Nobody likes this reality show: A locked TV screen and ransomware demand

June 16 2016, by Nancy Owano

Credit: Trend Micro

(Tech Xplore)—A newer malware variant could affect smart TVs running on the Android operating system *Softpedia*'s Catalin Cimpanu reported earlier this week.

Security watchers are calling this FLocker (Frantic Locker). FLocker had been at work previously on mobile devices, but then versions started

encrypting data on smart TVs running on Android, said Cimpanu.

FLocker asks users for $200 in iTunes gift cards. Mobile Threat Response Engineer Echo Duan from Texas-based Trend Micro reported on June 13 (with additional analysis by Veo Zhang and Kenny Ye) that the lock-screen ransomware known as FLocker was capable of locking smart TVs.

Duan described the latest FLocker variant as "a police Trojan that pretends to be US Cyber Police or another law enforcement agency. It accuses potential victims of crimes they didn't commit. Then, it demands 200 USD worth of iTunes gift cards."

Trend Micro in April this year spotted a spike with over 1000 variants.

Duan offered some history on this: "Ever since FLocker (detected as ANDROIDOS_FLOCKER.A and short for 'Frantic Locker') first came out in May 2015, we have gathered over 7,000 variants in our sample bank. Its author kept rewriting the malware to avoid detection and improve its routine. Over the past few months, we have seen spikes and drops in the number of iterations released. The latest spike came in mid-April with over 1,200 variants."

According to *Softpedia*, the ransomware nightmare works according to these steps: (1) users download the malicious apps spread through these links. (2) the malware lies in hiding for 30 minutes. (3) After the 30 minute period, "Flocker starts pestering the user to give it admin rights. If the user declines, FLocker freezes the screen with a fake system update message to scare them into giving it the required access." (4) Once FLocker gains administrator privileges, it will talk with its C&C server, from where it downloads another APK and the ransom note.

Interestingly, the FLocker will deactivate itself if the device is located in

Kazakhstan, Azerbaijan, Bulgaria, Georgia, Hungary, Ukraine, Russia, Armenia or Belarus, according to Trend Micro.

Ransomware usually gets to users via spam SMS or malicious links" Duan said, reminding users to be wary if receiving messages or email from unknown sources.

Solutions? Trend Micro:

"We suggest user to contact the device vendor for solution first if their Android TV gets infected. Another way of removing the malware is possible if the user can enable ADB debugging. Users can connect their device with a PC and launch the ADB shell and execute the command "PM clear %pkg%". This kills the ransomware process and unlocks the screen. Users can then deactivate the device admin privilege granted to the application and uninstall the app."

More information: blog.trendmicro.com/trendlabs- … re-crosses-smart-tv/