CERT-PH Cybersecurity Threat Feeds

Issue Date	May 17, 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:

- QNAP Warns of eCh0raix Ransomware Attacks, Roon Server Zero-Day
- MSBuild Tool Used To Deliver RATs Filelessly
- Magecart Gang Hides PHP-based Web Shells In Favicons
- Pakistan-Linked Hackers Added New Windows Malware to Its Arsenal

- CRITICAL
- URGENT
- INFORMATION

Description

QNAP Warns of eCh0raix Ransomware Attacks, Roon Server Zero-Day

2021.05.14 | Source(s): Bleeping Computer, Security Affairs

Analysis:

The Taiwan-based NAS appliance maker, QNAP warns customers of an actively exploited Roon Server zero-day bug and eCh0raix ransomware attacks targeting their Network Attached Storage (NAS) devices. According to security researchers, an actively exploited zero-day vulnerability impacting Roon Labs' Roon Server 2021-02-01 and earlier versions. The eCh0raix ransomware has been reported to affect QNAP NAS devices and devices using weak passwords may be more susceptible to attacks. ECh0raix is written in the Go programming language and uses AES encryption to encrypt files. The malicious code appends .encrypt extension to filenames of encrypted files.

Read more:

[https://www.bleepingcomputer[.]com/news/security/qnap-warns-of-ech0raix-ransomware-attacks-roon-server-zero-day/]
[https://securityaffairs[.]co/wordpress/117943/hacking/qnap-ech0raix-ransomware-roon-server.html]

MSBuild Tool Used to Deliver RATs Filelessly

2021.05.16 | Source(s): Security Affairs, The Hacker News

Analysis:

Security researchers observed that threat actors were abusing Microsoft Build Engine (MSBuild) to filelessly deliver remote access trojans and RedLine Stealer password-stealing malware on targeted Windows systems. MSBuild is a free and open-source build tool set for managed code as well as native C++ code and was part of .NET Framework. It is used for building apps and gives users an XML schema that controls how the build platform processes and builds software, to filelessly deliver RemcosRAT, and RedLine stealer using callbacks. The MSBuild files employed in the attacks contained encoded executables and shellcode, some of which were hosted on Russian image-hosting site (joxi[.]net). Most of the samples analyzed were used to deliver the Remcos RAT, while others were also delivering the Quasar RAT and RedLine Stealer. Remcos is a commercial software that can be used for remote control, remote admin, remote anti-theft, remote support and pentesting. The Quasar RAT is available for free on GitHub, many other attackers used it in their campaigns, including the Gaza Cybergang, which is also known as Gaza Hackers Team and Molerats.

Read more:

[https://securityaffairs[.]co/wordpress/117969/malware/msbuild-delivers-rat.html]
[https://thehackernews[.]com/2021/05/hackers-using-microsoft-build-engine-to.html]

Magecart Gang Hides PHP-based Web Shells in Favicons

2021.05.14 | Source(s): Security Affairs, The Hacker News

Analysis:

Magecart hackers are distributing malicious PHP web shells hidden in website favicon to inject JavaScript e-skimmers into online stores and steal payment information. Tracked as Smilodon or Megalodon, the web shells employed in the attacks dynamically load JavaScript skimming code via

server-side requests into online stores. This technique allows bypassing most client-side security tools. Threat actors edited the shortcut icon tags with a path to the fake PNG file. Unlike previous incidents that involved the use of fake favicons to hide malicious JavaScript code, in this recent wave of attacks the webshell is written in PHP. The web shell retrieves the e-skimmer from a remote host, the code involved in this attack is similar to a variant used in Cardbleed attacks. The attribution of the attack to Magecart Group 12 is based on overlaps in TTPs observed in the attacks, experts also noticed that the domain name used in the attack (zolo[.]pw) is associated to the same IP address (217.12.204[.]185) as recaptcha-in[.]pw and google-statik[.]pw, domains previously associated with Magecart Group 12.

Read more:

[https://securityaffairs[.]co/wordpress/117909/cyber-crime/magecart-web-shells.html]
[https://thehackernews[.]com/2021/05/magecart-hackers-now-hide-php-based.html]

Pakistan-Linked Hackers Added New Windows Malware to its Arsenal

2021.05.14 | Source(s): The Hacker News

Analysis:

Security researchers Pakistan-linked cybercriminals continue to rely on social engineering as a crucial component of its operations as part of an evolving espionage campaign against Indian targets. Tracked as Transparent Tribe, the group was linked with the recent attacks, which has created fraudulent domains mimicking legitimate Indian military and defense organizations, and other fake domains posing as file-sharing sites to host malicious artifacts. These domains are used to deliver maldocs distributing CrimsonRAT, and ObliqueRAT, with the group incorporating new phishing, lures such as resume documents, conference agendas, and defense and diplomatic themes into its operational toolkit. According to security experts, Transparent Tribe relies heavily on the use of maldocs to spread their Windows implants. The variety of maldoc lures Transparent Tribe employs indicates the group still relies on social engineering as a core component of its operations.

Read more:

[https://thehackernews[.]com/2021/05/pakistan-linked-hackers-added-new.html]

CERT-PH Recommendations:

- Users of QNAP NAS devices that runs vulnerable Roon servers are urged to disable the Roon Server temporarily until a security patch is published. If not possible, ensure that the NAS devices are not publicly exposed on the Internet to protect it from possible attacks.
- 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.*