CERT-PH Cybersecurity Threat Feeds

Issue Date	April 16, 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:

- Attackers Target ProxyLogon Exploit to Install Cryptojacker
- Gafgyt Botnet Lifts DDoS Tricks from Mirai
- Experts Discovered 1-Click Hack in Popular Desktop Apps
- Celsius Email System Breach Leads To Phishing Attack On Customers

- CRITICAL
- URGENT
- INFORMATION

Description

Attackers Target ProxyLogon Exploit to Install Cryptojacker

2021.04.14 | Source(s): Threatpost

Analysis:

Threat actors are observed to be targeting Exchange servers using the highly publicized exploit chain to host malicious Monero cryptominer in attacks. According to researchers, the attacks began with a PowerShell command to retrieve a batch script pretending to be a zip file named win_r.zip from another compromised server's Outlook Web Access logon path (/owa/auth). The batch script runs another command that outputs the decoded executable into the same directory. Once decoded, the batch script runs the executable, which extracts the miner and configuration data from the QuickCPU.dat file, injects it into a system process, and then deletes any evidence that it was there. The executable in the attack appears to contain a modified version of a tool in Github, dubbed as PEx64-Injector, capable of migrating any x64 exe to any x64 process with no administrator privileges required.

Read more:

[https://threatpost[.]com/attackers-target-proxylogon-cryptojacker/165418/]

Gafgyt Botnet Lifts DDoS Tricks from Mirai

2021.04.15 | Source(s): Bleeping Computer

Analysis:

Cybersecurity experts discovered variants of a Linux-based botnet malware family that incorporates code from the infamous Mirai botnet. Dubbed as Gafgyt, the botnet targets vulnerable internet of things (IoT) devices to launch large-scale distributed denial-of-service (DDoS) attacks. According to researchers, the new Mirai-variants are capable of HTTP flooding, UDP flooding, TCP flood attacks and STD module. Threat actors are believed to be exploiting several vulnerabilities in Huawei, Realtek and Dasan GPON routers, tracked as CVE-2017-17215, CVE-2014-8361 and CVE-2018-10561 respectively.

Read more:

[https://threatpost[.]com/gafgyt-botnet-ddos-mirai/165424/]

Experts Discovered 1-Click Hack in Popular Desktop Apps

2021.04.15 | Source(s): The Hacker News

Analysis:

Cybersecurity experts discovered multiple one-click vulnerabilities have been discovered across a variety of popular software applications, allowing an attacker to potentially execute arbitrary code on target systems. According to researchers, the flaws stem from an insufficient validation of URL input that, when opened with the help of the underlying operating system, leads to inadvertent execution of a malicious file. In addition, analysis found that many apps failed to validate the URLs, thereby allowing an adversary to craft a specially crafted link pointing to a piece of attack code, resulting in remote code execution.

Read more:

[https://thehackernews[.]com/2021/04/1-click-hack-found-in-popular-desktop.html]

Celsius Email System Breach Leads To Phishing Attack On Customers

2021.04.13 | Source(s): Bleeping Computer

Analysis:

Cryptocurrency rewards platform Celsius Network has disclosed a security breach exposing customer information that led to a phishing attack. According to the authorities, an unauthorized party managed to gain access to a back-up third-party email distribution system which had connections to a partial customer email list. Once inside the system, this unauthorized party sent a fraudulent email announcement, of which we know some of the recipients to be Celsius customers. After gaining access to the customer list, the threat actors impersonated Celsius Networks in phishing texts and emails that promoted a new Celsius Web Wallet. As an incentive to get people to visit the site, the text states Celsius is offering $500 in the CEL cryptocurrency if they create a wallet and enter a special promo code. Clicking on the link led recipients to the phishing site celsiuswallet[.]network that asked visitors to create a Celsius Web Wallet. When potential victims attempted to create this fake wallet, the site asked visitors to link their other online wallets and input those wallet's seed phrases. Once this seed phrase is provided, the threat actors can import the victim's wallet and steal any cryptocurrency within it.

Read more:

[https://www.bleepingcomputer[.]com/news/security/celsius-email-system-breach-leads-to-phishing-attack-on-customers/]

CERT-PH Recommendations:

- Users should regularly monitor for suspicious processes, events and network traffic spawned on the execution of any untrusted binary.
- 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.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Microsoft Exchange Server - April 2021 Security Update**
  - **Huawei Routers** - latest firmware
  - **Realtek and ASUS Routers** - latest firmware
  - **Nextcloud** - version 3.1.3
  - **Telegram** - latest version
  - **VLC Player** - version 3.0.13
  - **OpenOffice** - latest version
  - **LibreOffice** - latest version
  - **Mumble** - version 1.3.4
  - **Dogecoin** - version 1.14.3
  - **Bitcoin ABC** - version 0.22.15
  - **Bitcoin Cash** - version 23.0.0
  - **Wireshark** - version 3.4.4
  - **WinSCP** - version 5.17.10
- 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.*