CERT-PH Cybersecurity Threat Feeds

Issue Date	May 20, 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:

- MountLocker Ransomware Uses Windows API To Worm Through Networks
- Google Addresses 4 Zero-day Flaws In Android Exploited In The Wild
- Google Clouds Hijacked for Gobs of Phishing
- Keksec Cybergang Debuts Simps Botnet for Gaming DDoS

- CRITICAL
- URGENT
- INFORMATION

Description

MountLocker Ransomware Uses Windows API To Worm Through Networks

2021.05.19 | Source(s): Bleeping Computer

Analysis:

Cybersecurity experts shared a sample of what was believed to be a new MountLocker executable that contains a new worm feature that allows it to spread and encrypt to other devices on the network. A brief analysis determined that users could enable the worm feature by running the malware sample with the /NETWORK command-line argument. It was discovered that MountLocker is now using the Windows Active Directory Service Interfaces API as part of its worm feature. The ransomware first uses the NetGetDCName() function to retrieve the name of the domain controller. Then it performs LDAP queries against the domain controller's ADS using the ADsOpenObject() function with credentials passed on the command line. Once it connects to the Active Directory services, it will iterate over the database for objects of 'objectclass=computer'. For each object it finds, MountLocker will attempt to copy the ransomware executable to the remote device's '\C$\ProgramData' folder. The ransomware will then remotely create a Windows service that loads the executable so it can proceed to encrypt the device. Using this API, the ransomware can find all devices that are part of the compromised Windows domain and encrypt them using stolen domain credentials.

Read more:

[https://www.bleepingcomputer[.]com/news/security/mountlocker-ransomware-uses-windows-api-to-worm-through-networks/]

Google Addresses 4 Zero-day Flaws In Android Exploited In The Wild

2021.05.19 | Source(s): Security Affairs, Bleeping Computer

Analysis:

Android Security Bulletin for May 2021 security updates address four zero-day vulnerabilities that were actively exploited in the wild. The four zero-day vulnerabilities impact Qualcomm GPU and Arm Mali GPU Driver components. Tracked as CVE-2021-1905, the first flaw is a Qualcomm - Use After Free in Graphics. Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. The second flaw, tracked as CVE-2021-1906, is a Qualcomm - Detection of Error Condition Without Action in Graphics and is due to Improper handling of address deregistration on failure can lead to new GPU address allocation failure. For the third flaw, tracked as CVE-2021-28663, the vulnerability is an ARM - Mali GPU Kernel Driver that allows improper operations on GPU memory. A non-privileged user can make improper operations on GPU memory to enter into a use-after-free scenario and may be able to gain root privilege, and/or disclose information. The last flaw, tracked as CVE-2021-28664, is an ARM - Mali GPU Kernel Driver elevates CPU RO pages to writable. A non-privileged user can get write access to read-only memory, and may be able to gain root privilege, corrupt memory and modify the memory of other processes.

Read more:
[https://www.bleepingcomputer[.]com/news/security/may-android-security-updates-patch-4-zero-days-exploited-in-the-wild/]
[https://securityaffairs[.]co/wordpress/118089/mobile-2/android-4-zero-day-flaws.html]

Google Clouds Hijacked for Gobs of Phishing

2021.05.19 | Source(s): Threatpost

Analysis:

Threat actors are cashing in on the rapid shift to cloud-based business services during the pandemic, by hiding behind ubiquitous, trusted services from Microsoft and Google to make their email phishing scams look legit. Attackers sent 52M malicious messages leveraging the likes of Office 365, Azure, OneDrive, SharePoint, G-Suite and Firebase storage. According to researchers, the malicious message volume from these trusted cloud services exceeded that of any botnet in 2020, and the trusted reputation of these domains increases the difficulty of detection for defenders. Once attackers have credentials, they can easily move in and out of a range of services and use those to send additional and convincing phishing emails.

Read more:
[https://threatpost[.]com/microsoft-google-clouds-hijacked-phishing/166329/]

Keksec Cybergang Debuts Simps Botnet for Gaming DDoS

2021.05.19 | Source(s): Threatpost

Analysis:

Cybersecurity researchers discovered a recently developed malware that infects Internet of Things (IoT) devices in tandem with the prolific Gafgyt botnet using publicly known security vulnerabilities. Dubbed as Simps, the botnet was developed to carry out distributed denial-of-service (DDoS) attacks on gaming targets and others, using IoT nodes. It's part of the toolset used by the Kek Security (KekSec) cybercrime group. According to the experts, Simps was first seen in April being dropped on IoT devices by the Gafgyt botnet. Also known as Bashlite, Gafgyt is a Linux-based botnet that targets vulnerable IoT devices which is then used to launch large-scale DDoS attacks and download next-stage payloads to infected machines. The shell script and Gafgyt can deploy various next-stage Simps payloads for several Linux-based architectures, using the Wget utility. Wget is a legitimate software package for retrieving files from web servers using HTTP, HTTPS, FTP and FTPSa. Once the Simps executes, it drops a log file that records the fact that the target device is infected, and connects to the command-and-control server (C2).

Read more:
[https://threatpost[.]com/keksec-simps-botnet-gaming-ddos/166306/]

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 unsecured 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.
- Avoid installing unknown or unverified applications, especially from third-party distribution platforms.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - Android Security Bulletin May 2021
- 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.*