CERT-PH Cybersecurity Threat Feeds

Issue Date	April 08, 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:

• Android malware infects wannabe Netflix thieves via WhatsApp • Google Forms and Telegram Abused To Collect Phished Credentials • New Cring Ransomware Hits Unpatched Fortinet VPN Devices • Cisco Fixes Bug Allowing Remote Code Execution With Root Privileges	• CRITICAL • URGENT • INFORMATION

Description

Android malware infects wannabe Netflix thieves via WhatsApp

2021.04.07 | Source(s): Bleeping Computer, Threatpost

Analysis:

Researchers discovered a new Android malware in Google's Play Store disguised as a Netflix tool designed to automatically spread to other devices using WhatsApp auto-replies to incoming messages. Dubbed as FlixOnline, the malware tries to lure potential victims with promises of free access to Netflix content. Once installed, the malware starts a service that requests overlay, battery optimization ignore and notification permissions. According to researchers, FlixOnline will start monitoring for new WhatsApp notifications to auto-reply to all incoming messages using custom text payloads received from the command-and-control server maliciously crafted by its operators. This malware is capable of spreading further via malicious links, stealing data from user's WhatsApp accounts, spreading fake or malicious messages to users' WhatsApp contacts and groups and extorting users by threatening to send sensitive WhatsApp data or conversations to all of their contacts.

Read more:

[https://www.bleepingcomputer[.]com/news/security/android-malware-infects-wannabe-netflix-thieves-via-whatsapp/]
[https://threatpost[.]com/netflix-app-google-play-malware-whatsapp/165288/]

Google Forms and Telegram Abused To Collect Phished Credentials

2021.04.07 | Source(s): Security Affairs, Bleeping Computer

Analysis:

Cybersecurity experts observed that threat actors increasingly often use legitimate services such as Google Forms and Telegram to obtain user data stolen on phishing websites. Ready-to-go platforms that automate phishing and which are available on the darknet also have Telegram bots at their core, with an admin panel that is used to manage the entire process of the phishing attack and keep financial records linked to them. Such platforms are distributed under the cybercrime-as-a-service model, which subsequently leads to more groups conducting attacks. According to security researchers, they identified phishing kits targeting over 260 unique brands, that help create and operate phishing web pages that mimic a specific company or even several at once. To obtain data of deceived users, cybercriminals mainly resort to free email services to which all the info harvested on phishing websites is automatically sent.

Read more:

[https://www.bleepingcomputer[.]com/news/security/cisco-fixes-bug-allowing-remote-code-execution-with-root-privileges/]

New Cring Ransomware Hits Unpatched Fortinet VPN Devices

2021.04.06 | Source(s): Threatpost

Analysis:

Threat actors are actively exploiting a flaw in Fortinet VPN to deploy a new piece of ransomware, dubbed as Cring ransomware. Tracked as CVE-2018-13379, the flaw is a path traversal vulnerability in FortiOS SSL VPN web portal that could be exploited by an authenticated attacker to download FortiOS system files through specially crafted HTTP resource requests. Also known as Crypt3r, Vjiszy1lo, Ghost and Phantom, the ransomware encrypts data from victims with AES-256 + RSA-8192 and then demands a ~ 2 BTC ransom to get the files back. Once access to a system is granted, attackers download the Mimikatz utility to steal the credentials of Windows users who logged in to the compromised system.

Read more:
[https://threatpost[.]com/critical-cloud-bug-vmware-carbon-black/165278/]

Cisco Fixes Bug Allowing Remote Code Execution With Root Privileges

2021.04.07 | Source(s): Bleeping Computer

Analysis:

Cisco has released security updates to address a critical pre-authentication remote code execution (RCE) vulnerability affecting SD-WAN vManage Software's remote management component. Tracked as CVE-2021-1479, receives a severity score of 9.8 out of 10 and allows unauthenticated, remote attackers to trigger a buffer overflow on vulnerable devices in low complexity attacks that don't require user interaction. In addition, two more high-severity security vulnerabilities in the user management and system file transfer were addressed, tracked as CVE-2021-1137 and CVE-2021-1480 respectively. Successful exploitation of these flaws could allow threat actors targeting them to obtain root privileges on the underlying operating system.

Read more:
[https://www.bleepingcomputer[.]com/news/security/cisco-fixes-bug-allowing-remote-code-execution-with-root-privileges/]

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.
- Android users are urged to check their devices and immediately uninstall and remove the following applications:
  - **FlixOnline**
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Fortinet VPN** - latest version
  - **Cisco SD-WAN vManage** - versions 20.4.1, 20.3.3 and 19.2.4
- 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.*