CERT-PH Cybersecurity Threat Feeds

Issue Date	February 01, 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 Pro-Ocean Malware Worms Through Apache, Oracle, Redis Servers
- Oscorp, A New Android Malware Targets Italian Users
- Experts Addressed Flaws in Popup Builder WordPress Plugin
- Vovalex is likely the first ransomware written in D

- CRITICAL
- URGENT
- INFORMATION

Description

New Pro-Ocean Malware Worms Through Apache, Oracle, Redis Servers

2021.01.29 | Source(s): Bleeping Computer

Analysis:

The financially-motivated Rocke hackers are using a new piece of cryptojacking malware to target vulnerable instances of Apache ActiveMQ, Oracle WebLogic, and Redis. Rocke cryptojacking hackers have a habit of attacking cloud applications and leverage known vulnerabilities to take control of unpatched Oracle WebLogic (CVE-2017-10271) and Apache ActiveMQ (CVE-2016-3088) servers. Tracked as Pro-Ocean, uses LD_PRELOAD, a native Linux feature that forces binaries to prioritize the loading of specific libraries. The new part is that the developers took the rootkit capabilities further by implementing publicly available code that helps conceal malicious activity and spread to unpatched software on the network.

Read more:

[https://www.bleepingcomputer[.]com/news/security/microsoft-shares-how-solarwinds-hackers-evaded-detection/]
[https://securityaffairs[.]co/wordpress/113681/apt/microsoft-solorigate.html]

Oscorp, A New Android Malware Targets Italian Users

2021.01.29 | Source(s): Security Affairs

Analysis:

Security researchers warn of new Android malware that abuses accessibility services for malicious purposes. Dubbed as Oscorp, is a malware that tricks users into granting them access to the Android Accessibility Service, which means threat actors will be able to read the text on the phone screen, determine an app installation prompt, scroll through the permission list and press the install button on the behalf of the user. Experts identified a domain called “supportoapp [.] Com” that was serving the file “Client assistance.apk”. Once the app is installed, which is presented with the name “Customer Protection”, it asks users to enable the accessibility service allowing it to enable keylogger functionality, automatically obtain the permissions and capabilities required by the malware, uninstall apps, make calls, send SMS, steal cryptocurrency and steal the PIN for Google’s 2FA.

Read more:

[https://securityaffairs[.]co/wordpress/113983/malware/oscorp-android-malware.html]

Experts Addressed Flaws in Popup Builder WordPress Plugin

2021.01.29 | Source(s): Security Affairs

Analysis:

Multiple issues were addressed in WordPress ‘Popup Builder’ plugin that could be exploited by hackers to perform various malicious actions on affected websites. According to experts, the plugin flaw is caused by the lack of authorization in most AJAX methods. This would allow to send out newsletters with any content, for local file inclusion (but limited to first-line), to import or delete subscribers, and perform other activities. One of the vulnerable methods allows users to import a list of subscribers from a remote

URL, while another could be abused by an authenticated user to send out newsletters with “custom email body content, email sender, and several other attributes that will essentially allow a malicious user to send out emails to all subscribers.” The flaws could be exploited by a logged-in user with access to the nonce token.

Read more:

[https://securityaffairs[.]co/wordpress/113998/hacking/popup-builder-wordpress-plugin.html]

Vovalex is likely the first ransomware written in D

2021.01.21 | Source(s): Threatpos

Analysis:

Tracked as Vovalex, a new ransomware that is being distributed through pirated software that impersonates popular Windows utilities. All ransomware infections boil down to the same function, encrypt a device's files and then drop a ransom note demanding payment in some form. Vovalex is distributed as a warez copy of the CCleaner Windows utility and when executed, the ransomware will launch a legitimate CCleaner installer and copy itself to the random file name in the %Temp%folder. The ransomware will begin to encrypt files on the drive and append the .vovalex extension to encrypted file's names. According to security researchers, Vovalex may be the first ransomware written in D. Dlang is inspired by C++ but shares components from other languages.

Read more:

[https://www.bleepingcomputer[.]com/news/security/vovalex-is-likely-the-first-ransomware-written-in-d/]

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

- **Apache ActiveMQ** - latest version
- **Oracle WebLogic** - latest version

o Users of NetExtender VPN client and Secure Mobile Access are advised to check the advisory published by Sonicwall and apply necessary mitigation measures while waiting for the security patch

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.*