CERT-PH Cybersecurity Threat Feeds

Issue Date	March 11, 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:

- Unpatched QNAP Devices Are Being Hacked to Mine Cryptocurrency
- Fake Google ReCAPTCHA Phishing Attack Swipes Office 365 Passwords
- Microsoft Releases Proxylogon Patches for Unsupported Microsoft Exchange Versions
- Google Chrome To Block Port 554 To Stop NAT Slipstreaming Attacks

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

Unpatched QNAP Devices Are Being Hacked to Mine Cryptocurrency

2021.03.08 | Source(s): Bleeping Computer, Security Affairs, ZDNet

Analysis:

Threat actors are observed to be targeting unpatched networked-attached storage (NAS) devices in ongoing attacks where the attackers try to take them over and install cryptominer malware to mine for cryptocurrency. According to cybersecurity experts, the threat actors exploit two-pre auth remote command execution (RCE) vulnerabilities in the Helpdesk app, tracked as CVE-2020-2506 and CVE-2020-2507, that could allow attackers to obtain control of a QNAP device. The flaws affect QNAP NAS firmware versions prior to August 2020 and were fixed by the vendor last October 2020. Dubbed as UnityMiner, this malware was involved in the campaign and was used to hide the mining process and the real CPU memory resource usage information to hide the malicious activity to QNAP owners that could check their system usage via the WEB management interface.

Read more:
[https://www.bleepingcomputer[.]com/news/security/unpatched-qnap-devices-are-being-hacked-to-mine-cryptocurrency/]
[https://securityaffairs[.]co/wordpress/115403/hacking/unityminer-qnap-nas-devices.html]
[https://www.zdnet[.]com/article/unityminer-cryptocurrency-malware-hijacks-qnap-storage-devices/]

Fake Google ReCAPTCHA Phishing Attack Swipes Office 365 Passwords

2021.03.08 | Source(s): Threatpost

Analysis:

Cybersecurity experts discovered a phishing campaign that targets Microsoft users by leveraging a bogus Google reCAPTCHA system. The attack begins with phishing emails pretending to be automated emails from victims' unified communications tools, which say that they have a voicemail attachment. Once the victims clicks on the attachment, they then encounter the fake Google reCAPTCHA screen, which contains a typical reCAPTCHA box, featuring a checkbox that the user must click that says "I'm not a robot", which then triggers the turing test. After filling out the fake reCAPTCHA system, victims are then directed to what appears to be a Microsoft login screen. After giving the login credentials, the phishing campaign will show a fake message that says 'Validation successful' then users are then shown a recording of a voicemail message that they can play, allowing threat actors to avoid suspicion.

Read more:
[https://threatpost[.]com/google-recaptcha-phishing-office-365/164566/]

Microsoft Releases Proxylogon Patches for Unsupported Microsoft Exchange Versions

2021.03.09 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Microsoft released ProxyLogon security updates for Microsoft Exchange servers running vulnerable unsupported Cumulative Update versions to address four zero-day issues tracked as CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 respectively. According to security researchers, the China-linked APT group tracked as HAFNIUM, chained these vulnerabilities to access on-premises Exchange servers to access email accounts and install backdoors to maintain access to victim environments. These updates temporarily protect the servers of its customers until they can install the latest updates for the Exchange servers.

Read more:
[https://securityaffairs[.]co/wordpress/115428/security/microsoft-exchange-emergency-update.html]
[https://www.bleepingcomputer[.]com/news/security/microsoft-releases-proxylogon-updates-for-unsupported-exchange-servers/]

Google Chrome To Block Port 554 To Stop NAT Slipstreaming Attacks

2021.03.08 | Source(s): Bleeping Computer

Analysis:

Google Chrome will block the browser's access to TCP port 554 to protect against attacks using the NAT Slipstreaming 2.0 vulnerability. Last year, security researchers disclosed a new version of the NAT Slipstreaming vulnerability that allows malicious scripts to bypass a website visitor's NAT firewall and access any TCP/UDP port on the visitor's internal network. As this vulnerability only works on specific ports monitored by a router's Application Level Gateway (ALG), browser developers, including Google, Safari, and Mozilla, have been blocking vulnerable ports that do not receive a lot of traffic.

Read more:
[https://www.bleepingcomputer[.]com/news/security/google-chrome-to-block-port-554-to-stop-nat-slipstreaming-attacks/]

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:

  - QNAP QNAS firmware - Latest version
  - Microsoft Exchange - March Security Updates
- 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.*