CERT-PH Cybersecurity Threat Feeds

Issue Date	April 06, 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:

- Apple Mail Zero-Click Security Vulnerability Allows Email Snooping
- State Hackers Attacking Fortinet FortiOS Servers
- Attackers Are Abusing Github Infrastructure To Mine Cryptocurrency
- Spy Operations Target Vietnam with Sophisticated RAT

- CRITICAL
- URGENT
- INFORMATION

Description

Apple Mail Zero-Click Security Vulnerability Allows Email Snooping

2021.04.05 | Source(s): Threatpost

Analysis:

Cybersecurity experts discovered a zero-click security vulnerability in Apple's macOS mail that could allow attackers to add or modify any arbitrary file inside Mail's sandbox environment, leading to a range of attack types. Tracked as CVE-2020-9922, the vulnerability is rated 6.5 on the CVSS vulnerability-severity scale and successful exploitation could lead to unauthorized disclosure of sensitive information to a third party, ability to modify a victim's Mail configuration, takeover of victim's other accounts via password resets and the ability to change the victim's configuration so that the attack can propagate to correspondents in a worm-like fashion.

Read more:

[https://threatpost[.]com/apple-mail-zero-click-security-vulnerability/165238/]

State Hackers Attacking Fortinet FortiOS Servers

2021.04.02 | Source(s): Bleeping Computer

Analysis:

Cybersecurity experts discovered three security vulnerabilities in the FortiOS used in Fortinet SSL VPN are currently being observed to be exploited by advanced persistent threat (APT) actors. Tracked as CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591, these vulnerabilities can be exploited by threat actors to gain a foothold within vulnerable networks before moving laterally and carrying out reconnaissance activity. In addition, successful exploitation of the vulnerabilities could allow threat actors to conduct distributed denial-of-service (DDoS) attacks, ransomware attacks, structured query language (SQL) injection attacks, spear phishing campaigns, website defacements, and disinformation campaigns.

Read more:

[https://www.bleepingcomputer[.]com/news/security/fbi-and-cisa-warn-of-state-hackers-attacking-fortinet-fortios-servers/]

Attackers Are Abusing Github Infrastructure To Mine Cryptocurrency

2021.04.03 | Source(s): Security Affairs

Analysis:

The popular code repository hosting service GitHub is investigating a crypto-mining campaign abusing its infrastructure. According to security experts, threat actors are abusing the GitHub Actions feature which was implemented to allow the automatic execution of software workflows. Moreover, these threat actors are targeting repositories that have this feature enabled to add malicious GitHub Actions and fill malicious Pull Requests to execute the malicious attacker's code. Threat actors are executing their own malicious code to mine cryptocurrency miners on the infrastructure of the code repository hosting service, in some cases, attackers could deploy hundreds of miners in a single attack. These kinds of attacks have a significant impact on the computational capabilities of the abused infrastructure.

Read more:

[https://securityaffairs[.]co/wordpress/116294/malware/github-infrastructure-attacks-miner.html]

Spy Operations Target Vietnam with Sophisticated RAT

2021.04.05 | Source(s): Threatpost

Analysis:

An advanced cyberespionage campaign targeting government and military entities in Vietnam has been discovered that delivered a remote-access tool (RAT) for carrying out espionage operations. Researchers believed that the campaign was conducted by a Chinese-speaking advanced persistent threat (APT) known as Cycldek, also known as Goblin Panda, APT 27 and Conimes. The analysis showed that dozens of computers were targeted in the campaign with the vast majority (80 percent) located in Vietnam. The other targets were found in Central Asia and in Thailand. Dubbed as FoundCore, the malware allows attackers to conduct filesystem manipulation, process manipulation, screenshot captures and arbitrary command execution. The campaign also uses sideloading of dynamic-link libraries (DLLs), which happens when a legitimately signed file is tricked into loading a malicious DLL, allowing the attackers to bypass security products.

Read more:

[https://threatpost[.]com/spy-operations-vietnam-rat/165243/]

CERT-PH Recommendations:

- 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.
- Users are encouraged 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:
  - **Apple macOS:**
    - **Mojave** - version 10.14.6
    - **High Sierra** - version 10.13.6
    - **Catalina** – version 10.15.5
  - **FortiOS** - latest versions
- 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.*