CERT-PH Cybersecurity Threat Feeds

Issue Date	February 26, 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:

- LazyScripter Hackers Target Airlines with Remote Access Trojans
- Heavily Used Node.Js Package Has a Code Injection Vulnerability
- VMware Addresses a Critical RCE Issue in vCenter Server
- APT32 State Hackers Target Human Rights Defenders with Spyware

- CRITICAL
- URGENT
- INFORMATION

Description

LazyScripter Hackers Target Airlines with Remote Access Trojans

2021.02.24 | Source(s): Bleeping Computer

Analysis:

Security researchers observed a recent activity of threat actors, dubbed as LazyScripter, that uses phishing to target individuals seeking immigration for a job, airlines and the International Air Transport Association (IATA). The recent activity involves the use of the freely available Octopus and Koadic malware. Both were delivered through malicious document and ZIP archives that contained embedded objects (VBScript or batch files) and not macro code commonly seen in phishing attacks. According to researchers, LazyScripter switched to the double-RAT tactic after initially using the PowerShell Empire post-exploitation framework. The researchers named the loaders for these payloads KOCTOPUS and Empoder, respectively. Used to deploy Octopus and Koadic and ensure their persistence on the system, KOCTOPUS is highly obfuscated using the BatchEncryption tool. The overall compromise process via KOCTOPUS involves bypassing the User Account Control (UAC) security feature in Windows, disabling Microsoft security products, and downloading RMS or LuminosityLink RAT.

Read more:
[https://www.bleepingcomputer[.]com/news/security/lazyscripter-hackers-target-airlines-with-remote-access-trojans/]

Heavily Used Node.Js Package Has a Code Injection Vulnerability

2021.02.24 | Source(s): Bleeping Computer

Analysis:

Tracked as CVE-2021-21315, is a high severity command injection vulnerability that impacts the "systeminformation" npm component which gets about 800,000 weekly downloads and has scored close to 34 million downloads to date since its inception. The "systeminformation" is a lightweight Node.js library that developers can include in their project to retrieve system information related to CPU, hardware, battery, network, services, and system processes. The presence of the code injection flaw within "systeminformation" meant an attacker could execute system commands by carefully injecting payload within the unsanitized parameters used by the component.

Read more:
[https://www.bleepingcomputer[.]com/news/security/heavily-used-nodejs-package-has-a-code-injection-vulnerability/]

Google Discloses Technical Details of Windows RCE flaw

2021.02.25 | Source(s): Security Affairs

Analysis:

Google Project Zero disclosed the details of a recently patched Windows vulnerability, tracked as CVE-2021-24093, that can be exploited for remote code execution in the context of the DirectWrite client. DirectWrite is a Windows API designed to provide support for measuring, drawing, and hit-testing of multi-format text. An attacker could exploit the flaw by tricking the victims into visiting a specially crafted site hosting a file set up to trigger the issue. The issue affects the Windows graphics component in all operating systems and received a CVSS score of 8.8.

Read more:
[https://securityaffairs[.]co/wordpress/115008/hacking/cve-2021-24093-rce-flaw-details.html]

APT32 State Hackers Target Human Rights Defenders with Spyware

2021.02.24 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Vietnam-linked APT32 (aka Ocean Lotus) group has conducted a cyberespionage campaign targeting Vietnamese human rights defenders (HRDs) and a nonprofit (NPO) human rights organization from Vietnam between February 2018 and November 2020. The attack chain begins with spear-phishing messages that include a link to an alleged important document to download. The link points to files containing spyware that could infect both Mac OS or Windows systems. The Windows spyware employed in this campaign is a variant of malware, tracked as Kerrdown, that was exclusively used by the Ocean Lotus group in the past. Kerrdown downloads and installs additional spyware from a server on the victim's system, then it opens a decoy document. The attackers used the Cobalt Strike post-exploitation toolkit to access the compromised system.

Read more:
[https://www.bleepingcomputer[.]com/news/security/apt32-state-hackers-target-human-rights-defenders-with-spyware/]
[https://securityaffairs[.]co/wordpress/114973/malware/apt32-spyware-human-rights-defenders.html]

CERT-PH Recommendations:

- Node.js developers are encouraged to ensure if their applications properly sanitize user input prior to using it within commands and database queries.
- 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.
- Update any vulnerable system/applications/devices to their latest and patched versions:

  - **Node.js -** version 5.3.1 or later
  - **Microsoft -** February 2021 Patch
- 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.*