CERT-PH Cybersecurity Threat Feeds

Issue Date	February 17, 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:

- Hackers Abusing the Ngrok Platform Phishing Attacks
- A Sticker Sent on Telegram Could Have Exposed Your Secret Chats
- Vendor Ships Unofficial Patch for IE Zero-Day Vulnerability
- 12-Year-Old vulnerability in Windows Defender risked 1 billion devices

- CRITICAL
- URGENT
- INFORMATION

Description

Hackers Abusing the Ngrok Platform Phishing Attacks

2021.02.16 | Source(s): Security Affairs

Analysis:

Researchers discovered a new wave of phishing attacks targeting multiple organizations that are abusing the ngrok platform, a secure and introspectable tunnel to the localhost. Ngrok is a cross-platform application used to expose a local development server to the Internet, the server appears to be hosted on a subdomain of ngrok by creating a long-lived TCP tunnel to the localhost. Experts pointed out that ngrok server software runs on a VPS or a dedicated server and can bypass NAT mapping and Firewall restriction. Multiple malware strains and phishing campaigns were discovered including: Njrat, DarkComet, Quasar RAT, asynrat and Nanocore RAT.

Read more:

[https://securityaffairs[.]co/wordpress/114644/cyber-crime/ngrok-phishing-attacks.html]

A Sticker Sent on Telegram Could Have Exposed Your Secret Chats

2021.02.15 | Source(s): The Hacker News

Analysis:

Security researchers revealed details of a now-patched vulnerability in the Telegram app that could expose users' private messages, photos, and videos to remote malicious actors. The issues were discovered in iOS, Android, and macOS versions of the app. The flaws originated from the method secret chat functionality runs and in the app's handling of animated stickers, allowing attackers to send malformed stickers to users and gain access to messages, photos, and videos that were exchanged with their Telegram contacts through both classic and secret chats. Researchers warned that the flaws could have been used in an attack to gain access to the devices of political opponents, journalists, or dissidents.

Read more:

https://thehackernews[.]com/2021/02/a-sticker-sent-on-telegram-could-have.html

Vendor Ships Unofficial Patch for IE Zero-Day Vulnerability

2021.02.15 | Source(s): Security Week

Analysis:

Security researcuers released a micro-patch for a zero-day flaw in Microsoft Internet Explorer that hacker groups in North Korea exploited in a campaign. North Korean hackers were reported to have been exploited the flaw to target cybersecurity researchers with malicious MHTML files leading to drive-by downloads of malicious payloads. Microsoft was informed of the issue but did not patch the flaw in last week's security updates. The flaw allows an attacker to execute code in Internet Explorer when they visit a malicious website and does not require any additional user interaction.

Read more:

https://www.securityweek[.]com/vendor-ships-unofficial-patch-ie-zero-day-vulnerability

12-Year-Old vulnerability in Windows Defender risked 1 billion devices

2021.02.15 | Source(s): Hack Read

Analysis:

A critical vulnerability was detected in Windows Defender, an anti-malware component of Microsoft Windows that comes pre-installed with every Windows copy. This vulnerability could let threat actors execute sophisticated attacks by enabling malicious escalation of privileges. Windows Defender has a redemption process used by its driver named "BTR.sys." This driver is responsible for deleting file system and registry resources created by malicious software from kernel mode. For this purpose, the driver keeps a log of all the operations done by a specific file by creating a handle. The issue is related to the method of the handle creation. According to researchers, the process does not verify if the file is actually a link, and therefore allows an attacker to potentially overwrite arbitrary files.

Read more:

https://www.hackread[.]com/12-year-old-vulnerability-in-windows-defender/

CERT-PH Recommendations:

- **o** Update any vulnerable system/applications/devices to their latest and patched versions:
  - **- Telegram**
  - **- Windows Device**
- **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.*