CERT-PH Cybersecurity Threat Feeds

Issue Date	May 21, 2021
TLP: White	

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:

- Blind SQL Injection Flaw in WP Statistics Impacted Plugin
- Dozen Android Apps Exposes Users' Data
- STRRAT RAT Spreads Masquerading As Ransomware
- Fake Microsoft Authenticator Extension Discovered in Chrome Store

- CRITICAL
- URGENT
- INFORMATION

Description

Blind SQL Injection Flaw in WP Statistics Impacted Plugin

2021.05.20 | Source(s): Security Affairs, Bleeping Computer

Analysis:

Cybersecurity researchers discovered a Time-Based Blind SQL Injection vulnerability in a WordPress plugin. The WordPress plugin, WP Statistics, was developed by VeronaLabs that provides complete website statistics to site owners. The vulnerability could be exploited by an unauthenticated attacker to extract sensitive information from a WordPress website using the vulnerable plugin. The flaw has been rated with a CVSS Score of 7.5 and affects versions prior to 13.0.8. Site administrators could display detailed statistics about traffic to their site by accessing the WP Statistics "Pages" menu item that generates a SQL query in order to provide statistics. Researchers discovered that it was possible to access the WP Statistics "Pages" even without admin privileges.

Read more:

[https://securityaffairs[.]co/wordpress/118099/hacking/wordpress-wp-statistics-flaw-2.html]

Dozen Android Apps Exposes Users' Data

2021.05.20 | Source(s): Security Affairs

Analysis:

Security researchers have detected 23 Android applications that exposed personal data of more than 100 million users due to misconfigurations of third-party cloud services. The experts pointed out that the misconfiguration also exposes developer's internal resources, such as access to update mechanisms and storage, at risk. Upon accessing the backend databases of 13 apps that were found to contain sensitive information such as email addresses, passwords, personal images, private chats, location coordinates, user identifiers, social media credentials, screen recordings. In some cases, the apps analyzed exposed access keys that would have allowed attackers to send push notifications to all the users of the applications. Threat actors could abuse push notification services to conduct malicious activities, such as sending out messages containing links to malicious websites set up to deliver malware or phishing sites.

Read more:

[https://securityaffairs[.]co/wordpress/118112/mobile-2/android-apps-exposed-data.html]
[https://www.bleepingcomputer[.]com/news/security/data-of-100-plus-million-android-users-exposed-via-misconfigured-cloud-services/]

STRRAT RAT Spreads Masquerading as Ransomware

2021.05.20 | Source(s): Security Affairs

Analysis:

Microsoft Security Intelligence researchers uncovered a malware campaign that is spreading a remote access trojan (RAT). Tracked as STRRAT, the RAT was designed to steal data from victims while masquerading as a ransomware attack. The Java-based STRRAT RAT was distributed in a massive spam campaign, the malware shows ransomware-like behavior of appending the file name extension .crimson to files without actually encrypting them. According to the experts, threat actors behind the campaign used compromised email accounts to send out spam messages containing an

image that posed as a PDF attachment. Upon opening the image, the malicious code connects to a domain to download the STRRAT RAT. In addition, researchers noticed that STRRAT version 1.5 is notably more obfuscated and modular than previous versions. The malware is capable of multiple features such as collecting browser passwords, running remote commands and PowerShell, and logging keystrokes.

Read more:

[https://securityaffairs[.]co/wordpress/118118/malware/strrat-rat-masquerading-ransomware.html]

Fake Microsoft Authenticator Extension Discovered in Chrome Store

2021.05.19 | Source(s): Hot For Security

Analysis:

Cybersecurity researchers have detected a Chrome extension that claims to be a legitimate Microsoft Authenticator. Microsoft states that its Authenticator product is not available as a browser extension but as an Android and iOS smartphone application only. The Microsoft Authenticator application cannot be used to authenticate Microsoft account sign-ins or any other sign-in for the matter. It displays a basic page with the option to "run Microsoft Authenticator''. A click on the button opens a Polish webpage that redirects to another webpage automatically asking for a sign-in or the creation of an account. According to researchers, this bogus extension may have been used to collect sensitive information and credentials from victims.

Read more:

[https://hotforsecurity.bitdefender[.]com/blog/fake-microsoft-authenticator-extension-discovered-in-chrome-store-25845.html]

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 unsecured 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.
- Avoid installing unknown or unverified applications, especially from third-party distribution platforms.
- User's who have downloaded the fake Microsoft Authenticator extension should immediately remove the plugin and change the passwords for all existing online accounts.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **WP Statistics plugin** - version 13.0.8
- 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.*