CERT-PH Cybersecurity Threat Feeds

Issue Date	February 19, 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:

- WebKit Zero-day Abused to Redirect Online Gift Cards
- New Masslogger Trojan Variant Exfiltrates User Credentials
- SonicWall Releases Second Firmware Updates For SMA-100 Vulnerability
- Cashalo Reports Data Breach

- CRITICAL
- URGENT
- INFORMATION

Description

WebKit Zero-day Abused to Redirect Online Gift Cards

2021.02.17 | Source(s): Security Affairs

Analysis:

Dubbed as ScamClub, the malvertising gang is recently observed to be abusing an unpatched zero-day vulnerability in WebKit-based browsers to bypass security measures and redirect users from legitimate sites to websites hosting online gift card scams. The gang mainly targets iOS users with malicious ads that often redirected users to sites hosting online scams. The landing pages were designed to trick victims into providing their financial information. The trick abused by the threat actors in these malvertising campaigns only worked with browsers using the open-source WebKit engine, such as Apple's Safari and Google Chrome for iOS.

Read more:

[https://securityaffairs[.]co/wordpress/114689/cyber-crime/scamclub-malvertising-webkit-zero-day.html]

New Masslogger Trojan Variant Exfiltrates User Credentials

2021.02.19 | Source(s): Security Affairs

Analysis:

Dubbed as MassLogger, the infamous Windows credential stealer is back and has been upgraded to steal additional credentials from Outlook, Chrome, and instant messaging applications. Unlike previous Masslogger trojan samples previously documented and analyzed, the new variant uses Microsoft Compiled HTML Help file format, which is a Microsoft proprietary online help format, to start the infection chain. The Microsoft file format can also contain active script components, in this case JavaScript, which is used to launch the malware in the attacks. The infection chain starts with an email message containing a legitimate-looking subject line and comes with a RAR attachment with a slightly unusual filename extension. Upon opening the attachments, the message "Customer service" is displayed while an obfuscated JavaScript code creates an HTML page, which in turn contains a PowerShell downloader that fetches from a legitimate server the loader used to launch the MassLogger payload. The malware is able to exfiltrate stolen data via SMTP, FTP or HTTP.

Read more:

[https://securityaffairs[.]co/wordpress/114783/malware/masslogger-trojan.html]

SonicWall Releases Second Firmware Updates For SMA-100 Vulnerability

2021.02.20 | Source(s): Security Affairs

Analysis:

Security provider SonicWall released a new firmware update for an SMA-100 zero-day vulnerability that was exploited in attacks. Tracked as CVE-2021-20016, is a vulnerability that results in improper SQL command neutralization in the SonicWall SSLVPN SMA100 product, it could be exploited by a remote, unauthenticated attacker for credential access on SMA100 build version 10.x. The flaw is rated as critical and received a CVSS score of 9.8

Read more:

[https://securityaffairs[.]co/wordpress/114818/security/sonicwall-firmware-updates-sma-100.html]

Cashalo Reports Data Breach

2021.02.20 | Source(s): CNN Philippines, NewsBytes

Analysis:

The online lending platform Cashalo has reported an unauthorized access to its database that contained some personal data of its customers, but assured that accounts or passwords were not compromised. Cashalo, a fintech company, discovered a potential data security incident involving a Cashalo database archive and was being sold on a dark web forum. This incident resulted in the unauthorized access to a database archive that contained some personal data of Cashalo customers, including some combination of usernames, email, phone numbers, device ID, and encrypted passwords. However, according to the company no customer accounts or passwords were compromised.

Read more:

https://www.cnnphilippines[.]com/news/2021/2/20/cashalo-data-breach.html
https://newsbytes[.]ph/2021/02/20/cashalo-confirms-data-breach-incident-says-it-is-working-with-npc/

CERT-PH Recommendations:

o 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.

o Users are advised to conduct continuous background memory scans and to configure their systems for logging PowerShell events such as module loading and executed script blocks as they will show executed code in its deobfuscated format.

o Cashalo users are strongly advised to change their Cashalo account's password and other online accounts that uses the same set of credentials to avoid other cyber attacks.

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

- SonicWall firmware - version 10.2 and later

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.*