CERT-PH Cybersecurity Threat Feeds

Issue Date	January 13, 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 Sunspot Malware Found While Investigating SolarWinds Hack
- Hackers Leak Stolen Pfizer COVID-19 Vaccine Data Online
- Microsoft January 2021 Patch Tuesday Fixes 83 Flaws
- Sophisticated Hacking Campaign Uses Windows and Android Zero-days

- CRITICAL
- URGENT
- INFORMATION

Description

New Sunspot Malware Found While Investigating SolarWinds Hack

2021.01.12 | Source(s): Bleeping Computer

Analysis:

A cybersecurity firm discovered the malware used by the SolarWinds hackers to inject backdoors in Orion platform builds during the supply-chain attack that led to the compromise of several companies and government agencies. Dubbed as Sunspot, was dropped by the attackers in the development environment of SolarWinds' Orion IT management software. After being executed, the malware would monitor and automatically injects a Sunburst backdoor by replacing the company's legitimate source code with malicious code.

Read more:

[https://www.bleepingcomputer[.]com/news/security/new-sunspot-malware-found-while-investigating-solarwinds-hack/]
[https://securityaffairs[.]co/wordpress/113316/malware/sunspot-solarwinds-attack.html]

Hackers Leak Stolen Pfizer COVID-19 Vaccine Data Online

2021.01.12 | Source(s): Bleeping Computer, Security Affairs

Analysis:

The European Medicines Agency (EMA) revealed that some of the Pfizer/BioNTech COVID-19 vaccine data stolen from its servers in December was leaked online. EMA is a decentralized agency responsible for reviewing and approving COVID-19 vaccines, as well as for evaluating, monitoring, and supervising any new medicines introduced to the EU. The leaked stolen data includes email screenshots, EMA peer review comments, Word documents, PDFs, and PowerPoint presentations. The data breach was limited to a single IT application with the attackers primarily targeting data related to COVID-19 medicines and vaccines.

Read more:

[https://www.bleepingcomputer[.]com/news/security/hackers-leak-stolen-pfizer-covid-19-vaccine-data-online/]
[https://securityaffairs[.]co/wordpress/113326/data-breach/ema-data-breach.html]

Microsoft January 2021 Patch Tuesday Fixes 83 Flaws

2021.01.12 | Source(s): Bleeping Computer

Analysis:

With the release of the January 2021 Patch security updates, Microsoft has released fixes for 83 vulnerabilities, with ten classified as Critical and 73 as Important. This includes a zero-day vulnerability, tracked as CVE-2021-1647, which is a remote code execution (RCE) found in the Malware Protection Engine component (mpengine.dll). Affected version of this vulnerability is Microsoft Malware Protection Engine version 1.1.17600.5.

Read more:

[https://www.bleepingcomputer[.]com/news/microsoft/microsoft-january-2021-patch-tuesday-fixes-83-flaws-1-zero-day/]
[https://www.bleepingcomputer[.]com/news/security/microsoft-patches-defender-antivirus-zero-day-exploited-in-the-wild/]

Sophisticated Hacking Campaign Uses Windows and Android Zero-days

2021.01.12 | Source(s): Security Affairs

Analysis:

Cybersecurity experts spotted a hacking campaign that exploits multiple vulnerabilities, including zero-days exploits in Chrome and Windows and n-days exploits in Android. The attacks employed two exploit servers that were triggering multiple vulnerabilities through different exploit chains in watering hole attacks. The two servers were hosting exploits to trigger Google Chrome vulnerabilities to gain an initial foothold on the visitors' devices. The attackers exploited Windows and Android exploit to take over the victim's devices.

Read more:

[https://securityaffairs[.]co/wordpress/113342/hacking/project-zero-watering-hole-attack.html]

CERT-PH Recommendations:

- **o** Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Microsoft's January 2021 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.