CERT-PH Cybersecurity Threat Feeds

Issue Date	January 07, 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:

- Cross-platform ElectroRAT Malware Drains Cryptocurrency Wallets
- Series of Ransomware Attacks Linked to China-linked APT27 Group
- Babuk Locker Is the First New Enterprise Ransomware Of 2021
- Hackers Start Exploiting Recently Disclosed Zyxel Vulnerability

- CRITICAL
- URGENT
- INFORMATION

Description

Cross-platform ElectroRAT Malware Drains Cryptocurrency Wallets

2021.01.05 | Source(s): Bleeping Computer, Security Affairs, ZDNet

Analysis:

Security researchers discovered a large-scale operation targeting cryptocurrency users with a previously undetected RAT. Dubbed as ElectroRAT, is a malware that is written in Golang and compiled to target multiple operating systems: Windows, Linux and MacOS. In addition, the attackers developed three different malicious applications as part of this campaign, the cryptocurrency trade management applications “Jamm” and “eTrade” and the cryptocurrency poker app “DaoPoker”. Once a victim runs the application, an innocent GUI will open, while ElectroRat runs hidden in the background as “mdworker”. Finally, the malware then steals all funds from the victim’s wallet.

Read more:

[https://securityaffairs[.]co/wordpress/113064/malware/electrorat-campaign.html]
[https://www.bleepingcomputer[.]com/news/security/cross-platform-electrorat-malware-drains-cryptocurrency-wallets/]
[https://www.zdnet[.]com/article/hackers-target-cryptocurrency-users-with-new-electrorat-malware/]

Series of Ransomware Attacks Linked to China-linked APT27 Group

2021.01.05 | Source(s): Security Affairs, Bleeping Computer

Analysis:

Cybersecurity experts linked a series of ransomware attacks to the Chinese cyberespionage group APT27 (aka Emissary Panda, TG-3390, Bronze Union, and Lucky Mouse). The recent attacks were aimed at several gambling companies. The researchers also spotted a web shell name ASPXSpy, which is a modified version of this malware that has been employed in attacks attributed to APT27, in addition to a backdoor, dubbed as Clambling, and a remote access trojan, dubbed as PlugX, which is widely used by China-linked threat actors.

Read more:

[https://securityaffairs[.]co/wordpress/113000/apt/apt27-ransomware-attacks.html]
[https://threatpost[.]com/ransomware-major-gaming-companies-apt27/162735/]
[https://www.bleepingcomputer[.]com/news/security/chinas-apt-hackers-move-to-ransomware-attacks/]

Babuk Locker Is the First New Enterprise Ransomware Of 2021

2021.01.05 | Source(s): Bleeping Computer

Analysis:

Babuk Locker is a new ransomware operation that launched at the beginning of 2021 and targets corporate victims in human-operated attacks. Security experts discovered that each Babuk Locker executable has been customized on a per-victim basis to contain a hardcoded extension, ransom note, and a Tor victim URL. When encrypting files, Babuk Locker will use a hardcoded extension and append it to each encrypted file. Unfortunately, the ransomware's use of ChaCha8 and Elliptic-curve Diffie–Hellman (ECDH) makes the ransomware secure and not decryptable for free.

Read more:

[https://www.bleepingcomputer[.]com/news/security/babuk-locker-is-the-first-new-enterprise-ransomware-of-2021/]

Hackers Start Exploiting Recently Disclosed Zyxel Vulnerability

2021.01.06 | Source(s): Security Affairs, Bleeping Computer

Analysis:

Threat actors have been detected to be targeting Zyxel's firewall and WLAN controller products that contains an undocumented account with an unchangeable password, which can be found in cleartext in the product's firmware. Tracked as CVE-2020-29583, a hardcoded credential vulnerability that exists in Zyxel firewalls and AP controllers with an unchangeable static plain-text password and administrative privilege. Successful exploitation of the flaw could allow an attacker to access this user account remotely and compromise affected Zyxel devices.

Read more:

[https://securityaffairs[.]co/wordpress/113076/hacking/cve-2020-29583-zyxel-under-attack.html?utm_source=rss&utm_medium=rss&utm_campaign=cve-2020-29583-zyxel-under-attack]
[https://www.bleepingcomputer[.]com/news/security/hackers-start-exploiting-the-new-backdoor-in-zyxel-devices/]

CERT-PH Recommendations:

o Users are advised to check their device and immediately remove the following applications and kill related processes and files:
- **Jamm**
- **eTrade**
- **DaoPoker**

o Update any vulnerable system/applications/devices to their latest and patched versions:
- **ATP series running firmware ZLD V4.60** - ZLD V4.60 Patch 1
- **USG series running firmware ZLD V4.60** - ZLD V4.60 Patch 1
- **USG FLEX series running firmware ZLD V4.60** - ZLD V4.60 Patch 1
- **VPN series running firmware ZLD V4.60** - ZLD V4.60 Patch 1

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.