CERT-PH Cybersecurity Threat Feeds

Issue Date	April 12, 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:

- Google Patches Critical Code Execution Vulnerability in Android
- REvil Ransomware Now Changes Password To Auto-Login In Safe Mode
- Attackers Blowing Up Discord, Slack with Malware
- Phishing Campaign Evades Detection with HTML Lego Pieces

- CRITICAL
- URGENT
- INFORMATION

Description

Google Patches Critical Code Execution Vulnerability in Android

2021.04.07 | Source(s): Security Week

Analysis:

Google has released its April 2021 monthly security update in Android addressing more than 30 vulnerabilities, including a remote code execution flaw in the System component. Tracked as CVE-2021-0430, it affects Android 10 and 11 that could enable a remote attacker using a specially crafted file to execute arbitrary code within the context of a privileged process. The flaw was addressed during the first part of the security patch along with 12 other high-severity vulnerabilities. The second batch of the patch includes fixes for 18 vulnerabilities. Five other vulnerabilities were addressed in the System component: three elevation of privilege and two information disclosure issues.

Read more:

[https://www.securityweek[.]com/google-patches-critical-code-execution-vulnerability-android]

Attackers Blowing Up Discord, Slack with Malware

2021.04.07 | Source(s): Bleeping Computer

Analysis:

Cybersecurity researchers have observe a recent change to the REvil ransomware, which allows the threat actors to automate file encryption via Safe Mode after changing Windows passwords. It was reported that the new encryption method was added to the REvil/Sodonokibi ransomware was added as a way to evade detection by security software and to shut down backup software, database servers, or mail servers to have greater success when encrypting files. The malware will encrpyt the data on the systems via the '-smode' command-line argument, which would reboot the device into Safe Mode, where it would perform the encryption of files.

Read more:

[https://www.bleepingcomputer[.]com/news/security/revil-ransomware-now-changes-password-to-auto-login-in-safe-mode/]

Attackers Blowing Up Discord, Slack with Malware

2021.04.07 | Source(s): Threatpost

Analysis:

Workflow and collaboration tools like Slack and Discord have been infiltrated by threat actors, who are abusing their legitimate functions to evade security and deliver info-stealers, remote-access trojans (RATs) and other malware. Security researchers have reported that threat actors abuse collaboration applications, such as Discord and Slack, to trick users into opening opening malicious attachments, that will then deploy various RATs and stealers into their systems. Once infected, threat actors can then extract information from the user, install other malicious application into the system, or spread the malicious file to other user. Threat actors abuses the functionality where files can be uploaded to Slack, and users can create external links that allow the files to be accessed, regardless of whether the recipient even has Slack installed. They can deliver their malicious payload to the CDN over encrypted HTTPS, and that the files will be compressed, further disguising the content.

Read more:
[https://threatpost[.]com/attackers-discord-slack-malware/165295/]

Phishing Campaign Evades Detection with HTML Lego Pieces

2021.04.08 | Source(s): Bleeping Computer

Analysis:

A recent phishing campaign was observed to deliver fraudulent web pages by building it from chunks of HTML code stored locally and remotely. Security researchers detected the phishing campaign that collects Microsoft Office 365 credentials that uses a clever trick to deliver fraudulent web pages via multiple HTML pieces hidden within JavaScript files to build the fake login interface that prompts the potential victim to type in sensitive information. Initially, an attachment was attached to the victims' emails claiming to be an Excel spreadsheet on an investment, which contins URL encoded text to links to two JavaScript files used for other phishing campaigns. Both JavaScript files had two blocks of base64 encoded text hiding HTML code and URL that is used to validates the victim's email and password, act as the 'submit' function and code that displayed a popup alerting the victim that they had been logged out and needed to log in again.

Read more:
[https://www.bleepingcomputer[.]com/news/security/microsoft-office-365-phishing-evades-detection-with-html-lego-pieces/]

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.
- Discord, Slacks, and other users of collaborative platforms are advised to be cautious in clicking links and downloading applications while using the said applications. Thoroughly check the authenticity of the webpage being redirected before giving any information.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Android Devices** – April monthly update
- 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.*