CERT-PH Cybersecurity Threat Feeds

Issue Date	February 15, 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:

- Experts Spotted Two Android Spyware Used by Indian APT Confucius
- Lampion Trojan Disseminated in Portugal Using COVID-19 Template
- Buggy WordPress Plugin Exposes 100K Sites to Takeover Attacks
- PayPal Mitigates XSS Vulnerability

- CRITICAL
- URGENT
- INFORMATION

Description

Experts Spotted Two Android Spyware Used by Indian APT Confucius

2021.02.11 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Security researchers provided details about two recently discovered Android spyware families used by an APT group tracked as Confucius. Confucius is a pro-India APT group that has been active since 2013 and mainly focused on Pakistani and other South Asian targets. Dubbed as Hornbill and SunBird, the two malware used to spy on personnel linked to Pakistan's military, nuclear authorities and Indian election in Kashmir. Both malware can exfiltrate a wide range of information, including call logs, contacts, device's metadata (i.e. phone number, IMEI/Android ID, Model and Manufacturer, and Android version), geolocation, images stored on external storage and WhatsApp voice notes.

Read more:

[https://securityaffairs[.]co/wordpress/114473/malware/confucius-apt-malware.html]
[https://www.bleepingcomputer[.]com/news/security/pro-india-hackers-use-android-spyware-to-spy-on-pakistani-military/]

Lampion Trojan Disseminated in Portugal Using COVID-19 Template

2021.02.12 | Source(s): Security Affairs

Analysis:

A new release of the Latin American Lampion trojan was released in Portugal using a template related to COVID-19. This trojan has been distributed in Portugal in different ways, but this time the pandemic situation and the ongoing vaccination process is the reason behind this campaign to drop the beast in the wild. The threat is impersonating the domain "min-saude.pt" and the link to the zip file is also distributed in the email body. When the malware is executed, it communicates with the C2 server and the browser overlay process begins every time a target home banking portal is accessed on the victim side.

Read more:

[https://securityaffairs[.]co/wordpress/114496/cyber-crime/lampion-trojan-portugal-covid19.html]

Buggy WordPress Plugin Exposes 100K Sites to Takeover Attacks

2021.02.11 | Source(s): Bleeping Computer

Analysis:

Researchers discovered critical and high severity vulnerabilities in the 'Responsive Menu' WordPress plugin exposed over 100,000 sites to takeover attacks. Responsive Menu is a WordPress plugin designed to help admins create W3C compliant and mobile-ready responsible site menus. Security researchers found three vulnerabilities that can be exploited by attackers with basic user permissions to upload arbitrary files and remotely execute arbitrary code. The first flaw enables authenticated attackers to upload arbitrary files which eventually allows them to achieve remote code execution. The other two vulnerabilities allow a potential threat actor to forge requests to modify plugin settings of the plugin which, in turn, allows them to upload arbitrary files allowing for remote code execution. To abuse the critical vulnerability, attackers logged in as subscribers or another low-level user have to upload menu themes archived as ZIP files and containing malicious PHP files. After the archive is extracted for

installation, the attacker can access the files via the site frontend to remotely execute the malicious code which ultimately can lead to a full site takeover.

Read more:

[https://www.bleepingcomputer[.]com/news/security/buggy-wordpress-plugin-exposes-100k-sites-to-takeover-attacks]

PayPal Mitigates XSS Vulnerability

2021.02.12 | Source(s): ZDNet, Bank Infosecurity

Analysis:

PayPal has fixed a reflected cross-site scripting (XSS) vulnerability found in the currency converter feature of user wallets and is caused by a failure to properly sanitize user inputs. According to security researchers, a weak URL parameter failed to clean up input which could allow threat actors to inject malicious JavaScript, HTML, or any other code that the browser could execute. By loading a malicious payload into a victim's browser, hackers could potentially steal data or take control of a device.

Read more:

[https://www.zdnet[.]com/article/paypal-fixes-reflected-xss-vulnerability-in-business-wallet]
[https://www.bankinfosecurity[.]com/bounty-hunter-finds-paypal-xss-vulnerability-a-15984]

CERT-PH Recommendations:

o Avoid installing unknown or unverified applications, especially from third-party distribution platforms. Scrutinize the application's permissions before installation and avoid allowing apps to view unnecessary information and other application's data.

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

- Responsive Menu - version 4.0.4

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.*