CERT-PH Cybersecurity Threat Feeds

Issue Date	March 09, 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:

- Supermicro, Pulse Secure Release Fixes For 'trickboot' Attacks
- New Ransomware Only Decrypts Victims Who Join Their Discord Server
- WordPress Injection Anchors Widespread Malware Campaign
- Updated MSERT To Detect Web Shells Used in Attacks Against Microsoft Exchange

- CRITICAL
- URGENT
- INFORMATION

Description

Supermicro, Pulse Secure Release Fixes For 'trickboot' Attacks

2021.03.04 | Source(s): Bleeping Computer

Analysis:

Supermicro and Pulse Secure have released advisories warning that some of their X10 UP motherboards are vulnerable to the TrickBot malware's UEFI firmware-infecting module. Tracked as TrickBoot, the new malicious firmware-targeting module is capable of analyzing a device's UEFI firmware to determine if it has 'write protection' disabled. If so, the malware contains the functionality to read, write and erase the firmware. This could allow the malware to perform various malicious activities, such as bricking a device, bypassing operating system security controls, or reinfecting a system even after a full reinstall.

Read more:

[https://www.bleepingcomputer.com/news/security/supermicro-pulse-secure-release-fixes-for-trickboot-attacks]

New Ransomware Only Decrypts Victims Who Join Their Discord Server

2021.03.05 | Source(s): Bleeping Computer

Analysis:

Cybersecurity experts discovered a new ransomware that encrypts users' devices and only decrypts them if they join the developer's Discord server. Tracked as Hog, this ransomware, when executed, will check if a particular Discord server exists, and if it does, begins to encrypt the victims' files. When encrypting, the malware will append the .hog extension and automatically extract the decryptor component. After the encryption process, it will launch the DECRYPT-MY-FILES.exe decryptor program from the Windows Startup folder. This decryptor will explain what happened to the victims and then prompt them to enter their Discord user token. A Discord token allows the ransomware to authenticate to Discord's APIs as the user and check if they joined their server.

Read more:

[https://threatpost[.]com/wordpress-injection-malware-campaign/164555/]

WordPress Injection Anchors Widespread Malware Campaign

2021.03.05 | Source(s): Threatpost

Analysis:

Tracked as Gootloader, the downloader malware is poisoning websites globally as part of an extensive drive-by and watering-hole cybercampign that abuses Wordpress sites by injecting them with hundreds of pages with fake content. According to cybersecurity experts, the modus operandi is to entice a business professional to one of the compromised websites, and then have them click on a link, leading to Gootloader, which attempts to retrieve the final payload, whether it be ransomware, a banking trojan or intrusion tool/credential stealer. Moreover, the Gootloader was able to deliver Cobalt Strike Intrusion Tool, the Godotkit banking trojan or the REvil ransomware.

Read more:

[https://threatpost[.]com/wordpress-injection-malware-campaign/164555/]

Updated MSERT To Detect Web Shells Used in Attacks Against Microsoft Exchange

2021.03.08 | Source(s): Security Affairs, Bleeping Computer

Analysis:

Microsoft updated its Microsoft Safety Scanner (MSERT) tool to detect web shells employed in the recent Exchange Server attacks. The MSERT tool is a self-contained executable file that scans a computer for malware and reports its findings, it is also able to remove detected malware. Administrators could use MSERT to make a full scan of the install or they can perform a 'Customized scan' where malicious files from the threat actor have been observed. According to Microsoft, this remediation step is effective against known attack patterns but is not guaranteed as complete mitigation for all possible exploitation of these vulnerabilities.

Read more:

[https://securityaffairs[.]co/wordpress/115388/hacking/microsoft-msert-microsoft-exchange-attacks.html]
[https://www.bleepingcomputer[.]com/news/security/microsofts-msert-tool-now-finds-web-shells-from-exchange-server-attacks/]

CERT-PH Recommendations:

- Discord administrators are advised to monitor Discord traffic for threats and other abnormal behavior.
- Users are advised to be cautious and check the email thoroughly before downloading and opening email attachments, especially when received from unknown email senders, as ransomware are usually found on email attachments and pirated application software.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Supermicro X10 UP-series motherboards** - BIOS version 3.4
- 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.*