CERT-PH Cybersecurity Threat Feeds

Issue Date	March 19, 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:

- New XcodeSpy Malware Targets iOS Devs in Supply-chain Attack
- Chinese Nation State Hackers Linked to Finnish Parliament Hack
- Expert found a 1-Click RCE in the TikTok App for Android
- New CopperStealer Malware Steals Google, Apple, Facebook Accounts

- CRITICAL
- URGENT
- INFORMATION

Description

New XcodeSpy Malware Targets iOS Devs in Supply-chain Attack

2021.03.18 | Source(s): Bleeping Computer, Security Affairs, Threatpost

Analysis:

Cybersecurity experts identified a malicious Xcode project that is targeting iOS devs in a supply-chain attack to install a macOS backdoor on the developer's computer. Dubbed as XcodeSpy, threat actors cloned the legitimate iOS TabBarInteraction Xcode project and added an obfuscated malicious 'Run Script' script to the project. Xcode will automatically execute the Run Script to open a remote shell back to the threat actor's server. The script contacts the attackers' C2 and drops a custom variant of the EggShell backdoor on the development machine. Furthermore, researchers discovered the EggShell backdoor allows them to upload files, download files, execute commands, and snoop on a victim's microphone, camera, and keyboard activity.

Read more:

[https://www.bleepingcomputer[.]com/news/security/new-xcodespy-malware-targets-ios-devs-in-supply-chain-attack/]
[https://securityaffairs[.]co/wordpress/115729/malware/xcodespy-mac-malware.html]
[https://threatpost[.]com/xcode-macos-malware-apple-developers/164897/]

Chinese Nation State Hackers Linked to Finnish Parliament Hack

2021.03.18 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Dubbed as APT31, also known as Zirconium and Judgement Panda, a China-linked cyber espionage group was believed to be behind an attack on the Parliament of Finland that took place in 2020. According to the authorities, some parliament email accounts may have been compromised as a result of the attack, among them email accounts that belong to MPs. APT31 is a China-backed hacking group known for its involvement in numerous information theft and espionage operations, working at the behest of the Chinese Government.

Read more:

[https://www.bleepingcomputer[.]com/news/security/chinese-nation-state-hackers-linked-to-finnish-parliament-hack/]
[https://securityaffairs[.]co/wordpress/115723/apt/apt31-attack-parliament-finland.html]

Expert found a 1-Click RCE in the TikTok App for Android

2021.03.18 | Source(s): Security Affairs

Analysis:

security researcher Sayed Abdelhafiz discovered multiple vulnerabilities in the TikTok Android Application that can be chained to achieve remote code execution. The list of vulnerabilities discovered includes an Universal XSS on TikTok WebView, another XSS on AddWikiActivity, Start Arbitrary Components, Zip Slip in TmaTestActivity and Remote Code Execution. TikTok quickly responded to the issues such as addressing the vulnerable XSS code, deleted the TmaTestActivity,

and implemented restrictions to the intent scheme that doesn't allow an intent for TikTok Application on AddWikiActivity and Main WebViewActivity.
Read more:
[https://securityaffairs[.]co/wordpress/115714/hacking/rce-tiktok-android-app.html]

New CopperStealer Malware Steals Google, Apple, Facebook Accounts

2021.03.18 | Source(s): Bleeping Computer

Analysis:

Dubbed as CopperStealer, the malware is an actively developed password and cookie stealer with a downloader feature that enables its operators to deliver additional malicious payloads to infected devices. It works by harvesting passwords saved in the Google Chrome, Edge, Firefox, Yandex, and Opera web browsers. It will also retrieve the victims' Facebook User Access Token using stolen cookies to collect additional context, including their list of friends, advertisement accounts info, and a list of Facebook pages they can access. According to security experts, CopperStealer is being distributed via fake software crack sites and known malware distribution platforms such as including keygenninja[.]com, piratewares[.]com, startcrack[.]com, and crackheap[.]net.
Read more:
[https://www.bleepingcomputer[.]com/news/security/new-copperstealer-malware-steals-google-apple-facebook-accounts/]

CERT-PH Recommendations:

- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **TikTok** - 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.*