CERT-PH Cybersecurity Threat Feeds

Issue Date	January 26, 2021
TLP: GREEN	

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:

- A New Wormable Android Malware Spreading Through WhatsApp
- DreamBus Botnet Targets Linux Systems
- Discord-Stealing Malware Invades npm Packages
- Windows-Native PDF Viewers Vulnerable to Multiple Attack Techniques

- CRITICAL
- URGENT
- INFORMATION

Description

A New Wormable Android Malware Spreading Through WhatsApp

2021.01.24 | Hacker News

Analysis:

A newly discovered Android malware has been discovered to propagate through WhatsApp messages to other contacts, which is speculated to be an adware campaign. Infected users will send a link to their contacts to a fake Huawei Mobile app, which redirects users to a website masquerading as Google Play Store. Once installed, the wormable app prompts victims to grant it notification access, which is then abused to carry out the wormable attack.

Read more:

[https://thehackernews[.]com/2021/01/beware-new-wormable-android-malware.html?&web_view=true]

DreamBus Botnet Targets Linux Systems

01.21.2021 | Source(s): ZDNet, Bank Info Security, Security Affairs

Analysis:

Security researchers have discovered a botnet malware that spread via the internet and cause a wormlike behavior once installed in a targeted system. The DreamBus botnet installs the XMRig crypto-miner on powerful enterprise-class Linux and Unix systems to use their computing power to mine Monero. The malware locates victims using different modules to search for weak passwords or remote code execution vulnerabilities in popular enterprise applications, including Secure Shell, in addition to IT administration tools, cloud-based applications, and databases. The botnet can exploit applications that include PostgreSQL, Redis, Hadoop YARN, Apache Spark, and HashiCorp Consul.

Read more:

[https://www.zdnet[.]com/article/dreambus-botnet-targets-enterprise-apps-running-on-linux-servers/]
[https://www.bankinfosecurity[.]com/dreambus-botnet-targets-linux-systems-a-15828]
[https://securityaffairs[.]co/wordpress/113832/malware/dreambus-botnet-linux-servers.html]

Discord-Stealing Malware Invades npm Packages

2021.01.22 | Source(s): Bleeping Computer, The Hacker News

Analysis:

Three malicious software packages, which contained the CursedGrabber malware. have been detected being published to npm, a code repository for JavaScript developers to share and reuse code blocks. According to security researchers, any applications corrupted by the code can steal tokens and other information from Discord users. Discord tokens are used inside bot code to send commands back and forth to the Discord API, which in turn controls bot actions. Once stolen, the Discord token would allow an attacker to hack the Discord's server, which are designed for creating communities on the web where users can voice calls, video calls, text messaging, media and files.

Read more:

[https://threatpost[.]com/discord-stealing-malware-npm-packages/163265/?web_view=true]

Windows-Native PDF Viewers Vulnerable to Multiple Attack Techniques

2021.01.21 | Source(s): The Daily Swig

Analysis:

Security researchers identified that the vast majority popular Windows-native PDF viewers were vulnerable to multiple attack techniques exploiting standard PDF features. Several PDF software brands were vulnerable to the most serious attacks, which resulted in local file leakage, file write access, and remote code execution. The researchers highlighted that the PDF-Xchange Viewer and PDF-Xchange Viewer for Windows were susceptible most of the attack techniques and suggested that applications built into browsers, which offer sandboxing protections, may be a better choice for a suspicious document than a native third-party PDF viewer.

Read more:

[https://portswigger[.]net/daily-swig/pwnable-document-format-windows-pdf-viewers-outperformed-by-browser-macos-linux-counterparts?&web_view=true]

CERT-PH Recommendations:

o Avoid installing unknown or unverified applications, especially from third-party distribution platforms and scrutinize the application's permissions before installation.

o 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.