CERT-PH Cybersecurity Threat Feeds

Issue Date	April 21, 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:

- Fake Microsoft Store and Spotify Sites Spread Info-stealing Malwares
- Pulse Secure VPN Zero-day Used to Hack Defense Firms and Government Organizations
- Microsoft Partially Fixes Windows 7 and Server 2008 Vulnerability
- WeChat Users Targeted Using Recently Disclosed Chromium Exploit

- CRITICAL
- URGENT
- INFORMATION

Description

Fake Microsoft Store and Spotify Sites Spread Info-stealing Malware

2021.04.20 | Source(s): Bleeping Computer

Analysis:

Threat actors are actively promoting malicious sites that impersonate Microsoft Store, Spotify and an online document converter that distribute malware to steal credit cards and passwords saved in web browsers. According to researchers, the attack is conducted through malicious advertising that appears to be legitimate applications. When users click on the ad, they are redirected to a fake Microsoft Store page for a fake application which is automatically downloaded. The downloaded zip file contains an information-stealing malware in disguise. Dubbed as Ficker, the malware is an information-stealing Trojan used by threat actors to steal saved credentials in web browsers, desktop messaging clients and FTP clients. Moreover, the malware can steal over fifteen cryptocurrency wallets, steal documents and take screenshots of the active applications running on victims' computers. The stolen data will then be compiled into a zip file and transmitted back to the attacker to be used on other malicious activities.

Read more:

[https://www.bleepingcomputer[.]com/news/security/fake-microsoft-store-spotify-sites-spread-info-stealing-malware/]

Pulse Secure VPN Zero-day used to Hack Defense Firms and Government Organizations

2021.04.20 | Source(s): Bleeping Computer

Analysis:

Pulse Secure shared mitigation measures for a zero-day authentication bypass vulnerability in the Pulse Connect Secure (PCS) SSL VPN appliance actively exploited in attacks against worldwide organizations and focused on US Defense Industrial base (DIB) networks. Tracked as CVE-2021-22893, the flaw is an authentication by-pass vulnerability, residing in the Pulse Connect Secure (PCS), that can allow an unauthenticated user to perform remote arbitrary file execution on the Pulse Connect Secure gateway. According to security experts, at least two threat actors, tracked as UNC2630 and UNC2717, are actively deploying 12 malware strains in these attacks. In addition, these threat actors are highly skilled to develop a malware that enables them to harvest Active Directory credentials and bypass multifactor authentication on Pulse Secure devices to access victim networks for several months without being detected.

Read more:

[https://www.bleepingcomputer[.]com/news/security/pulse-secure-vpn-zero-day-used-to-hack-defense-firms-govt-orgs/]

Microsoft Partially Fixes Windows 7 and Server 2008 Vulnerability

2021.04.20 | Source(s): Bleeping Computer

Analysis:
Microsoft issued a partial fix for a local privilege escalation (LPE) vulnerability impacting all Windows 7 and Server 2008 R2 devices. The flaw stems from the misconfiguration of two service registry keys and it allows local attackers to escalate privileges on any fully patched systems. Experts discovered that insecure permissions on the registry keys of the RpcEptMapper and DnsCache services enable attackers to trick the RPC Endpoint Mapper service to load malicious DLLs on Windows 7 and Windows Server 2008 R2. Successful exploitation of the vulnerability allows attackers to execute arbitrary code in the context of the Windows Management Instrumentation (WMI) service that runs with LOCAL SYSTEM permissions. Microsoft is yet to release security updates for ESU customers to address the issue fully.
Read more:
[https://www.bleepingcomputer[.]com/news/security/microsoft-partially-fixes-windows-7-server-2008-vulnerability/]

WeChat Users Targeted Using Recently Disclosed Chromium Exploit

2021.04.20 | Source(s): Security Affairs
Analysis:
Threat actors are observed to have weaponized the recently disclosed Chrome exploit to target WeChat users in China. According to researchers, the attacks only targeted users of the WeChat Windows app. Attackers are sharing specially crafted links with WeChat users, upon clicking them, a JavaScript code will execute a shellcode on their underlying operating systems. The remote code execution vulnerabilities disclosed recently could not escape Chromium's sandbox, which means that attackers must have chained them with a sandbox escape exploit to execute arbitrary code on the underlying system.
Read more:
[https://securityaffairs[.]co/wordpress/117017/hacking/wechat-chromium-bug-attack.html]

CERT-PH Recommendations:

- Pulse Secure users are advised to disable Windows File Share Browser and Pulse Secure Collaboration features and imports the Workaround-2104[.]xml file that can be found on the Pulse Secure Security Advisory. Users can also check whether they are impacted by the flaw via the Pulse Connect Secure Integrity Tool.
- 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:
  - **Pulse Secure (with gateways running PCS9.0R3 and higher)** - version 9.1R.11.4
  - **Microsoft April** - 2021 Windows Updates (ESU)
  - **Google Chrome** - latest version
  - **Microsoft Edge** - latest version
- 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.*