CERT-PH Cybersecurity Threat Feeds

Issue Date	March 08, 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:

- Multiple Cisco Products Exposed to DoS Attack Due to A Snort Issue
- Microsoft Reveals 3 New Malware Strains Used by SolarWinds Hackers
- Five Privilege Escalation Flaws Fixed in Linux Kernel
- REvil Ransomware Gang Uses DDoS Attacks And Voice Calls To Make Pressure On The Victims

- CRITICAL
- URGENT
- INFORMATION

Description

Microsoft Reveals 3 New Malware Strains Used by SolarWinds Hackers

2021.03.05 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Microsoft researchers discovered three new pieces of malware that the threat actors behind the SolarWinds attack, tracked as Nobelium. Tracked as GoldMax, Sibot and Goldfinder, the three pieces of malware were used by the threat actors to maintain persistence and perform malicious actions in very targeted attacks. The tailor-made malware were used as second-stage payloads, the attack vectors were compromised credentials, the SolarWinds binary, lateral movements conducted with the TEARDROP malware, or in some cases manually deployed. The first malware, dubbed GoldMax, is a Go-based malware used as a command-and-control backdoor by the attackers. The malware used a scheduled task impersonating systems management software as a persistence trick. GoldMax implements a decoy network traffic generator to hide network traffic and avoid detection. The second malware, dubbed Sibot, is a dual-purpose malicious code written in VBScript used by the threat actors to gain persistence and to download and execute a payload from a remote C2 server. The third malware is a malware written in Go, dubbed GoldFinder, likely used as a custom HTTP tracer tool that logs the route or hops that a packet takes to reach a hardcoded C2 server.

Read more:

[https://www.bleepingcomputer[.]com/news/security/microsoft-reveals-3-new-malware-strains-used-by-solarwinds-hackers/]

[https://securityaffairs[.]co/wordpress/115311/malware/microsoft-solarwinds-malware.html]

Multiple Cisco Products Exposed to DoS Attack Due to A Snort Issue

2021.03.06 | Source(s): Security Affairs

Analysis:

Cisco detected a vulnerability in the Snort detection engine that exposes several of its products to denial-of-service (DoS) attacks. Tracked as CVE-2021-1285, the vulnerability is due to improper handling of error conditions when processing Ethernet frames. An attacker could exploit this vulnerability by sending malicious Ethernet frames through an affected device. A successful exploit could allow the attacker to exhaust disk space on the affected device, which could result in administrators being unable to log in to the device or the device being unable to boot up correctly. The vulnerability has been rated high severity, received a CVSS score of 7.4 and affects all open source Snort project releases earlier than release 2.9.17.

Read more:

[https://securityaffairs[.]co/wordpress/115341/security/cisco-products-dos-snort-issue.html]

Five Privilege Escalation Flaws Fixed in Linux Kernel

2021.03.05 | Source(s): Security Affairs

Analysis:

Experts discovered five vulnerabilities in the Linux kernel that could lead to local privilege escalation. Tracked as CVE-2021-26708, the Linux kernel vulnerabilities are race conditions that reside in AF_VSOCK

implementation. The race conditions stems in wrong locking in net/vmw_vsock/af_vsock.c. The flaw received a CVSS score of 7.0. Successful exploitation may allow bypassing x86_64 platform protections such as SMEP and SMAP.

Read more:

[https://securityaffairs[.]co/wordpress/115296/security/privilege-escalation-flaws-linux-kernel.html]

REvil Ransomware Gang Uses DDoS Attacks and Voice Calls To Make Pressure On The Victims

2021.03.07 | Source(s): Security Affairs

Analysis:

Cybersecurity experts discovered that the REvil ransomware operators are using DDoS attacks and voice calls to journalists and victim's business partners to force victims to pay the ransom. Recently, the REvil ransomware gang published a job notice where they searched for experts to perform DDoS attacks and use VOIP calls to contact victims and their business partners. The malware researcher who goes online with the moniker 3xp0rt, reported that REvil operators are offering to their network of affiliates new options to make pressure on victims, in particular calls to news media and business partners for free, and DDoS (Layer 3 and 7) attacks as a paid service.

Read more:

[https://thehackernews[.]com/2021/03/hackers-now-hiding-obliquerat-payload.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.
- 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.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Linux Kernel** - version 5.11-rc7
  - **Cisco IOS XE Software** - latest version
  - **Cisco IOS XE SD-WAN Software** - latest version
  - **Snort** - version 2.9.17
- 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.*