding incident response team investigations," researchers stressed in the paper.

Most targeted attack strategies leave employees out of incident response solutions. However, given that the human component is a typical weak spot in a system's defenses, doing so is an oversight that can lead to data loss or theft.

We have previously noted that organizations need to complement security efforts with a proactive security awareness program. This program should train the workforce to practice safe habits and how to react to actual security incidents.

[Read:**How Employees Make or Break Enterprise Security]**

In addition, everyone should be reminded that sexually explicit content is a mainstay in a cybercriminal's bag of targeted attack tricks. It is not just organizations that are in danger of these schemes, as we have seen in the case of the South Korean mobile banking app scheme.

Consumers and enterprises alike should establish proactive measures against targeted attacks, which should also address malware and flaws in mobile devices.

[Read: Are You Guilty of Poor Mobile Security?]

[Read: Proven Protection Against Targeted Attacks and Advanced Threats]

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, Targeted Attacks