CERT-PH Cybersecurity Threat Feeds

Issue Date	January 22, 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:

- Microsoft Shares How SolarWinds Hackers Evaded Detection
- QNAP Warns Users to Secure NAS Devices Against Dovecat Malware
- Windows Remote Desktop Servers Used to Amplify DDoS Attacks
- Google Forms Set Baseline for Widespread BEC Attacks

- CRITICAL
- URGENT
- INFORMATION

Description

Microsoft Shares How SolarWinds Hackers Evaded Detection

2021.01.20 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Microsoft shared details on how the SolarWinds hackers were able to remain undetected by hiding their malicious activity inside the networks of breached companies. The hackers who orchestrated the SolarWinds attack showcased a range of tactics, operational security, and anti-forensic behavior that drastically decreased the breached organizations' ability to detect their malicious actions. The new analysis shed lights on the handover from the Solorigate DLL backdoor to the Cobalt Strike loader. The attackers focused on separating these two components of the attack chain as much as possible to evade detection.

Read more:

[https://www.bleepingcomputer[.]com/news/security/microsoft-shares-how-solarwinds-hackers-evaded-detection/]
[https://securityaffairs[.]co/wordpress/113681/apt/microsoft-solorigate.html]

QNAP Warns Users to Secure NAS Devices Against Dovecat Malware

2021.01.21 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Taiwanese vendor QNAP, urges customers to secure their network-attached storage (NAS) devices against an ongoing malware campaign that infects and exploits them to mine bitcoin without their knowledge. Dubbed as Dovecat, the malware is designed to abuse NAS resources and mine cryptocurrency . User reports of this malware campaign have been surfacing with customers saying that affected NAS devices are almost unusable due to the Bitcoin miner hogging up almost all CPU and memory resources.

Read more:

[https://www.bleepingcomputer[.]com/news/security/qnap-warns-users-to-secure-nas-devices-against-dovecat-malware/]
[https://securityaffairs[.]co/wordpress/113710/malware/qnap-dovecat-malware.html]
[https://www.zdnet[.]com/article/qnap-warns-users-of-a-new-crypto-miner-named-dovecat-infecting-their-devices/]

Windows Remote Desktop Servers Used to Amplify DDoS Attacks

2021.01.21 | Source(s): Bleeping Computer

Analysis:

Windows Remote Desktop Protocol (RDP) servers are now being abused by DDoS-for-hire services to amplify Distributed Denial of Service (DDoS) attacks. The Microsoft RDP service is a built-in Windows service running on TCP/3389 and/or UDP/3389 that enables authenticated remote virtual desktop infrastructure (VDI) access to Windows servers and workstations. Attacks taking advantage of this new UDP reflection/amplification attack vector by targeting Windows servers with RDP enabled on UDP/3389 have an amplification ratio of 85.9:1 and peak at ~750 Gbps. Such platforms are used by threat actors, hacktivists, or pranksters without the skills or time to invest in building up their own DDoS infrastructure.

Read more:

[https://www.bleepingcomputer[.]com/news/security/windows-remote-desktop-servers-now-used-to-amplify-ddos-attacks/]

Google Forms Set Baseline for Widespread BEC Attacks

2021.01.21 | Source(s): Threatpost

Analysis:

Researchers warn that attackers are collecting reconnaissance for future business email compromise attacks using Google Forms. A threat actor has been sending thousands of emails to organizations, in what researchers warn is a reconnaissance campaign to identify targets for a possible follow-up business-email-compromise (BEC) attack. The messages contain unique names of C-level executives from the target organizations, indicating that the cybercriminals have done their homework when it comes to pinpointing victims. Researchers believe that the primary goal is to elicit an email reply from the victim, to respond that the survey is broken or not what they expected. That can then set the ball rolling for further dialogue between the victim and attacker, setting the foundation for the future BEC attack.

Read more:

[https://threatpost[.]com/google-forms-set-baseline-for-widespread-bec-attacks/163223/]

CERT-PH Recommendations:

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

- QNAP - QTS latest version

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 Organizations are advised to implement DDoS defenses for public-facing servers to make sure that they can properly respond to an incoming RDP reflection/amplification DDoS attack.

o QNAP customers are advised to follow best practices for enhancing their NAS device's security as detailed on QNAP's support website.

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.