CERT-PH Cybersecurity Threat Feeds

Issue Date	**April 05, 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:

- **VMware Fixes Authentication Bypass in Data Center Security Software**
- **Tens of Thousands of QNAP SOHO NAS Devices Affected by Unpatched RCEs**
- **Evolution and Rise of the Avaddon Ransomware-as-a-Service**
- **Data of 533 Million Facebook Users Leaked in A Hacking Forum for Free**

- **CRITICAL**
- **URGENT**
- **INFORMATION**

Description

VMware Fixes Authentication Bypass in Data Center Security Software

2021.04.01 | Source(s): Bleeping Computer, Security Affairs

Analysis:

VMware addressed a critical vulnerability in the VMware Carbon Black Cloud Workload appliance that could allow attackers to bypass authentication after exploiting vulnerable servers. Tracked as CVE-2021-21982, the vulnerability can be exploited by manipulating an administrative interface URL to obtain valid authentication tokens. Using this auth token, the malicious actor can then access the administration API of unpatched VMware Carbon Black Cloud Workload appliances. Successful exploitation could allow an attacker to view and alter administrative configuration settings.

Read more:

[https://www.bleepingcomputer[.]com/news/security/vmware-fixes-authentication-bypass-in-data-center-security-software/]
[https://securityaffairs[.]co/wordpress/116233/security/vmware-carbon-black-cloud-flaw.html]

Linux Kernel Flaws that can Allow Bypassing Spectre Mitigations

2021.04.02 | Source(s): Security Affairs

Analysis:

Security researchers discovered critical flaws in QNAP small office/home office (SOHO) network-attached storage (NAS) devices that could allow remote attackers to execute arbitrary code on vulnerable devices. The first vulnerability is a remote code execution (RCE) issue that affects any QNAP device exposed to the internet that resides in the NAS web server. The second vulnerability is an arbitrary file write vulnerability that resides in the DLNA server which handles UPNP requests on this port. The vulnerability could be exploited by remote attackers to execute arbitrary code on a remote NAS device.

Read more:

[https://securityaffairs[.]co/wordpress/116260/iot/qnap-soho-nas-rces.html]

Evolution and Rise of the Avaddon Ransomware-as-a-Service

2021.04.03 | Source(s): Security Affairs

Analysis:

The Avaddon ransomware operators updated their malware after security researchers released a public decryptor in February 2021. The Avaddon ransomware quickly reacted to the availability of the decryptor and released an update for the code of their malware that made the tool inefficient. The new version of the Avaddon is advertised with capabilities such as file encryption via AES256 + RSA2048, supporting full-file encryption & custom parameters, encryption of all local and remote (and accessible) drives, ability to spread across network shares (SMB, DFS), payload executes as administrator, encrypts hidden files and volumes, among others.

Read more:
[https://securityaffairs[.]co/wordpress/116282/cyber-crime/avaddon-ransomware-evolution.html]

Data of 533 Million Facebook Users Leaked in A Hacking Forum for Free

2021.04.03 | Source(s): Security Affairs

Analysis:

A user has leaked the phone numbers and personal data of 533 million Facebook users in a hacking forum for free online. The data of Facebook users from 106 countries are available for free, over 32 million records belonging to users from the US, 11 from the UK, and 6 million users from India. According to security researchers, the leaked data includes users' phone numbers, Facebook IDs, full names, locations, birthdates, bios, and for some accounts the associated email addresses. The leaked data could be exploited by threat actors to carry out a broad range of malicious activities.

Read more:
[https://securityaffairs[.]co/wordpress/116316/social-networks/facebook-phone-numbers.html]

CERT-PH Recommendations:

- 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.
- Users are encouraged to be cautious and check the email thoroughly before downloading and opening email attachments, especially when received from unknown email senders, as ransomware are usually found on email attachments and pirated application software.
- Update any vulnerable system/applications/devices to their latest and patched versions:
    - **VMware Carbon Black Cloud Workload Appliance** - version 1.0.2
    - **QNAP SOHO/Home NAS** - latest 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.*