CERT-PH Cybersecurity Threat Feeds

Issue Date	February 22, 2021
TLP: GREEN	

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:

- Brave Browser Exposes Tor addresses to user's DNS provider
- Recently Fixed Windows Zero-day Actively Exploited Since Mid-2020
- Google Alerts Abused To Push Fake Adobe Flash Updater
- Agora SDK Bug Left Several Video Calling Apps Vulnerable to Snooping

- CRITICAL
- URGENT
- INFORMATION

Description

Brave Browser Exposes Tor Addresses to User's DNS provider

2021.02.17 | Source(s): Security Affairs, ZDNet, Hacker News

Analysis:

Brave has fixed a flaw in its browser that sent queries for '.onion' domains to public internet DNS resolvers rather than routing them through Tor nodes, which exposes users' visits to dark web websites. A privacy bug in the Brave Browser may cause leakage of the Tor onion URL addresses visited in the Tor mode by the users. The Tor mode implemented in the Brave web browser allows users to access .onion sites inside Brave private browsing windows. When users are inside a Private Window with Tor, Brave doesn't connect directly to a website, instead, it connects to a chain of three different computers in the Tor network. The bug is addressed in The Brave Nightly version and it will be released to the stable version with the next Brave browser update.

Read more:

[https://securityaffairs[.]co/wordpress/114793/deep-web/privacy-bug-brave-browser.html]
[https://www.zdnet[.]com/article/brave-browser-leaks-onion-addresses-in-dns-traffic/]
[https://thehackernews[.]com/2021/02/privacy-bug-in-brave-browser-exposes.html]

Recently Fixed Windows Zero-day Actively Exploited Since Mid-2020

2021.02.20 | Source(s): Bleeping Computer

Analysis:

A recently patched high-severity Windows zero-day vulnerability is actively being exploited in the wild. Tracked as CVE-2021-1732, is a Windows Win32k Elevation of Privilege vulnerability that allows a local attacker to elevate their privileges to the admin level by triggering a use-after-free condition in the win32k.sys core kernel component. The flaw can be exploited by attackers with basic user privileges in low complexity attacks that don't require user interaction.

Read more:

[https://www.bleepingcomputer[.]com/news/security/recently-fixed-windows-zero-day-actively-exploited-since-mid-2020/]

Google Alerts Abused to Push Fake Adobe Flash Updater

2021.02.21 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Cybersecurity researchers discovered that threat actors are using Google Alerts to promote a fake Adobe Flash Player updater that installs other unwanted programs on unsuspecting users' computers. If a user clicks on the Update button, they will download a setup.msi file that installs a potentially unwanted program called 'One Updater.' Over time, One Updater will display updates that should be installed and offer potentially unwanted programs. Using this program, similar software in the past has installed password-stealing Trojans and cryptocurrency miners.

Read more:

[https://www.bleepingcomputer[.]com/news/security/warning-google-alerts-abused-to-push-fake-adobe-flash-updater/]
[https://securityaffairs[.]co/wordpress/114871/cyber-crime/google-alerts-abuse.html]

Agora SDK Bug Left Several Video Calling Apps Vulnerable to Snooping

2021.02.15 | Source(s): Security Affairs

Analysis:

A severe security vulnerability in Agora, a popular video calling software development kit (SDK), could have allowed an attacker to spy on ongoing private video and audio calls. Tracked as CVE-2020-25605, is the consequence of incomplete encryption, that could be leveraged by bad actors to launch man-in-the-middle attacks and intercept communications between two parties. The flaw in Agora.io's SDK is used by several social apps such as eHarmony, Plenty of Fish, MeetMe, and Skout; healthcare apps like Talkspace, Practo, and Dr. First's Backline; and in the Android app that's paired with "temi" personal robot.

Read more:

[https://thehackernews[.]com/2021/02/agora-sdk-bug-left-several-video.html]

CERT-PH Recommendations:

o Avoid installing unknown or unverified applications, especially from third-party distribution platforms and pop-ups/alerts. Scrutinize the application’s permissions before installation and avoid allowing apps to view unnecessary information and other application’s data.

o Update any vulnerable system/applications/devices to their latest and patched versions:

- **Windows** - February 2021 security patch
- **Brave Browser** - version 1.20.108

o 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.*