CERT-PH Cybersecurity Threat Feeds

Issue Date	February 09, 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 Phishing Attack Uses Morse Code to Hide Malicious URLs
- Android App Joins the Dark Side, Sends Malware Update to Millions
- Critical Vulnerability Fixed in WordPress Plugin With 800K Installs
- The Great Suspender Chrome Extension's Fall from Grace

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

New Phishing Attack Uses Morse Code to Hide Malicious URLs

2021.02.07 | Source(s): Bleeping Computer, Security Affairs

Analysis:

A new targeted phishing campaign includes the novel obfuscation technique of using Morse code to hide malicious URLs in an email attachment. The phishing attack starts with an email pretending to be an invoice for the company with a mail subject like 'Revenue_payment_invoice February_Wednesday 02/03/2021.' This email includes an HTML attachment named in such a way as to appear to be an Excel invoice for the company. These attachments are named in the format '[company_name]_invoice_[number]._xlsx.hTML.' When viewing the attachment in a text editor,it is visible that the threat actors included a JavaScript that maps letters and numbers to Morse code. The script then calls a decodeMorse() function to decode a Morse code string into a hexadecimal string. This hexadecimal string is further decoded into JavaScript tags that are injected into the HTML page. These injected scripts combined with the HTML attachment contain the various resources necessary to render a fake Excel spreadsheet that states their sign-in timed out and prompts them to enter their password again. From there, the attackers can then collect the victim's login credentials.

Read more:

[https://www.bleepingcomputer[.]com/news/security/new-phishing-attack-uses-morse-code-to-hide-malicious-urls/]
[https://securityaffairs[.]co/wordpress/114346/cyber-crime/hishing-technique-morse-code.html]

Malicious Extension Abuses Chrome Sync to Steal Users' Data

2021.02.08 | Source(s): Bleeping Computer, ZDNet

Analysis:

Google has removed a popular Android barcode scanner app, named as Barcode Scanner and developed by LAVABIRD, with over 10 million installs from the Play Store after researchers found that it turned malicious following a December 2020 update. Security researchers categorize the app as a Trojan after the detection of 'Android/Trojan.HiddenAds.AdQR'. The malicious behavior experienced by its millions of users included seeing their default browser launching without any user interaction and displaying ads that promoted other, potentially malicious, Android apps.

Read more:

[https://www.bleepingcomputer[.]com/news/security/android-app-joins-the-dark-side-sends-malware-update-to-millions/]
[https://www.zdnet[.]com/article/with-one-update-this-malicious-android-app-hijacked-10-million-devices/]

Critical Vulnerability Fixed in WordPress Plugin With 800K Installs

2021.02.08 | Source(s): Bleeping Computer

Analysis:

Security researchers addressed two severe Cross-Site Request Forgery vulnerabilities to protect sites from potential takeover attacks. One of the severe CSRF vulnerabilities, tracked as CVE-2020-35942, can lead to Reflected Cross-Site Scripting (XSS) and remote code execution (RCE) attacks via file upload or Local File

Inclusion (LFI). Attackers can exploit these security flaws by tricking WordPress admins into clicking specially crafted links or attachments to execute malicious code in their browsers. After successful exploitation, the vulnerabilities can let hackers set up malicious redirects, inject spam, abuse compromised sites for phishing, and, ultimately, take over the sites completely.

Read more:
[https://www.bleepingcomputer[.]com/news/security/critical-vulnerability-fixed-in-wordpress-plugin-with-800k-installs/]

Mozilla fixes Windows 10 NTFS Corruption Bug in Firefox

2021.02.06 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Google removed the popular The Great Suspender from the official Chrome Web Store for containing malware and deactivated it from the users' PC. The Great Suspender is a Chrome extension that will suspend unused tabs and unload its resources to decrease the browser's memory usage. When a user is ready to use the tab again, they simply have to click it on to make it visible. Security experts discovered that a new maintainer of the extensions has secretly added a feature that could be exploited to remotely execute arbitrary code. The malicious code could be exploited to carry out malicious activities, such as committing advertising fraud.

Read more:
[https://www.bleepingcomputer[.]com/news/software/the-great-suspender-chrome-extensions-fall-from-grace/]
[https://securityaffairs[.]co/wordpress/114272/malware/the-great-suspender-extension-malware.html]

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 As a safety precaution, Android users are advised to uninstall LAVABIRD's Barcode Scanner.
o Users are urged to check their browser extensions and immediately remove the Great Suspender Chrome extension
o Update any vulnerable system/applications/devices to their latest and patched versions:
  - NextGen Gallery - version 3.5.0
o To block attackers abusing Google Chrome's Sync API for harvesting and exfiltrating data from corporate environments, group policies are urged to create a list of approved CHrome extensions and block all others who haven't been checked for red flags.**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.*