CERT-PH Cybersecurity Threat Feeds

Issue Date	January 18, 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:

- **Windows Finger Command Abused by Phishing to Download Malware**
- **Experts Uncover Malware Attacks Against Colombian Government and Companies**
- **Hackers Leaked Altered Pfizer Data to Sabotage Trust in Vaccines**
- **Undisclosed Apache Velocity XSS Vulnerability**

- CRITICAL
- URGENT
- INFORMATION

Description

Windows Finger Command Abused by Phishing to Download Malware

2021.01.15 | Source(s): Bleeping Computer

Analysis:

Attackers are using the normally harmless Windows Finger command to download and install a malicious backdoor on victims' devices. Dubbed as MineBridge, is a 32-bit C++ backdoor designed to be loaded by an older, unpatched instance of the legitimate remote desktop software TeamViewer by DLL load-order hijacking. The 'Finger' command is a utility that originated in Linux/Unix operating systems that allows a local user to retrieve a list of users on a remote machine or information about a particular remote user. In addition to Linux, Windows includes a finger.exe command that performs the same functionality. Once MineBridge is loaded, the remote threat actors will gain full access to the computer and allow them to listen in via the infected device's microphone, and perform other malicious activities.

Read more:
[https://www.bleepingcomputer[.]com/news/security/windows-finger-command-abused-by-phishing-to-download-malware/]

Experts Uncover Malware Attacks Against Colombian Government and Companies

2021.01.14 | Source(s): The Hacker News

Analysis:

Cybersecurity researchers uncover an ongoing surveillance campaign directed against Colombian government institutions and private companies in the energy and metallurgical industries. Dubbed as Operation Spalax, is a phishing campaign that began in 2020. The attack chain begins with the targets receiving phishing emails that lead to the download of malicious files, which are RAR archives hosted on OneDrive or MediaFire containing various droppers responsible for decrypting and running RATs such as Remcos, njRAT, and AsyncRAT on a victimized computer. The RATs not only come with capabilities for remote control but also to spy on targets by capturing keystrokes, recording screenshots, stealing clipboard data, exfiltrating sensitive documents, and even downloading and executing other malware.

Read more:
[https://thehackernews[.]com/2021/01/experts-uncover-malware-attacks-against.html]

Hackers Leaked Altered Pfizer Data to Sabotage Trust in Vaccines

2021.01.15 | Source(s): Bleeping Computer

Analysis:

The European Medicines Agency (EMA) revealed that some of the stolen Pfizer/BioNTech vaccine candidate data was doctored by threat actors before being leaked online with the end goal of undermining the public's trust in COVID-19 vaccines. The leaked data archives included email screenshots, EMA peer review comments, as well as Word, PDF, PowerPoint documents. EMA is the decentralized agency that reviews and approves COVID-19 vaccines in the European Union, and the agency that evaluates, monitors, and supervises any new medicines introduced to the EU.

Read more:
[https://www.bleepingcomputer[.]com/news/security/hackers-leaked-altered-pfizer-data-to-sabotage-trust-in-vaccines/]

Undisclosed Apache Velocity XSS Vulnerability

2021.01.15 | Source(s): Bleeping Computer

Analysis:

An undisclosed Cross-Site Scripting (XSS) vulnerability in Apache Velocity Tools can be exploited by unauthenticated attackers to target government sites, including NASA and NOAA. Tracked as CVE-2020-13959, is a reflected XSS flaw that exists in how the VelocityViewServlet view class renders error pages. When an invalid URL is accessed, the "template not found" error page reflects the resource path portion of the URL as it is without escaping it for potential XSS scripts. An attacker can consequently trick a victim into clicking such a URL, which leads the victim to an altered phishing page, or exfiltrates their login session information. Apache Velocity is a Java-based template engine used by developers for designing views in a Model-View-Controller (MVC) architecture.

Read more:
[https://www.bleepingcomputer[.]com/news/security/undisclosed-apache-velocity-xss-vulnerability-impacts-gov-sites/]

CERT-PH Recommendations:

o 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.

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.