CERT-PH Cybersecurity Threat Feeds

Issue Date	April 26, 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:

- Phishing Impersonates Global Recruitment Firm To Push Malware
- A New Linux Botnet Abuses Iac Tools To Spread And Other Emerging Techniques
- Passwordstate Password Manager Hacked in Supply Chain Attack
- New Qlocker Ransomware Infected Hundreds of QNAP NAS devices

- CRITICAL
- URGENT
- INFORMATION

Description

Phishing Impersonates Global Recruitment Firm to Push Malware

2021.04.23 | Source(s): Bleeping Computer

Analysis:

Cybersecurity researchers discovered a phishing campaign impersonating a global recruitment firm to push malware capable of harvesting credentials and sensitive data from infected computers. These emails use embedded links to redirect potential victims to phishing landing pages featuring GeoIP and antibot checks. The victims are then asked to download archives containing malicious macro-enabled Microsoft Excel spreadsheets (XSLM) and featuring DocuSign branding, asking the targets to enable editing to decrypt and open the document. Once the victims enable macros, they are shown a decoy document with information on a fake management position, while the malware payload is downloaded and installed on their computer in the background. Dubbed as Ursnif, the malware is an information-stealing trojan and an offspring of the original Gozi banking trojan capable of recording the victims' keystrokes, the sites they visit, harvests clipboard content, and collects all this info into log files and sent back to its operators' servers. Using this stolen info, the attackers can steal their victims' login credentials and other sensitive data to further compromise their accounts or networks.

Read more:

[https://www.bleepingcomputer[.]com/news/security/phishing-impersonates-global-recruitment-firm-to-push-malware/]

New Linux Botnet Abuses IaC Tools to Spread and other Emerging Techniques

2021.04.24 | Source(s): Security Affairs

Analysis:

Experts spotted a new Linux botnet employing multiple emerging techniques among cyber-criminals, including the use of Tor proxies, the abuse of legitimate DevOps tools, and the removal or deactivation of competing malware. this Linux botnet downloads all the files it needs from the Tor network, including legitimate binaries like ss, ps, and curl. Botmasters maintain a big network of proxies that receive the connection coming from the surface web. The malware also performs HTTP requests using shell script and Unix system design to get more information on the infected systems. The malware leverages a network of proxies to convert the requests to the Tor network before reaching out to the server and retrieving the files. In addition, the malware could run on different architectures using Linux-based OS, a circumstance that suggests that the botnet was involved in a wider campaign targeting Linux systems.

Read more:

[https://securityaffairs[.]co/wordpress/117155/malware/linux-botnet-emerging-techniques.html]

Passwordstate Password Manager Hacked in Supply Chain Attack

2021.04.23 | Source(s): Bleeping Computer, The Hacker News

Analysis:
Click Studios, the company behind the Passwordstate enterprise password manager, notified customers that attackers compromised the app's update mechanism to deliver malware in a supply-chain attack after breaching its networks. According to security researchers, initial analysis indicates that bad actors using sophisticated techniques had compromised the In-Place Upgrade functionality and malicious upgrades were potentially downloaded by customers between April 20 and April 22. Dubbed as Moserpass, the malware would collect system information and Passwordstate data, which later gets sent to attacker-controlled servers. The attackers crudely added a 'Loader' code section, just an extra 4KB from an older version, to Passwordstate's original code.
Read more:
[https://www.bleepingcomputer[.]com/news/security/passwordstate-password-manager-hacked-in-supply-chain-attack/]
[https://thehackernews[.]com/2021/04/passwordstate-password-manager-update.html]

New Qlocker Ransomware Infected Hundreds of QNAP NAS devices

2021.04.23 | Source(s): Security Affairs, The Hacker News, Bleeping Computer
Analysis:
Researchers discovered a new strain of ransomware is infecting hundreds of QNAP NAS devices on daily bases. Dubbed as Qlocker, the malware moves all files stored on the device to password-protected 7zip archives and demands the payment of a $550 ransom. QNAP warns its customers of the ongoing attacks and is urging them to install the latest Malware Remover version and scan their devices for indicators of compromise.
Read more:
[https://securityaffairs[.]co/wordpress/117144/malware/qlocker-ransomware-infections.html]
[https://thehackernews[.]com/2021/04/new-qnap-nas-flaws-exploited-in-recent.html]
[https://www.bleepingcomputer[.]com/news/security/a-ransomware-gang-made-260-000-in-5-days-using-the-7zip-utility/]

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.
- Passwordstate customers who have upgraded their client during the breach (April 20-22) are urged to reset all passwords in their Passwordstate database.
- QNAP users are advised to install the latest Malware Remover version and run a malware scan as a precautionary measure.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - QNAP NAS:
    - Multimedia Console - latest version
    - Media Streaming Add-on - latest version
    - Hybrid Backup Sync - latest version
- 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.*