CERT-PH Cybersecurity Threat Feeds

Issue Date	January 05, 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:

- Pegasus Spyware: Now Targets New Zero-Day in iPhone
- CISA Updates SolarWinds Guidance, Urges Agencies to Update Right Away
- Alleged Docs Relating to Covid-19 Vaccine Leaked in Darkweb
- Secret Backdoor Account Found in Several Zyxel Firewall, VPN Products

- CRITICAL
- URGENT
- INFORMATION

Description

New Golang Worm Turns Windows and Linux Servers into Monero Miners

2020.12.30 | Source(s): SC Magazine

Analysis:

Cybersecurity researchers discovered an attack that utilizes three files: a dropper script (bash or powershell), a Golang binary worm and an XMRig Miner, all of which are hosted on the same command and control server, to turn Windows and Linux servers into miners of the cryptocurrency Monero. The malware targets public-facing services such as MySQL, Tomcat admin panel and Jenkins that have weak passwords.

Read more:

[https[:]//www.scmagazine.com/home/security-news/malware/new-golang-worm-turns-windows-and-linux-servers-into-monero-miners/?web_view=true]

CISA Updates SolarWinds Guidance, Urges Agencies to Update Right Away

2020.12.28 | Source(s): ZDNet

Analysis:

Security researchers urged agencies that still run SolarWinds Orion platforms to update to the latest 2020.2.1HF2 version. Tracked as CVE-2020-10148, this vulnerability is an authentication bypass in the Orion API that allows attackers to execute remote code on Orion installations. This vulnerability was being exploited in the wild to install the Supernova malware on servers where the Orion platform was installed.

Read more:

[https[:]//www.zdnet.com/article/cisa-updates-solarwinds-guidance-tells-us-govt-agencies-to-update-right-away/?&web_view=true]

Alleged Docs Relating to Covid-19 Vaccine Leaked in Darkweb

2021.01.01 | Source(s): Security Affairs

Analysis:

Security experts from threat intelligence firm Cyble have found several documents relating to the Covid-19 vaccine allegedly stolen from the European Medicines Agency (EMA) leaked in the Darkweb. The European agency plays a crucial role in the evaluation of COVID-19 vaccines across the EU, it has access to sensitive and confidential information, including quality, safety, and effectiveness data resulting from trials.

Read more:
[https[:]//securityaffairs.co/wordpress/112856/data-breach/covid-19-ema-docs-dark-web.html]

Secret Backdoor Account Found in Several Zyxel Firewall, VPN Products

2021.01.01 | Source(s): The Hacker News

Analysis:

Zyxel has released a patch to address a critical vulnerability in its firmware, tracked as CVE-2020-29583, concerning a hardcoded undocumented secret account that could be abused by an attacker to login with administrative privileges and compromise its networking devices. Successful exploitation may allow an attacker to change firewall settings to allow or block certain traffic. It could also be exploited to intercept traffic or create VPN accounts to gain access to the network behind the device.

Read more:
[https[:]//thehackernews.com/2021/01/secret-backdoor-account-found-in.html?&web_view=true]

CERT-PH Recommendations:

o Update any vulnerable system/applications/devices to their latest and patched versions:
- **SolarWinds** - Orion version 2020.2.1HF2
- **Zyxel ZLD** - V4.60 Patch1

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.