CERT-PH Cybersecurity Threat Feeds

Issue Date	May 11, 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:

- Over 25% Of TOR Exit Relays Spied On Users' Dark Web Activities
- Us and Australia Warn of Escalating Avaddon Ransomware Attacks
- iPhone Hack Allegedly Used to Spy on China's Uyghurs
- Researchers Provides Technical Details of FiveHands Ransomware

- CRITICAL
- URGENT
- INFORMATION

Description

Over 25% Of TOR Exit Relays Spied On Users' Dark Web Activities

2021.05.10 | Source(s): Hacker News

Analysis:

A new study on the dark web infrastructure revealed that an unknown threat actor managed to control more than 27% of the entire Tor network exit capacity in early February 2021. Exit nodes on the Tor network have been subverted in the past to inject malware such as OnionDuke, but this is the first time a single unidentified actor has managed to control such a large fraction of Tor exit nodes. According to security experts, the main purpose of the attack is to carry out "person-in-the-middle" attacks on Tor users by manipulating traffic as it flows through its network of exit relays. Specifically, the attacker appears to perform what's called SSL stripping to downgrade traffic heading to Bitcoin mixer services from HTTPS to HTTP in an attempt to replace bitcoin addresses and redirect transactions to their wallets instead of the user-provided bitcoin address.

Read more:

[https://thehackernews[.]com/2021/05/over-25-of-tor-exit-relays-are-spying.html]

Us and Australia Warn of Escalating Avaddon Ransomware Attacks

2021.05.09 | Source(s): Security Affairs

Analysis:

Cybersecurity experts warn of an ongoing Avaddon ransomware campaign targeting organizations from an extensive array of sectors in the US and worldwide. The ransomware gang's affiliates are targeting entities from a wide range of sectors, including but not limited to government, finance, law enforcement, energy, information technology, and health. In addition to leaking stolen data and encrypting their system, Avaddon threat actors threaten with denial-of-service (DDoS) attacks to persuade victims into paying ransoms. Moreover, Affiliates who join this RaaS operation are responsible for compromising networks to deploy payloads or distribute the ransomware via spam or exploit kits. At the same time, its operators are accountable for developing the malware and operating the TOR payment site. Avaddon pays each affiliate 65% of ransom payments they bring in, with the operators getting a 35% share. However, as with other RaaS programs, larger affiliates can usually negotiate higher revenue shares depending on the size of their attacks. Avaddon ransomware affiliates are also known for stealing data from their victims' networks before encrypting systems for double-extortion.

Read more:

[https://securityaffairs[.]co/wordpress/117721/security/anti-spam-wordpress-plugin-flaw.html]

iPhone Hack Allegedly Used to Spy on China's Uyghurs

2021.05.06 | Source(s): Threatpost

Analysis:

Cybersecurity researchers unveiled an intricately woven exploit that would allegedly let a remote attacker easily jailbreak an iPhone X iOS 12.1. Dubbed as Chaos, the exploit would allow a remote

attacker to jailbreak an iPhoneX, with the targeted user none the wiser, allowing the intruder to gain access to a victim's data, processing power and more. It worked as a drive-by malware download, only requiring that the iPhone user visit a web page containing malicious code. Apple issued an update to patch the flaw in January 2019.

Read more:

[https://threatpost[.]com/iphone-hack-spying-china-uyghurs/165950/]

Technical Details of FiveHands Ransomware Exploiting SonicWall Devices

2021.05.09 | Source(s): Security Affairs

Analysis:

Researchers from FireEye's Mandiant revealed that a sophisticated cybercrime gang tracked as UNC2447 has exploited an issue in SonicWall Secure Mobile Access (SMA) devices. Tracked as CVE-2021-20016, the flaw is a zero-day vulnerability in the SonicWall SMA100 build version 10.x resulting in improper SQL command neutralization in the SonicWall SSLVPN SMA100 product allows remote exploitation for credential access by an unauthenticated attacker. The malware employed by the group since 2020, includes Sombrat, FiveHands, the Warprism PowerShell dropper, the Cobalt Strike beacon, and FoxGrabber. UNC2447 extortion activity employed the FIVEHANDS ransomware, the threat actors aggressively threatened victims to disclose their hack on the media to sell the data on hacker forums. According to researchers, they are aware of a recent successful cyberattack against an organization using FiveHands ransomware, SombRAT, and open-source tools to ultimately steal information, obfuscate files, and demand a ransom. The malware will also encrypt files in the recovery folder at C:\Recovery, then it will write a ransom note to each folder and directory on the system called 'read_me_unlock.txt'. FiveHands ransomware uses a public key encryption scheme called NTRUEncrypt, it enumerates Volume Shadow copies with Windows Management Instrumentation (WMI) before deleting them to make it impossible to recover data. The FiveHands ransomware is written in C++ and presents multiple similarities with the DeathRansom, and both malware strains show a connection to the HelloKitty ransomware.

Read more:

[https://securityaffairs[.]co/wordpress/117672/cyber-crime/bec-gift-card-scam.html]

CERT-PH Recommendations:

- Organizations may block or monitor all web traffic to and from public Tor entry and exit nodes.
- In other cases, blocking contents from some Tor resources and allow monitoring for others
- Users are urged to be cautious and check the email thoroughly before downloading and opening email attachments, especially when received from unknown email senders, as ransomware are usually found on email attachments and pirated application software.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Apple iOS** - version 12.1.3 or later
  - **SonicWall SMA100** - version 10.2.0.5-d-29sv
- 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.*