CERT-PH Cybersecurity Threat Feeds

Issue Date	March 24, 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:

- Purple Fox Malware Worms its Way Into Exposed Windows Systems
- CISA Releases CHIRP, a Tool to Detect SolarWinds Malicious Activity
- DDoS Booters Abuse DTLS Servers to Amplify Attacks
- Google Fixes An Android Vulnerability that is Exploited in the Wild

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

Purple Fox Malware Worms its Way into Exposed Windows Systems

2021.03.23 | Source(s): Bleeping Computer

Analysis:

Dubbed as Purple Fox, which was previously distributed only via exploit kits and phishing emails, has now added a worm module that allows it to scan and infect Windows systems reachable over the Internet. The malware comes with rootkit and backdoor capabilities that targets Windows systems to infect Windows users through their web browsers after exploiting memory corruption and elevation privilege vulnerabilities. In addition, it has the capability to infect servers by brute-forcing its way in via vulnerable Internet-exposed SMB services and also utilizes phishing campaigns and web browser vulnerabilities to deploy its payloads. Once the malware is executed on a system, it will subsequently scan the Internet for other targets and attempt to compromise them and add them to its botnet.

Read more:

[https://www.bleepingcomputer[.]com/news/security/purple-fox-malware-worms-its-way-into-exposed-windows-systems/]

CISA Releases CHIRP, a Tool to Detect SolarWinds Malicious Activity

2021.03.21 | Source(s): Security Affairs, Bleeping Computer

Analysis:

CISA has released a new tool that can help in detecting malicious activity associated with the SolarWinds hackers in compromised on-premises enterprise environments. Dubbed as CISA Hunt and Incident Response Program (CHIRP), the Python-based tool has the ability to detect malicious activity associated with the SolarWinds hackers in compromised on-premises enterprise Windows environments. It is capable of scanning for signs of APT compromise by searching for IOCs associated with malicious activity detailed in its alerts, AA20-352A and AA21-008A. Moreover, it has a capability to examine Windows event logs for artifacts associated with this activity, Windows Registry for evidence of intrusion, query Windows network artifacts, and apply YARA rules to detect malware, backdoors, or implants.

Read more:

[https://securityaffairs[.]co/wordpress/115821/security/cisa-chirp-solarwinds-tool.html]
[https://www.bleepingcomputer[.]com/news/security/cisa-releases-new-solarwinds-malicious-activity-detection-tool/]

DDoS Booters Abuse DTLS Servers to Amplify Attacks

2021.03.22 | Source(s): Bleeping Computer

Analysis:

Cybersecurity experts observed that DDoS-for-hire services are now actively abusing misconfigured or out-of-date Datagram Transport Layer Security (D/TLS) servers to amplify Distributed Denial of Service (DDoS) attacks. DTLS is a UDP-based version of the Transport Layer Security (TLS) protocol

that prevents eavesdropping and tampering in delay-sensitive apps and services. Also known as stressers or booters, DDoS-for-hire platforms are now using DTLS as an amplification vector. Booster services are used by threat actors, pranksters, or hacktivists without the time to invest or skills to build their own DDoS infrastructure. They rent stresser services to launch DDoS attacks triggering a denial of service that commonly brings down targeted servers or sites or causes various levels of disruption.
[https://www.bleepingcomputer[.]com/news/security/ddos-booters-now-abuse-dtls-servers-to-amplify-attacks/]

Google Fixes an Android Vulnerability that is Exploited in the Wild

2021.03.23 | Source(s): Security Affairs, The Hacker News

Analysis:

Google addressed a zero-day vulnerability, affecting Android devices that use Qualcomm chipsets, which is actively exploited in the wild. Tracked as CVE-2020-11261, an improper input validation in Graphics that could allow attackers to access huge portion of the device's memory. According to security researchers, the memory corruption was due to improper check to return error when user application requests memory allocation of a huge size. In addition, attackers needs physical access to the vulnerable device to exploit the flaw.

Read more:
[https://securityaffairs[.]co/wordpress/115888/mobile-2/google-android-flaw-exploited.html]
[https://thehackernews[.]com/2021/03/warning-new-android-zero-day.html]

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.
- Update any vulnerable system/applications/devices to their latest and patched versions:
    - **Android System** – latest security patch
- System administrators are advised to check wether the DTLS services of their servers are open and are publicly available in the Internet and implement necessary actions such as closing the port, if unused, and use anti-spoofing mechanism to remove the DTLS amplification vector.
- Agencies mus 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.*