Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City

ACG-CYBER SECURITY BULLETIN NR 172

ACG-CSB 090419172

Reference Number ACG-CSB 090419172

Understanding the Risk of Wirelurker Malware

The following information was obtained from different cyber security sources for notification to all parties concerned pursuant to the mandate of the Philippine National Police Anti-Cybercrime Group (PNP ACG) and classified as “Restricted” pursuant to the PNP Regulation 200-012 on Document Security and Impact Rating as high based on PNP Information Communication Technology (ICT) Security Manual s.2010-01 p. 22 and p.129.

SUMMARY

WireLurker is a family of malware targeting both macOS and iOS systems. The malware will infect a Mac device then laid dormant, waiting for an iOS device to be connected by USB. It will then download itself to the iOS device through the USB cable. The malware is capable of both generating malicious apps and infecting preexisting apps on the device. If a target app is installed, it copies the app from the mobile device to the desktop or laptop PC then infects the app and copies it back.

Once the WireLurker is installed it steal information from the device such as serial number, phone number, model number, product version, AppleID, product type, hardware serial number, installed applications, first and last name, contact information of received text messages. It can even regularly requests for updates from the attacker’s command and control server.

If the user connects its iOS device to the machine infected by WireLurker, the malware scans the mobile device and analyze the installed applications. If WireLurker finds a target app, it copies the app from the mobile device to the machine, infects its binary and then installs it again on the mobile unit.

As smartphones are now the device on which we do everything, from sending of personal emails to carrying out online banking, the amount of sensitive information stored on them is incredible.

More and more people are using their smartphones for work and the threat increases significantly. The fact that malware is actively looking for updates, it means that the attackers is capable of remotely adding new features to the malware once it is installed on a device.

This malware combines a number of techniques to successfully realize a new breed of threat to all iOS devices. WireLurker exhibits complex code structure, multiple component versions, file hiding, code obfuscation and customized encryption to thwart anti-reversing.

In this regard, the community are advised to keep antivirus/anti-spyware software up to date. This will go a long way in keeping malware away and preventing the systems from being compromised.

RECOMMENDATION

The public are advised to follow these tips in order to avoid the risks of WireLucker malware, to wit:

- Employ an anti-virus or security protection for the Mac OS X system and keep its signatures up to date;
- Do not download and run Mac applications or games from any third-party app store, download site or other untrusted sources;
- Do not pair your iOS device with untrusted or unknown computers or devices;
- Avoid powering your iOS device through chargers from untrusted or unknown sources;
- Do not accept random provisioning profiles that show up on your iDevice for no apparent reason;
- Remove any suspicious profiles from your iOS devices; and
- Do not jailbreak your iOS device.

For additional information, please refer to the following websites:

- https://www.cyber.nj.gov/threat-profiles/ios-malware-variants/wirelurker
- https://www.ibtimes.co.uk/what-wirelurker-malware-attacking-iphones-ipads-through-your-mac-1473633
- https://www.bankinfosecurity.com/malware-infects-apple-ios-devices-a-7531
- https://appleinsider.com/articles/14/11/10/wirelurker-masque-attack-malware-only-a-threat-for-users-who-disable-apples-ios-os-x-security

POINT OF CONTACT

Please contact PMAJ ANGELICA STARLIGHT L. RIVERA, Asst. Chief, ARMD thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 7230401 local 3562 for any inquiries related to this CYBER SECURITY BULLETIN.