CERT-PH Cybersecurity Threat Feeds

Issue Date	May 14, 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:

- Microsoft: Threat Actors Target Aviation Orgs With New Malware
- FragAttacks Vulnerabilities Expose All WiFi Devices To Hack
- Cisco Fixes 6-month-old AnyConnect VPN Zero-Day with Exploit Code
- Cybersecurity Experts Warns of a New Android Banking Trojan Stealing Users' Credentials

- CRITICAL
- URGENT
- INFORMATION

Description

Microsoft: Threat Actors Target Aviation Orgs with New Malware

2021.05.12 | Source(s): Bleeping Computer

Analysis:

Microsoft warns of an ongoing spear-phishing campaign targeting aerospace and travel organizations with multiple remote access trojans (RATs) deployed using a new and stealthy malware loader. Attackers' phishing emails spoof legitimate organizations and use image lures posing as PDF documents containing info relevant to several industry sectors, including aviation, travel, and cargo. Dubbed as Snip3, the newly discovered loader monetized under a Crypter-as-a-Service model, is used to drop Revenge RAT, AsyncRAT, Agent Tesla, and NetWire RAT payloads on compromised systems. According to security experts, the threat actors' end goal is to harvest and exfiltrate data from infected devices using the RATs' remote control, keylogging, and password-stealing capabilities. Snip3 comes with the ability to identify sandboxing and virtual environments which makes it particularly capable of circumventing detection-centric anti-malware solutions. To avoid detection, the malware loader uses additional techniques such as execution of PowerShell code with the 'remotesigned' parameter, use of Pastebin and top4top for staging and compilation of RunPE loaders on the endpoint in runtime.

Read more:

[https://www.bleepingcomputer[.]com/news/security/microsoft-threat-actors-target-aviation-orgs-with-new-malware/]
[https://securityaffairs[.]co/wordpress/117858/cyber-crime/microsoft-aerospace-travel-sectors-attacks.html]

FragAttacks Vulnerabilities Expose All WiFi Devices To Hack

2021.05.12 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Security researchers discovered a series of flaws that impact the WiFi devices including computers, smartphones, and smart devices sold for the past 24 years. Three of these bugs are Wi-Fi 802.11 standard design flaws in the frame aggregation and frame fragmentation functionalities affecting most devices, while others are programming mistakes in Wi-Fi products. The three flaws were an aggregation attack, a mixed key attack and a fragment cache attack and were tracked as CVE-2020-24588, CVE-2020-24587 and CVE-2020-24586, respectively. The vulnerabilities could be exploited by an attacker within a device's WiFi radio range to steal info from it and also execute malicious code. The devices were exposed to the FragAttacks even if they were using WiFi security protocols such as WEP, WPA, and WPA3. In addition, several implementation vulnerabilities were also detected by researchers and are tracked CVE-2020-26145, CVE-2020-26144, CVE-2020-26140, CVE-2020-26143, CVE-2020-26139, CVE-2020-26146, CVE-2020-26147, CVE-2020-26142 and CVE-2020-26141. The vulnerabilities affect all major operating systems, including Windows, Linux, Android, macOS, and iOS.

Read more:

[https://securityaffairs[.]co/wordpress/117819/hacking/wifi-fragattacks.html]
[https://www.bleepingcomputer[.]com/news/security/all-wi-fi-devices-impacted-by-new-fragattacks-vulnerabilities/]

Cisco Fixes 6-month-old AnyConnect VPN Zero-Day with Exploit Code

2021.05.13 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Cisco has fixed a six-month-old zero-day vulnerability found in the Cisco AnyConnect Secure Mobility Client VPN software, with publicly available proof-of-concept exploit code. Tracked as CVE-2020-3556, the high-severity flaw exists in the CiscoAnyConnect Client's interprocess communication (IPC) channel, and can be exploited by threat actors to allow authenticated and local attackers to execute malicious scripts via a targeted user. The flaw affects all Windows, Linux, and macOS client versions with vulnerable configurations; however, mobile iOS and Android clients are not impacted. Moreover, successful exploitation requires active AnyConnect sessions and valid credentials on the targeted device.

Read more:

[https://www.bleepingcomputer[.]com/news/security/cisco-fixes-6-month-old-anyconnect-vpn-zero-day-with-exploit-code/]
[https://securityaffairs[.]co/wordpress/117855/security/cisco-anyconnect-zero-day.html]

Cybersecurity Experts Warns of a New Android Banking Trojan Stealing Users' Credentials

2021.05.11 | Source(s): The Hacker News

Analysis:

Cybersecurity researchers disclosed a new Android trojan that hijacks users' credentials and SMS messages to facilitate fraudulent activities against banks in Spain, Germany, Italy, Belgium, and the Netherlands. Dubbed as TeaBot, the malware is believed to be in its early stages of development with malicious attacks targeting financial apps commencing in late March 2021, followed by a rash of infections in the first week of May against Belgium and Netherlands banks. According to security experts, the main goal of TeaBot is stealing victim's credentials and SMS messages for enabling fraud scenarios against a predefined list of banks. Once TeaBot is successfully installed in the victim's device, attackers can obtain a live streaming of the device screen (on demand) and also interact with it via Accessibility Services. The rogue Android application, which masquerades as media and package delivery services acts as a dropper that not only loads a second-stage payload but also forces the victim into granting it accessibility service permissions. TeaBot exploits the access to achieve real-time interaction with the compromised device, enabling the adversary to record keystrokes, in addition to taking screenshots and injecting malicious overlays on top of login screens of banking apps to steal credentials and credit card information. TeaBot is also capable of disabling Google Play Protect, intercepting SMS messages, and accessing Google Authenticator 2FA codes. The collected information is then exfiltrated every 10 seconds to a remote server controlled by the attacker.

Read more:

[https://thehackernews[.]com/2021/05/experts-warn-of-new-android-banking.html]

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.
- 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:
  - **AnyConnect Secure Mobility Client Software - version 4.10.00093 or later**
- 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.*