CERT-PH Cybersecurity Threat Feeds

Issue Date	**April 13, 2021**
TLP: White	

Summary

The latest cyber threat topics gathered from the web and analyzed by the CERT-PH research team over the last 24 hours that may impact the Philippine government and cyberspace:

- **Joker Malware Infects Over 500,000 Huawei Android Devices** - **Android Malware Found Embedded In APKPure Store Application** - **Threat Actors Abuse Website Contact Forms To Deliver IcedID Malware** - **New Malware Discovered Snatching Users' Passwords**	● **CRITICAL** ● **URGENT** ● **INFORMATION**

Description

Joker Malware Infects Over 500,000 Huawei Android Devices

2021.04.10 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Cybersecurity experts discovered ten apps in Huawei's AppGallery that contained code for connecting to malicious command and control server to receive configurations and additional components. Dubbed as Joker, the malware could subscribe a user to a maximum of five services, although the threat actor could modify this limitation at any time. In addition, the malware communicates to its remote server to get the configuration file, which contains a list of tasks, websites for premium services, JavaScript that mimics user interaction.

Read more:

[https://www.bleepingcomputer[.]com/news/security/joker-malware-infects-over-500-000-huawei-android-devices/]
[https://securityaffairs[.]co/wordpress/116643/malware/huawei-store-joker-malware.html]

Android Malware Found Embedded In APKPure Store Application

2021.04.07 | Source(s): Bleeping Computer

Analysis:

Cybersecurity experts found malware embedded within the official application of APKPure, a popular third-party Android app store and an alternative to Google's official Play Store. According to the researchers, the malware detected looks like a variant of the Triada trojan capable of spamming users of infected devices with ads and delivering additional malware. In addition, the malware is capable of collecting information about the user device and sends it to their C&C server.

Read more:

[https://www.bleepingcomputer[.]com/news/security/android-malware-found-embedded-in-apkpure-store-application/]
[https://securityaffairs[.]co/wordpress/116635/cyber-crime/apkpure-client-malware.html]

Threat Actors Abuse Website Contact Forms To Deliver IcedID Malware

2021.04.10 | Source(s): Security Affairs

Analysis:

Security experts from Microsoft have uncovered a malware campaign abusing contact forms on legitimate websites to deliver the IcedID malware. Threat actors behind the operation are using contact forms published on websites to deliver malicious links to enterprises using emails with fake legal threats. The emails attempt to trick recipients into clicking a link to review supposed evidence behind their allegations, but instead, they start the IcedID malware infection. Dubbed as IcedID, the trojan has capabilities similar to other financial threats such as Gozi, Zeus and Dridex, capable of launching man-in-the-browser attacks and intercepting and stealing financial data from victims. According to researchers, attackers are abusing legitimate infrastructure, such as websites' contact forms, to bypass protections, making this threat highly evasive. In addition, attackers use legitimate URLs, in this case Google URLs that require targets to sign in with their Google credentials. The emails are being used to deliver the IcedID malware, which can be used for reconnaissance and data exfiltration, and can lead to additional malware payloads, including ransomware.

Read more:
[https://securityaffairs[.]co/wordpress/116620/cyber-crime/contact-forms-icedid-malware.html]

New Malware Discovered Snatching Users' Passwords

2021.04.09 | Source(s): The Hacker News

Analysis:

Cybersecurity experts spotted a malware downloader used in phishing attacks to deploy credential stealers and other malicious payloads. Dubbed as Saint Bot, the malware is a downloader that appeared recently caught dropping stealers and loaders and is designed to utilize it for distributing any kind of malware. The infection chain begins in phishing emails containing an embedded ZIP file ("bitcoin.zip") that claims to be a bitcoin wallet when, in fact, it's a PowerShell script under the guise of .LNK shortcut file. This PowerShell script then downloads the next stage malware, a WindowsUpdate.exe executable, which, in turn, drops a second executable (InstallUtil.exe) that takes care of downloading two more executables named def.exe and putty.exe. While the former is a batch script responsible for disabling Windows Defender, putty.exe contains the malicious payload that eventually connects to a command-and-control (C2) server for further exploitation.

Read more:
[https://thehackernews[.]com/2021/04/alert-theres-new-malware-out-there.html]

CERT-PH Recommendations:

- Users are advised to be cautious and always check the authenticity of the website before giving any private information or login credentials. Phishing attacks often use multiple redirects and unsecure connections before landing on the attacker's controlled website. If unsure of the website visited and causes to raise red flags, immediately put the website in your browser's list of locked webpages.
- Avoid installing unknown or unverified applications, especially from third-party distribution platforms.
- Scrutinize the application's permissions before installation and avoid allowing apps to view unnecessary information and other application's data.
- Android users are urged to check their devices and immediately uninstall and remove the following applications:
  - **Super Keyboard**
  - **Happy Colour**
  - **Fun Color**
  - **New 2021 Keyboard**
  - **Camera MX - Photo Video Camera**
  - **BeautyPlus Camera**
  - **Color RollingIcon**
  - **Funney Meme Emoji**
  - **Happy Tapping**
  - **All-in-One Messenger**
- Agencies must protect their assets and perimeter by minimizing the point of entry that an unwanted attacker might take. Thus, actions must be taken such as:
  - Closing misconfigured and/or unused ports that are accessible in the public internet.
  - Regularly monitoring and patching of systems, software application, and devices.
  - Educating employees regarding cyber hygiene and cybersecurity best practices.

Critical	*The information stated is deemed to be crucial to organizations and can significantly shift security concerns and issues based on following events.*
Urgent	*The information stated needs to be addressed timely, which may require immediate attention and/or prompt action.*
Information	*The information stated is good to know knowledge that provides awareness and understanding to the topic.*