CERT-PH Cybersecurity Threat Feeds

Issue Date	February 02, 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:

- NightScout: Supply Chain Attack on Noxplayer Android Emulator
- Malicious Home Depot Ad Gets Top Spot in Google Search
- Experts Discovered A New Trickbot Module Used for Lateral Movement
- DanaBot Malware Roars Back into Relevancy

- CRITICAL
- URGENT
- INFORMATION

Description

NightScout: Supply Chain Attack on Noxplayer Android Emulator

2021.02.02 | Source(s): Bleeping Computer, Security Affairs, ZDNet

Analysis:

Security experts uncovered a new supply chain attack leveraging the update process of NoxPlayer, a free Android emulator for PCs and Macs. Dubbed as NightScout, the threat actors compromised one of the company's official API (api.bignox.com) and file-hosting servers (res06.bignox.com). Once gained a foothold in the target infrastructure they tampered with the download URL of NoxPlayer updates in the API server to deliver tainted updates. The experts reported that threat actors employed at least three different malware families in this supply chain attack.

Read more:

[https://www.bleepingcomputer[.]com/news/security/android-emulator-supply-chain-attack-targets-gamers-with-malware/]
[https://securityaffairs[.]co/wordpress/114090/hacking/noxplayer-supply-chain-attack.html]
[https://www.zdnet[.]com/article/hacker-group-inserted-malware-in-noxplayer-android-emulator/]

Malicious Home Depot Ad Gets Top Spot in Google Search

2021.01.30 | Source(s): Bleeping Computer, Threatpost

Analysis:

A malicious Home Depot advertising campaign is redirecting Google search visitors to tech support scams. The ad clearly states it's for www[.]homedepot[.]com, and hovering over it shows the site's legitimate destination URL. However, when visitors click on the ad, they will be redirected through various ad services until eventually they are redirected to a tech support scam. Ultimately, the visitor will land at a page showing an incredibly annoying "Windows Defender - Security Warning' tech support scam. This scam will repeatedly open the Print dialog box which prevents the visitor from easily closing the page. Victims who fall for these scams, call the number thinking it is a legitimate alert. The scammers then state that the caller must purchase a support package to unlock Windows.

Read more:

[https://www.bleepingcomputer[.]com/news/security/beware-malicious-home-depot-ad-gets-top-spot-in-google-search/]

Experts Discovered A New Trickbot Module Used for Lateral Movement

2021.02.02 | Source(s): Security Affairs, ZDNet

Analysis:

Cybersecurity experts spotted a new Trickbot module that is used to scan local networks and make lateral movement inside the target organization. Dubbed as masrv, is a new module of the Trickbot malware that leverages the Masscan open-source utility for local network scanning and is used to search for other devices with open ports that can be compromised. Once infected a device, the masrv is used to drop the component and send a series of Masscan commands to scan the local network and send the scan results back to the C2 server. The bot scans the network for systems with sensitive or management ports left open inside an internal network, then botnet operators can then deploy other modules for lateral movements.

Read more:
[https://securityaffairs[.]co/wordpress/114103/malware/trickbot-new-module.html]
[https://www.zdnet[.]com/article/new-trickbot-module-uses-masscan-for-local-network-reconnaissance/]

DanaBot Malware Roars Back into Relevancy

2021.01.28 | Source(s): Threatpost

Analysis:

Researchers discovered a new fourth version of the DanaBot banking trojan. DanaBot is a banking trojan that first targeted users in Australia via emails containing malicious URLs. Criminals then developed a second variant and targeted US companies as a part of a series of large-scale campaigns. A third variant surfaced in February 2019 that was significantly enhanced with remote command-and-control functionality. The fourth version is written in Delphi and has several anti-analysis attributes. It also comes with the same deadly arsenal of tools with previous iterations such as ToR component to anonymize communications between the threat actors and an infected hardware. Current findings also suggest that the malware-as-a-service component to DanaBot was very much active and growing. Moreover, DanaBot's initial infection points are warez and cracks websites that offer software keys, cracks for download including anti-virus programs, VPNs, graphic and document editors, and games.

Read more:
[https://threatpost[.]com/danabot-malware-roars-back/163358/]

CERT-PH Recommendations:

o NoxPlayer users are advised to uninstall the software. If not possible, perform a standard reinstall from clean media and do not download any updates until BigNox sends notification that they have mitigated the threat.
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 Avoid installing unknown or unverified applications, especially from third-party distribution platforms. Scrutinize application's permissions before installation and avoid allowing apps to view unnecessary information and other application's data.
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.

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.*