CERT-PH Cybersecurity Threat Feeds

Issue Date	January 12, 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:

- DarkSide Ransomware Decryptor Recovers Victims' Files for Free
- Networking Giant Ubiquiti Alerts Customers of Potential Data Breach
- Mac Malware Uses 'run-only' AppleScripts To Evade Analysis
- Microsoft Releases Linux Endpoint Detection and Response Features'

- CRITICAL
- URGENT
- INFORMATION

Description

DarkSide Ransomware Decryptor Recovers Victims' Files for Free

2021.01.11 | Source(s): Bleeping Computer, ZDNet

Analysis:

Cybersecurity firm Bitdefender has released a free decryptor for the DarkSide ransomware to allow victims to recover their files without paying a ransom. DarkSide operates under a ransomware-as-a-service business model and the gang is made out of former affiliates who have already made millions working with other ransomware operations. After encrypting their victims' systems, they will charge different amounts for ransom ranging from $200,000 to $2,000,000,

Read more:

[https://www.bleepingcomputer[.]com/news/security/darkside-ransomware-decryptor-recovers-victims-files-for-free/]
[https://www.zdnet[.]com/article/free-decrypter-released-for-victims-of-darkside-ransomware/]

Networking Giant Ubiquiti Alerts Customers of Potential Data Breach

2021.01.11 | Source(s): Bleeping Computer, ZDNet

Analysis:

Networking device maker Ubiquiti has announced a security incident that may have exposed its customers' data. Ubiquiti began emailing customers to change their passwords and enable 2FA after an attacker hacked their systems hosted at a third-party cloud provider. The company states that they are not aware of any customer databases that were illegally accessed but cannot be sure that the attack did not expose customers' data. Ubiquiti is a very popular networking device manufacturer best known for its UniFi line of wired and wireless network products and a cloud management platform.

Read more:

[https://www.zdnet[.]com/article/ubiquiti-tells-customers-to-change-passwords-after-security-breach/]
[https://www.bleepingcomputer[.]com/news/security/networking-giant-ubiquiti-alerts-customers-of-potential-data-breach/]

Mac Malware Uses 'run-only' AppleScripts To Evade Analysis

2021.01.11 | Source(s): Bleeping Computer

Analysis:

A cryptocurrency mining campaign targeting macOS is using malware, tracked as OSAMiner, that has evolved into a complex variant giving researchers a lot of trouble analyzing it. Analyzing the previous variant is difficult because payloads are exported as run-only AppleScript files, which makes decompiling them into source code a tall order. Recently, the recent OSAMiner campaigns use three run-only AppleScript files to deploy the mining process on the infected

macOS machine: a parent script that executes from the trojanized application, an embedded script and the miner setup AppleScript.

Read more:

[https://www.bleepingcomputer[.]com/news/security/mac-malware-uses-run-only-applescripts-to-evade-analysis/]

Microsoft Releases Linux Endpoint Detection and Response Features

2021.01.11 | Source(s): Bleeping Computer

Analysis:

Microsoft Defender for Endpoint's detection and response (EDR) capabilities are now generally available on Linux servers. EDR capabilities allow admins and security teams to spot attacks targeting or involving Linux servers in their environments almost in real-time with the help of alerts automatically aggregated as incidents based on attacker techniques and attribution. EDR capabilities are available on Linux Server distributions supported by Microsoft Defender for Endpoint (Linux), including RHEL 7.2+, CentOS Linux 7.2+, Ubuntu 16 LTS or higher LTS, SLES 12+, Debian 9+, and Oracle Linux 7.2.

Read more:

[https://www.bleepingcomputer[.]com/news/security/windows-psexec-zero-day-vulnerability-gets-a-free-micropatch/]

CERT-PH Recommendations:

o DarkSide ransomware victims can check and download the free decrypter from the official Bitdefender site to recover encrypted files.

o Ubiquiti customers are advised to change their account passwords and turn on two-factor authentication (2FA).

o Update any vulnerable system/applications/devices to their latest and patched versions:

- Microsoft Defender for Endpoint for Linux - version 101.18.53 or higher

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.