CERT-PH Cybersecurity Threat Feeds

Issue Date	April 07, 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:

- Ongoing Attacks Are Targeting Unsecured Mission-critical SAP Apps
- LinkedIn Spear-Phishing Campaign Targets Job Hunters
- Critical Cloud Bug in VMWare Carbon Black Allows Takeover
- Chinese Cycldek APT Targets Vietnamese Military and Government in Sophisticated Attacks

- CRITICAL
- URGENT
- INFORMATION

Description

Ongoing Attacks Are Targeting Unsecured Mission-critical SAP Apps

2021.04.06 | Source(s): Bleeping Computer, Threatpost, Security Affairs

Analysis:

Threat actors are targeting mission-critical SAP applications unsecured against already patched vulnerabilities, exposing the networks of both commercial and government organizations to attacks. According to cybersecurity experts, 300 successful exploitation through 1500 attack attempts from nearly 20 countries were recorded between June 2020 and March 2021. Threat actors behind these attacks exploited multiple security vulnerabilities, tracked as CVE-2020-6287, CVE-2020-6207, CVE-2018-2380, CVE-2016-95, CVE-2016-3976 and CVE-2010-5326, and insecure configurations in vulnerable SAP applications in attempts to breach the target's systems. Successful exploitation of these vulnerabilities may result in theft of sensitive data, financial fraud, disruption of mission-critical business processes, deployment of ransomware and halt of all operations.

Read more:

[https://www.bleepingcomputer[.]com/news/security/ongoing-attacks-are-targeting-unsecured-mission-critical-sap-apps/]
[https://threatpost[.]com/sap-bugs-cyberattack-compromise/165265/]
[https://securityaffairs[.]co/wordpress/116431/reports/sap-systems-under-attacks.html]

LinkedIn Spear-Phishing Campaign Targets Job Hunters

2021.04.02 | Source(s): Bleeping Computer

Analysis:

Threat actors are crafting fake job offers to lure professionals into downloading backdoor trojan into their systems. Dubbed as Golden Chickens, the threat group is delivering the fileless backdoor, dubbed as more_eggs, through a spear-phishing campaign targeting professionals on LinkedIn with fake job offers. Once downloaded, more_eggs will fetch additional malware and provide access to the victim's system. According to cybersecurity experts, the malware abuses normal Windows processes to avoid antivirus protections.

Read more:

[https://threatpost[.]com/linkedin-spear-phishing-job-hunters/165240/]
[https://thehackernews[.]com/2021/04/hackers-targeting-professionals-with.html]

Critical Cloud Bug in VMWare Carbon Black Allows Takeover

2021.04.06 | Source(s): Threatpost

Analysis:

Cybersecurity experts discovered a critical security vulnerability in the VMware Carbon Black Cloud Workload appliance would allow privilege escalation and the ability to take over the administrative rights for the solution. Tracked as CVE-2021-21982, the flaw is rated 9.1 out of 10 on the CVSS vulnerability-severity scale and is due from incorrect URL handling. Successful exploitation of this flaw could allow an attacker to access the administration API of the appliance and alter administrative configuration settings, eventually taking control of the entire system.

Read more:

[https://threatpost[.]com/critical-cloud-bug-vmware-carbon-black/165278/]

Chinese Cycldek APT Targets Vietnamese Military and Government in Sophisticated Attacks

2021.04.06 | Source(s): Security Affairs, The Hacker News

Analysis:

Cybersecurity experts believed that a China-linked APT group, dubbed as Cycldek, is behind an advanced cyberespionage campaign targeting entities in the government and military sector in Vietnam. Also known as LuckyMouse, Goblin Panda, Hellsing, APT 27 and Conimes, the threat actors are sending out spear-phishing messages to compromise diplomatic targets in Southeast Asia, India and the US. Threat actors downloaded two additional malware DropPhone, a malware that collects environment information from the victim's machine and sends it to DropBox, and CoreLoader, a malware that runs code to evade detection by security products. According to security researchers, attackers targeted a legitimate component from Microsoft Outlook (FINDER.exe) by loading the malicious library outlib.dll that is used to hijacks the intended execution flow of the program to decode and run a shellcode placed in the rdmin.src binary file. Eventually, the final payload is a remote administration tool that provides full control over the victim machine to its operators.

Read more:

[https://securityaffairs[.]co/wordpress/116400/apt/cycldek-apt-targets-vietnam.html]
[https://thehackernews[.]com/2021/04/hackers-from-china-target-vietnamese.html]

CERT-PH Recommendations:

- SAP users and administrators are advised to immediately perform a compromise assessment on SAP applications for risks, existence of misconfigured and unauthorized high-privilege users.
- LinkedIn users are advised to be cautious and observative for any phishing and/or malicious attempts.
- VMware Carbon Black Cloud Workload administrators are urged to limit access to the administrative interface only to authorized users.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **SAP Applications** - latest version
  - **VMware Carbon Black Cloud Workload** - version 1.0.2
- 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.*