CERT-PH Cybersecurity Threat Feeds

Issue Date	April 30, 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:

- F5 BIG-IP Found Vulnerable to Kerberos KDC Spoofing Vulnerability
- Purple Lambert, a New Malware of CIA-linked Lambert APT Group
- QNAP Warns of AgeLocker Ransomware Attacks On NAS Devices
- Cybercriminals Widely Abusing Excel 4.0 Macro to Distribute Malware

- CRITICAL
- URGENT
- INFORMATION

Description

F5 BIG-IP Found Vulnerable to Kerberos KDC Spoofing Vulnerability

2021.04.28 | Source(s): The Hacker News

Analysis:

Cybersecurity researchers have disclosed a newly discovered bypass vulnerability in the Kerberos Key Distribution Center (KDC) security feature impacting F5 Big-IP application delivery services. Tracked as CVE-2021-23008, the KDC Spoofing vulnerability allows an attacker to bypass the Kerberos authentication to Big-IP Access Policy Manager (APM), bypass security policies and gain unfettered access to sensitive workloads and can be used to bypass authentication to the Big-IP admin console.

Read more:

[https://thehackernews[.]com/2021/04/f5-big-ip-found-vulnerable-to-kerberos.html]

Purple Lambert, a New Malware of CIA-linked Lambert APT Group

2021.04.29 | Source(s): Security Affairs

Analysis:

Cybersecurity experts discovered a new strain of malware believed to be part of the arsenal of the US Central Intelligence Agency (CIA). The new malware is linked with a cyber group, named Lambert APT, that has been active since at least 2008 and targets organizations worldwide using a complex cyberattack platform that could target both Windows and OSX systems. Dubbed as Purple Lambert, the malware has a modular structure and its network module passively listens for a magic packet. The malicious code collects basic information about the infected system and also allows attackers to execute additional payload.

Read more:

[https://securityaffairs[.]co/wordpress/117340/apt/purple-lambert-cia-arsenal.html]

QNAP Warns of AgeLocker Ransomware Attacks On NAS Devices

2021.04.29 | Source(s): Bleeping Computer

Analysis:

Cybersecurity experts warn QNAP customers to secure their Network Attached Storage (NAS) devices to defend against ransomware attacks targeting their data. Dubbed as AgeLocker, the ransomware was first spotted in July 2020 and is targeting QNAP NAS devices worldwide. AgeLocker uses an encryption algorithm known as Age (short for Actually Good Encryption), designed as a GPG replacement for encrypting files, backups, and streams. Age uses the X25519 (an ECDH curve), ChaChar20-Poly1305, and HMAC-SHA256 algorithms that makes it a very secure method to encrypt victims' files.

Read more:

[https://www.bleepingcomputer[.]com/news/security/qnap-warns-of-agelocker-ransomware-attacks-on-nas-devices/]

Microsoft Teams Outage Impacts User Logins and Chats

2021.04.28 | Source(s): The Hacker News

Analysis:

Threat actors are seen to be increasingly adopting Excel 4.0 documents as an initial stage vector to distribute malware such as ZLoader and Quakbot. Excel 4.0 macros (XLM), the precursor to Visual Basic for Applications (VBA), is a legacy feature incorporated in Microsoft Excel for backward compatibility reasons. Microsoft warns in its support document that enabling all macros can cause "potentially dangerous code" to run. Also known as QBOT, the Quakbot malware has remained a notorious banking trojan capable of stealing banking credentials and other financial information, while also gaining worm-like propagation features. Typically spread via weaponized Office documents, variants of QakBot have been able to deliver other malware payloads, log user keystrokes, and even create a backdoor to compromised machines.

Read more:

[https://thehackernews[.]com/2021/04/cybercriminals-widely-abusing-excel-40.html]

CERT-PH Recommendations:

- QNAP NAS Owners are highly advised to check for any unknown user accounts from the device, remove unknown or unused applications from the NAS devices.
- Additionaly, implement an access control list for the NAS devices and regular checking of device firmware updates and applications to mitigate against potential attacks.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **F5 BIG-IP APM** - versions 12.1.6, 13.1.4, 14.1.4, and 15.1.3
  - **QNAP QTS and QuTS** - latest stable version
- 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.*