CERT-PH Cybersecurity Threat Feeds

Issue Date	January 14, 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:

- Rogue Android RAT Emerges from The Dark Web
- Critical WordPress-Plugin Bug Found In 'Orbit Fox' Allows Site Takeover
- Microsoft Fixes Secure Boot Bug Allowing Windows Rootkit Installation
- Adobe Fixes 7 Critical Flaws with The Release Of First Security Update Of 2021

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

Rogue Android RAT Emerges from The Dark Web

2021.01.13 | Source(s): Security Affairs

Analysis:

Cybersecurity experts discovered an Android Remote Access Trojan (RAT) that can allow attackers to take over infected devices and steal user data. Dubbed as Rogue, is a new mobile RAT discovered by researchers while investigating the activity of the darknet threat actors known as Triangulum and HeXaGoN Dev. Rogue allows its operator to exfiltrate any kind of data from the infected device, delete data and download additional malicious payloads. After gaining all of the required permissions on the targeted device, the Rogue RAT will hide its icon from the device and leverages Google's Firebase platform to hide its activity.

Read more:

[https://securityaffairs[.]co/wordpress/113369/malware/rogue-android-rat-darkweb.html]

Critical WordPress-Plugin Bug Found In 'Orbit Fox' Allows Site Takeover

2021.01.13 | Source(s): Threatpost

Analysis:

Cybersecurity experts discovered two security vulnerabilities that exist in a WordPress plugin, called Orbit Fox, that could allow attackers to inject malicious code into vulnerable websites and/or take control of a website. The first flaw is an authenticated privilege-escalation flaw that carries a CVSS bug-severity score of 9.9, making it critical. Authenticated attackers with contributor level access or above can elevate themselves to administrator status and potentially take over a WordPress site. While the second bug is an authenticated stored cross-site scripting (XSS) issue that allows attackers with contributor or author level access to inject JavaScript into posts. This injection could be used to redirect visitors to malvertising sites or create new administrative users, among other actions. It's rated 6.4 on the CVSS scale, making it medium severity.

Read more:

[https://threatpost[.]com/orbit-fox-wordpress-plugin-bugs/163020/]

Microsoft Fixes Secure Boot Bug Allowing Windows Rootkit Installation

2021.01.13 | Source(s): Bleeping Computer

Analysis:

Microsoft has fixed a security feature bypass vulnerability in Secure Boot, tracked as CVE-2020-0689, that allows attackers to compromise the operating system's booting process even when

Secure Boot is enabled. Secure Boot blocks untrusted operating systems bootloaders on computers with Unified Extensible Firmware Interface (UEFI) firmware and a Trusted Platform Module (TPM) chip to help prevent rootkits from loading during the OS startup process. Affected Windows versions include multiple Windows 10 releases (from v1607 to v1909), Windows 8.1, Windows Server 2012 R2, and Windows Server 2012.

Read more:
[https://www.bleepingcomputer[.]com/news/security/microsoft-fixes-secure-boot-bug-allowing-windows-rootkit-installation/]

Adobe Fixes 7 Critical Flaws with The Release of First Security Update Of 2021

2021.01.12 | Source(s): Threatpost, ZDNet

Analysis:

Adobe Systems has patched seven critical vulnerabilities, which impact Windows, macOS and Linux users. The impact of the serious flaws range from arbitrary code execution to sensitive information disclosure. One of the most severe critical flaws, tracked as CVE-2021-21009, is a web-based flaw that exists in Adobe Campaign Classic that enables attackers to induce the server-side application to make HTTP requests to an arbitrary domain. Other critical flaws that exist in several Adobe products such as Photoshop, Illustrator, Bridge, Animate, InCopy and Captivate.

Read more:
[https://threatpost[.]com/adobe-critical-flaws-flash-player/162958/]
[https://www.zdnet[.]com/article/adobe-patches-code-execution-vulnerabilities-in-the-first-security-update-of-2021/]

CERT-PH Recommendations:

o Update any vulnerable system/applications/devices to their latest and patched versions:
  - Microsoft's January 2021 Patch
  - Adobe's January 2021 Patch

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.