CERT-PH Cybersecurity Threat Feeds

Issue Date	January 06, 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:

● New Credential Stealer Written in AutoHotkey Scripting Language ● Beware: PayPal Phishing Texts State Your Account Is 'limited' ● Google Releases January 2021 Security Updates for Android ● Alleged MuddyWater Attack Downloads a Powershell Script from GitHub	● CRITICAL ● URGENT ● INFORMATION

Description

New Credential Stealer Written in AutoHotkey Scripting Language

2020.12.29 | Source(s): The Hacker News

Analysis:

Financial institutions are under threat from a new credential stealer that targets various browsers, such as Chrome, Opera and Microsoft Edge, using a AutoHotkey-based password stealer. Once installed, the stealer attempts to download an SQLite module ("sqlite3.dll") on the infected machine, using it to perform SQL queries against the SQLite databases within browsers' app folders. Finally, the stealer then collects and decrypts credentials from browsers and exfiltrates the information to the C&C server in plaintext via an HTTP POST request.

Read more:
[https://thehackernews.com/2020/12/autohotkey-based-password-stealer.html]

Beware: PayPal Phishing Texts State Your Account Is 'limited'

2021.01.03 | Source(s): Bleeping Computer

Analysis:

A new SMS text phishing campaign pretends to be from PayPal, stating that your account has been permanently limited unless you verify your account by clicking on a link. Clicking on the enclosed link will bring you to a phishing page that prompts you to log in to your account. The collected information is used to conduct identity theft attacks, gain access to other accounts, or perform targeted spear-phishing attacks.

Read more:
[https://www.bleepingcomputer.com/news/security/beware-paypal-phishing-texts-state-your-account-is-limited/?&web_view=true]

Google Releases January 2021 Security Updates for Android

2021.01.05 | Source(s): Security Week

Analysis:

With the release of security patch 2021-01-01, Google addressed 42 vulnerabilities, including four rated critical severity. One of the most severe flaws addressed, tracked as CVE-2021-0316, could be exploited to achieve code execution remotely. An attacker looking to exploit the vulnerability would need to use a specially crafted transmission. Successful exploitation could lead to the execution of code within the context of a privileged process.

Read more:
[https://www.securityweek.com/google-releases-january-2021-security-updates-android?&web_view=true]

Alleged MuddyWater Attack Downloads a Powershell Script from GitHub

2021.01.04 | Source(s): Security Affairs

Analysis:

Cybersecurity experts discovered a new piece of malware that uses weaponized Word documents to download a PowerShell script from GitHub. The PowerShell is composed of a single line that downloads a PNG file from the image hosting service Imgur. The PowerShell script analyzes a set of pixel values of the image to prepare the next stage payload. Once decoded, the script reveals a Cobalt Strike payload that allows attackers to deploy “beacons” on compromised Windows machines.

Read more:
[https://securityaffairs.co/wordpress/112972/hacking/muddywater-attack-github-imgur.html]

CERT-PH Recommendations:

o Update any vulnerable system/applications/devices to their latest and patched versions:
- Android Devices - January Security Update

o PayPal users who received the Smishing message and mistakenly logged in to their PayPal account using the link provided, immediately go to Paypal.com and change their password.

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.