CERT-PH Cybersecurity Threat Feeds

Issue Date	April 27, 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:

- US Warns of Russian State Hackers Still Targeting US and Foreign Organizations
- Apple Fixes macOS Zero-day Bug Exploited by Shlayer Malware
- Flubot Spyware Spreading Through Android Devices
- Nvidia Warns: Severe Security Bugs in GPU Driver, vGPU Software

- CRITICAL
- URGENT
- INFORMATION

Description

US Warns of Russian State Hackers Still Targeting US and Foreign Organizations

2021.04.26 | Source(s): Bleeping Computer

Analysis:

The FBI, the US Department of Homeland Security (DHS), and the Cybersecurity and Infrastructure Security Agency (CISA) warned of continued attacks coordinated by the Russian Foreign Intelligence Service (SVR) against US and foreign organizations. Also known as APT29, the group primarily targets government networks, think tank and policy analysis organizations, information technology companies and seeks to gather intelligence information. Among Tactics, Techniques, and Procedures (TTP) associated with the SVR actors are password spraying, leveraging zero-day vulnerabilities and tradecraft similarities of SolarWinds-enabled Intrusions. In addition, threat actors are also employing a malware, dubbed as WELLMESS, that targets an organization's vaccine research repository and active directory servers.

Read more:

[https://www.bleepingcomputer[.]com/news/security/us-warns-of-russian-state-hackers-still-targeting-us-foreign-orgs/]

Apple Fixes macOS Zero-day Bug Exploited by Shlayer Malware

2021.04.26 | Source(s): Bleeping Computer

Analysis:

Apple has fixed a zero-day vulnerability in macOS that is being exploited in the wild by Shlayer malware to bypass Apple's File Quarantine, Gatekeeper, and Notarization security checks and download second-stage malicious payloads. Tracked as CVE-2021-30657, the zero-day vulnerability takes advantage of a logic flaw in the way Gatekeeper checked if app bundles were notarized to run on fully-patched macOS systems. The flaw can result in the misclassification of certain applications, and thus would cause the policy engine to skip essential security logic such as alerting the user and blocking the untrusted application. In addition, another WebKit Storage zero-day bug exploited in the wild is impacting iOS and watchOS devices by improving memory management. Tracked as CVE-2021-30661, The vulnerability allows attackers to execute arbitrary code after tricking targets into opening a maliciously crafted website on their devices.

Read more:

[https://www.bleepingcomputer[.]com/news/security/apple-fixes-macos-zero-day-bug-exploited-by-shlayer-malware/]

Flubot Spyware Spreading Through Android Devices

2021.04.26 | Source(s): Threatpost

Analysis:

A malware campaign is spreading rapidly through 'missed package delivery' SMS texts, prompting urgent scam warnings from mobile carriers. These SMS-based phishing, also known as smishing, is a

technique when cybercriminals send phishing links within mobile text messages. According to security experts, the malware is delivered to targets through SMS texts and prompts them to install a "missed package delivery" app. Instead, it takes victims to a scam website where they download the "app" which is actually a spyware. Dubbed as Flubot, the malware once installed and gained permissions, is capable of stealing banking information and credentials, lifting passwords stored on the device and squirreling away various pieces of personal information. It also sends out additional text messages to the infected device's contact list, which allows it to "go viral" like the flu hence the name.

Read more:
[https://threatpost[.]com/flubot-spyware-android-devices/165607/]

Nvidia Warns: Severe Security Bugs in GPU Driver, vGPU Software

2021.04.26 | Source(s): Threatpost

Analysis:

Nvidia disclosed a group of security vulnerabilities, including five flaws in the Nvidia graphics processing unit (GPU) display driver and eight flaws in the Nvidia virtualized GPU, which exposed users to privilege-escalation attacks, arbitrary code execution, denial of service (DoS) and information disclosure. The most severe among the five bugs in the GPU display driver, tracked as CVE-2021-1074, exists in the display driver's installer that could allow an attacker with local system access to replace an application resource with malicious files. Successful attacks may lead to code execution, escalation of privileges, denial of service, or information disclosure. Another is a high-severity bug tracked as CVE-2021-1075, all versions of NVIDIA Windows GPU Display Driver for Windows, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape where the program dereferences a pointer that contains a location for memory that is no longer valid. Successful exploitation could lead to code execution, denial of service, or escalation of privileges. Additionally, Four of the eight flaws found in NVIDIA's vGPU software are high-severity input-validation bugs that can lead to information disclosure, data tampering or DoS.

Read more:
[https://threatpost[.]com/nvidia-security-bugs-gpu-vgpu/165597/]

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.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **macOS Big Sur** - version 11.3
  - **iOS** - version 14.5
  - **iPadOS -** version 14.5
  - **NVIDIA GPU Display Driver** - latest version
  - **NVIDIA vGPU Software** - latest version
- 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.*