CERT-PH Cybersecurity Threat Feeds

Issue Date	March 04, 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:

- Google Fixes Critical Remote Code Execution Issue in Android System
- Cash App Phishing Kit Deployed in The Wild, Courtesy Of 16Shop
- The Ursnif Trojan Has Hit Over 100 Italian Banks
- GRUB2 Boot Loader Reveals Multiple High Severity Vulnerabilities

- CRITICAL
- URGENT
- INFORMATION

Description

Google Fixes Critical Remote Code Execution Issue in Android System

2021.03.02 | Source(s): Security Affairs

Analysis:

Google released security updates to address 37 vulnerabilities as part of the Android security updates for March 2021. One of the most severe vulnerabilities, tracked as CVE-2021-0397, is a remote code vulnerability that exists in the system component and affects Android 8.1, 9, 10 and 11 releases. Successful exploitation of the vulnerability, could enable a remote attacker using a specially crafted transmission to execute arbitrary code within the context of a privileged process.

Read more:

[https://securityaffairs[.]co/wordpress/115189/mobile-2/google-android-rce-2.html]

Cash App Phishing Kit Deployed in The Wild, Courtesy Of 16Shop

2021.03.03 | Source(s): Bleeping Computer

Analysis:

The developer of the 16Shop phishing platform added a new component that targets users of the popular Cash App mobile payment service. Deployment of the new 16Shop product started as soon as it became available, luring potential victims into providing sensitive details that would give fraudsters access to the account and the associated payment information. According to cybersecurity experts, the kit has the same base code as the others, and the template mimics the legitimate Cash App site and login workflow as closely as possible. Getting victims to the phishing page is done through emails and SMS messages that alert on a security issue that led to locking the Cash App account. Clicking on the fraudulent link triggers a series of checks before loading the phishing page. The visitor's IP address, their user agent, and ISP details are collected and processed to determine an association with an automated action (security checks, web crawlers) or a potential victim.

Read more:

[https://www.bleepingcomputer[.]com/news/security/cash-app-phishing-kit-deployed-in-the-wild-courtesy-of-16shop/]

The Ursnif Trojan Has Hit Over 100 Italian Banks

2021.03.03 | Source(s): Security Affairs, ZDNet

Analysis:

Experts recently obtained information on possible victims of Ursnif malware that confirms the interest of malware operators in targeting Italian banks. According to data obtained by cybersecurity experts, at least 100 Italian banks have been targeted with the Ursnif Trojan and in one case, crooks stole over 1,700 sets of credentials from an unnamed payment processor. Ursnif is one of the most and widespread common threats today delivered through malspam campaigns. Ursnif is usually spread via phishing emails, such as invoice requests, and attempts to steal financial data and account credentials.

Read more:

[https://securityaffairs[.]co/wordpress/115245/cyber-crime/ursnif-targets-italian-banks.html]
[https://www.zdnet[.]com/article/ursnif-trojan-has-targeted-over-100-italian-banks/]

GRUB2 Boot Loader Reveals Multiple High Severity Vulnerabilities

2021.03.03 | Source(s): Bleeping Computer

Analysis:

GRUB project maintainers have released hundreds of upstream patches for severe boot loader flaws. Previously, cybersecurity experts discovered a BootHole vulnerability in GRUB2 that could have let attackers compromise an operating system's booting process even if the Secure Boot verification mechanism was active. Threat actors could further abuse the flaw to hide arbitrary code ("bootkit") within the OS that would run on every boot. A total of 117 upstream code patches have been issued to resolve these CVEs, detailed instructions with regards to mitigation and obtaining updates would be provided by OS vendors. GRUB is a popular boot loader used by Unix-based operating systems has fixed multiple high severity vulnerabilities.

Read more:

[https://www.bleepingcomputer[.]com/news/security/grub2-boot-loader-reveals-multiple-high-severity-vulnerabilities/]

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:
  - **Android System** - March 2021 Security Updates
- 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.*