CERT-PH Cybersecurity Threat Feeds

Issue Date	April 23, 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:

- Pareto Botnet, Million Infected Android Devices Conduct Fraud in the CTV Ad Ecosystem
- North Korea-linked Lazarus APT Hides Malicious Code Within BMP Image to Avoid Detection
- Telegram Platform Abused in 'ToxicEye' Malware Campaigns
- Prometei Botnet Hunting for Unpatched Microsoft Exchange Servers

- CRITICAL
- URGENT
- INFORMATION

Description

Pareto Botnet, Million Infected Android Devices Conduct Fraud in the CTV Ad Ecosystem

2021.04.22 | Source(s): Security Affairs

Analysis:

Cybersecurity researchers discovered a huge botnet of Android devices being used to conduct fraud in the connected TV advertising ecosystem. Dubbed as Pareto, the botnet is composed of nearly a million infected mobile Android devices and was used to emulate the activity of millions of people watching ads on smart TVs and other devices. Pareto works by spoofing signals using the malicious Android mobile apps to impersonate consumer TV streaming products running Fire OS, tvO, Roku OS and other prominent CTV platforms.

Read more:

[https://securityaffairs[.]co/wordpress/117110/malware/pareto-botnet.html]

North Korea-linked Lazarus APT Hides Malicious Code Within BMP Image to Avoid Detection

2021.04.20 | Source(s): Security Affairs

Analysis:

Security experts discovered a spear-phishing attack conducted by a North Korea-linked Lazarus APT group that obfuscated a malicious code within a bitmap (.BMP) image file. The malicious code within the bitmap image file was used by threat actors to drop a remote access trojan (RAT) on the victims' systems that allow them to steal sensitive information. The attack chain related to the spear-phishing campaign begins using a weaponized Microsoft Office document in the Korean language. The email attempts to trick victims into enabling the macros in order to view the content, but once enabled the macros in order a malicious code is executed. The macro first calls MsgBoxOKCancel function that pops up a message box to the user with a message claiming to be an older version of Microsoft Office. In the background, the macro calls an executable HTA file compressed as a zlib file that is included within an overall PNG image file. The HTA drops a loader for a Remote Access Trojan (RAT), which is stored as "AppStore.exe" on the target machine. The RAT connects the command-and-control (C2) server to receive commands and drop shellcode.

Read more:

[https://securityaffairs[.]co/wordpress/117035/apt/lazarus-apt-bmp-image.html]

Telegram Platform Abused in 'ToxicEye' Malware Campaigns

2021.04.22 | Source(s): Threatpost

Analysis:

Threat actors are leveraging the popular Telegram messaging app by embedding its code inside a remote access trojan. Dubbed as ToxicEye, the malware can take over file systems, install ransomware and leak data from victim's PCs. The Telegram RAT attacks begin with threat actors

creating a Telegram account and a dedicated Telegram bot, or remote account that allows them to interact with other users in various ways. Attackers then bundle the bot token with the RAT or other chosen malware and spread the malware via email-based spam campaigns as an email attachment. Once a victim opens the malicious attachment, it connects to Telegram and leaves the machine vulnerable to a remote attack via the Telegram bot, which uses the messaging service to connect the victim's device back to that attackers' command-and-control server.

Read more:

[https://threatpost[.]com/telegram-toxiceye-malware/165543/]

Prometei Botnet Hunting for Unpatched Microsoft Exchange Servers

2021.04.22 | Source(s): ZDNet

Analysis:

Cybercriminals are trying to use vulnerabilities in Microsoft Exchange servers to add to their botnet for mining cryptocurrency to gain access on systems. Dubbed as Prometei, the botnet is a widespread global campaign that is targeting organizations in a multi-stage attack. Prometei is scanning the internet for organizations that have yet to apply the patch and using that to gain a foothold on networks. According to security experts, The main objective of the attackers is to install cryptojacking malware to mine for Monero, allowing the criminals to secretly use the processing power of infected devices to line their pockets with cryptocurrency. Prometei uses the vulnerabilities in Microsoft Exchange servers to gain initial access to the network and attempts to infect as many endpoints as it can using a variety of known attack techniques to move laterally around networks. Including harvesting login credentials, exploiting RDP vulnerabilities and even using older exploits such as EternalBlue and BlueKeep to move around networks, performing the reconnaissance required to compromise as many machines as possible.

Read more:

[https://www.zdnet[.]com/article/now-this-botnet-is-hunting-for-unpatched-microsoft-exchange-servers/]

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 check their system for a rat.exe located within the directory C:\Users\ToxicEye\rat.exe and immediately delete the file.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Microsoft Exchange Server** - latest patched version
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Email Security (Windows)** - version 10.0.9.6173
  - **Email Security (Hardware & ESXi Virtual Appliance)** - version 10.0.9.6177
  - **Hosted Email Security** - version 10.0.9.6173
  - **Google Chrome** - version 90.0.4430.85
- Android users are urged to check their devices and immediately uninstall and remove the following applications:
  - **Flash Light (digtoymedia.flashight)**
  - **Mobile Screen Recorder (wwmmedia.screenrecorder)**
  - **Sling Puck 3D Challenge**
  - **Hole Ball King**
  - **Carpet Clean 3D**
  - **Save The Balloons**
  - **Light Torch SOS**
  - **Any Light**
  - **Bump Challenge – MultiSport**
- 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.*