CERT-PH Cybersecurity Threat Feeds

Issue Date	January 19, 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:

- IObit Forums Hacked in Widespread DeroHE Ransomware Attack
- OpenWRT Forum User Data Stolen in Weekend Data Breach
- FBI Warns of Vishing Attacks Stealing Corporate Accounts
- Multiple Backdoors and Vulnerabilities Discovered In FiberHome Routers

- CRITICAL
- URGENT
- INFORMATION

Description

IObit Forums Hacked in Widespread DeroHE Ransomware Attack

2021.01.15 | Source(s): Bleeping Computer

Analysis:

Windows utility developer IObit was hacked to perform a widespread attack and distributed the strange DeroHE ransomware to its forum members. IObit forum members began receiving emails claiming to be from IObit stating that they are entitled to a free 1-year license to their software as a special perk of being a forum member. Included in the email is a 'GET IT NOW' link that was used to distribute a zip file that contains digitally signed files from the legitimate IObit License Manager program, but with the IObitUnlocker.dll replaced with an unsigned malicious version. When IObit License Manager.exe is executed, the malicious IObitUnlocker.dll will be executed to install the DeroHE ransomware to C:\Program Files (x86)\IObit\iobit.dll and execute it, encrypting files and appends the .DeroHE extension to encrypted files.

Read more:

[https://www.bleepingcomputer[.]com/news/security/iobit-forums-hacked-in-widespread-derohe-ransomware-attack/]

OpenWRT Forum User Data Stolen in Weekend Data Breach

2021.01.15 | Source(s): Bleeping Computer, Security Affairs

Analysis:

The OpenWRT forum, a large community of enthusiasts of alternative, open-source operating systems for routers, announced a data breach. According to forum administrators, an unauthorized third party gained admin access to and copied a list with details about forum users and related statistical information. The intruder used the account of an OpenWRT administrator. Although the account had "a good password," additional security provided by two-factor authentication (2FA) was not active. Email addresses and handles of the forum users have been stolen. Researchers add that they believe the attacker was not able to download the forum database, meaning that passwords should be safe but as a precaution, they reset all passwords and flushed any API keys.

Read more:

[https://www.bleepingcomputer[.]com/news/security/openwrt-forum-user-data-stolen-in-weekend-data-breach/]
[https://securityaffairs[.]co/wordpress/113586/data-breach/openwrt-forum-hacked.html]

FBI Warns of Vishing Attacks Stealing Corporate Accounts

2021.01.18 | Source(s): Bleeping Computer

Analysis:

The Federal Bureau of Investigation (FBI) has issued a notification warning of ongoing vishing attacks attempting to steal corporate accounts and credentials for network access and privilege

escalation from US and international-based employees. Vishing, also known as voice phishing, is a social engineering attack where attackers impersonate a trusted entity during a voice call to persuade their targets into revealing sensitive information such as banking or login credentials. The threat actors are using Voice over Internet Protocol (VoIP) platforms, aka IP telephony services to target employees of companies worldwide and to trick them into logging into a phishing webpage they controlled to harvest their usernames and passwords.

Read more:

[https://www.bleepingcomputer[.]com/news/security/fbi-warns-of-vishing-attacks-stealing-corporate-accounts/]

Multiple Backdoors and Vulnerabilities Discovered in FiberHome Routers

2021.01.18 | Source(s): ZDNet

Analysis:

At least 28 backdoor accounts and several other vulnerabilities have been discovered in the firmware of a popular FTTH ONT router, widely deployed across South America and Southeast Asia. Security researchers identified a large collection of security issues with FiberHome HG6245D and FiberHome RP2602, two FTTH ONT router models developed by Chinese company FiberHome Networks. Fiber-to-the-Home Optical Network Terminal (FTTH ONT) are special devices fitted at the end of optical fiber cables. Their role is to convert optical signals sent via fiber optics cables into classic Ethernet or wireless (WiFi) connections.

Read more:

[https://www.zdnet[.]com/article/multiple-backdoors-and-vulnerabilities-discovered-in-fiberhome-routers/]

CERT-PH Recommendations:

o For an additional layer of protection, users are advised to set up a Multifactor Authentication (MFA) whenever accessing sensitive data or assets.

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 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.