CERT-PH Cybersecurity Threat Feeds

Issue Date	February 23, 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:

- Silver Sparrow, A New Malware Infects Mac Systems Using Apple M1 Chip
- Security Researchers Uncovered a New Malware Builder, APOMacroSploit
- Python Updates to Tackle Remote Code Vulnerability
- Powerhouse VPN Products Can Be Abused for Large-scale DDos Attacks

- CRITICAL
- URGENT
- INFORMATION

Description

Silver Sparrow, A New Malware Infects Mac Systems Using Apple M1 Chip

2021.02.20 | Source(s): Security Affairs, Threatpost, ZDNet

Analysis:

Malware researchers discovered a new malware that is infecting Mac systems using the latest Apple M1 chip across the world. Dubbed as Silver Sparrow, the malware had already infected 29,139 macOS endpoints across 153 countries. It was discovered that Silver Sparrow is macOS adware that was recompiled to infect systems running the Apple M1 Chip. The adware writes each of its components out line by line with JavaScript commands which allows the attackers to quickly modify the code and avoid simple static antivirus signatures by dynamically generating the script rather than using a static script file.

Read more:

[https://securityaffairs[.]co/wordpress/114805/malware/silver-sparrow-malware-apple-m1-chip.html]
[https://threatpost[.]com/silver-sparrow-malware-30k-macs/164121/]
[https://www.zdnet[.]com/article/30000-macs-infected-with-new-silver-sparrow-malware/]

Security Researchers Uncovered a New Malware Builder, APOMacroSploit

2021.02.22 | Source(s): Security Affairs

Analysis:

Malware researchers discovered a new malware that is infecting Mac systems using the latest Apple M1 chip across the world. Dubbed as Silver Sparrow, the malware had already infected 29,139 macOS endpoints across 153 countries. It was discovered that Silver Sparrow is macOS adware that was recompiled to infect systems running the Apple M1 Chip. The adware writes each of its components out line by line with JavaScript commands which allows the attackers to quickly modify the code and avoid simple static antivirus signatures by dynamically generating the script rather than using a static script file.

Read more:

[https://securityaffairs[.]co/wordpress/114880/cyber-crime/apomacrosploit-macro-builder.html]

Python Updates to Tackle Remote Code Vulnerability

2021.02.22 | Source(s): ZDNet

Analysis:

The Python Software Foundation (PSF) has rushed out Python 3.9.2 and 3.8.8 to address two notable security flaws, including a remote code execution vulnerability tracked as CVE-2021-3177. According to researchers, the flaw affects Python applications that accept floating-point numbers as untrusted input, as demonstrated by a 1e300 argument to 'c_double.from_param'. The bug occurs because "sprintf" is used unsafely. The impact is broad because Python is pre-installed with multiple Linux distributions and Windows 10. The other flaw is tracked as CVE-2021-23336 concerns a web cache poisoning vulnerability by defaulting the query "args" separator to '&', and allowing users to choose a custom separator.

Read more:

[https://www.zdnet[.]com/article/python-programming-language-hurries-out-update-to-tackle-remote-code-vulnerability]

Powerhouse VPN Products Can Be Abused for Large-scale DDos Attacks

2021.02.22 | Source(s): ZDNet

Analysis:

Botnet operators are abusing VPN servers from VPN provider Powerhouse Management as a way to bounce and amplify junk traffic as part of DDoS attacks. According to researchers, the root cause of this new DDoS vector is a yet-to-be-identified service that runs on UDP port 20811 on Powerhouse VPN servers. Moreover, an attacker can send a single-byte UDP packet to a Powerhouse VPN server, which then amplifies it and sends it to the IP address of a victim of a DDoS attack

Read more:

[https://www.zdnet[.]com/article/powerhouse-vpn-products-can-be-abused-for-large-scale-ddos-attacks/]

CERT-PH Recommendations:

o 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.

o Avoid installing unknown or unverified applications, especially from third-party distribution platforms. Scrutinize the application's permissions before installation and avoid allowing apps to view unnecessary information and other application's data.

o Powerhouse VPN users are advised to block any traffic that comes from the VPN provider's networks with AS number, AS21926 and AS22363. In addition to blocking any traffic where the source port is 20811.

o Update any vulnerable system/applications/devices to their latest and patched versions:

- Python - versions 3.9.2 and 3.8.8

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.

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.*