CERT-PH Cybersecurity Threat Feeds

Issue Date	April 29, 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:

• Threat Actors Target Southeast Asian Military Organizations with New Backdoor • New Stealthy Linux Malware Used to Backdoor Systems for Years • Threat Actors Target Military Organizations with New Backdoor • Microsoft Teams Outage Impacts User Logins and Chats	● CRITICAL ● URGENT ● INFORMATION

Description

Threat Actors Target Southeast Asian Military Organizations with New Backdoor

2021.04.28 | Source(s): Bleeping Computer, Security Affairs

Analysis:

A Chinese-speaking threat actor has deployed a new backdoor in multiple cyber-espionage operations spanning roughly two years and targeting military organizations from Southeast Asia. Tracked as Naikon, the hacking group is likely a state-sponsored threat actor tied to China and is known for focusing its efforts on high-profile organizations, including government entities and military organizations in Southeast Asia. Dubbed as Nebulae, threat actors abused legitimate softwares to side-load this second-stage malware to achieve persistence. Nebulae provides additional capabilities allowing attackers to collect system information, manipulate files and folders, download files from the command-and-control server, and execute, list, or terminate processes on compromised devices. In addition, Naikon also delivered first-stage malware, known as RainyDay or FoundCore, used to deploy second-stage payloads and tools used for various purposes, including the Nebulae backdoor. Attackers can also send RainyDay commands over TCP or HTTP to manipulate services, access a command shell, uninstall the malware, take and collect screen captures, and manipulate, download, or upload files.

Read more:

[https://www.bleepingcomputer[.]com/news/security/cyberspies-target-military-organizations-with-new-nebulae-backdoor/]
[https://securityaffairs[.]co/wordpress/117321/apt/naikon-apt-nebulae-backdoor.html]

New Stealthy Linux Malware Used to Backdoor Systems for Years

2021.04.28 | Source(s): Bleeping Computer

Analysis:

Cybersecurity researchers recently discovered a Linux malware with backdoor capabilities has flown under the radar for years and is undetected by most anti-malware engines, allowing attackers to harvest and exfiltrate sensitive information from compromised devices. Dubbed as RotaJakiro, the malware is designed to operate as stealthy as possible, encrypting its communication channels using ZLIB compression and AES, XOR, ROTATE encryption. Threat actors can use RotaJakiro to exfiltrate system info and sensitive data, manage plugins and files, and execute various plugins on compromised 64-bit Linux devices.

Read more:

[https://thehackernews[.]com/2021/04/apple-airdrop-bug-could-leak-your.html]
[https://securityaffairs[.]co/wordpress/117250/hacking/apple-airdrop-bug.html]

Google Chrome V8 Bug Allows Remote Code-Execution

2021.04.28 | Source(s): Threatpost, Security Affairs

Analysis:

Google's Chrome browser rolled out the Chrome 90 stable channel release to address several security vulnerabilities that could pave the way to multiple types of attacks, including a V8 bug that could allow remote code execution (RCE) within a user's browser. Tracked as CVE-2021-21227, the high severity flaw is due to insufficient data validation in V8 and it doesn't allow attackers to escape the sandbox where Chrome runs, meaning attackers can't reach any of the other programs, data and applications on the computer. In this note, CVE-2021-21227 would need to be chained with another vulnerability in order to successfully damage and penetrate on a target's machine beyond the browser itself. In addition, two V8 vulnerabilities were also fixed. The first bug allows a remote attacker to exploit heap corruption if a user visits, or is redirected to, a specially crafted web page while the second bug is a type-confusion bug that allows a remote attacker to potentially perform out of bounds memory access, also exploitable with a specially crafted HTML page and were tracked as CVE-2020-16040 and CVE-2020-15965, respectively.

Read more:
[https://threatpost[.]com/google-chrome-v8-bug-remote-code-execution/165662/]
[https://securityaffairs[.]co/wordpress/117315/security/chrome-v8-flaw.html]

Microsoft Teams Outage Impacts User Logins and Chats

2021.04.29 | Source(s): Bleeping Computer

Analysis:

A worldwide Microsoft Teams outage is blocking users from logging into their accounts and preventing those already logged in from sending and receiving messages. According to Microsoft, the Teams outage is blocking users from sending and receiving messages, joining channels, joining chats and from seeing some channels. The outage was caused by a recent configuration change resulting in specific feature settings to include an incorrect value, resulting in impact to the service. In addition, Microsoft says all Teams features are now working as expected. Users still experiencing issues are advised to restart their clients to expedited recovery.

Read more:
[https://www.bleepingcomputer[.]com/news/microsoft/microsoft-teams-worldwide-outage-impacts-user-logins-chats/]

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 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.
- Microsoft Teams users that are still experiencing performance issues or outage are advised to restart their clients.
- Closely monitor the following application for any suspicious activities:
  - **Sandboxie COM Services (BITS) (SANDBOXIE L.T.D)**
  - **Outlook Item Finder (Microsoft Corporation)**
  - **VirusScan On-Demand Scan Task Properties (McAfee, Inc.)**
  - **Mobile Popup Application (Quick Heal Technologies (P) Ltd.)**
  - **ARO 2012 Tutorial**
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Google Chrome** - version 90.0.4430.93
- 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.*