

1. **Introduction.** A new **malware attack** capable of **Cryptojacking** has been discovered, is targeting **mac devices**. Cryptojacking is a form of **cyber-attack** in which a hacker hijacks a **target's processing power** in order to mine cryptocurrency.

2. **Technical analysis.**

a. The malware is mining for **Monero cryptocurrency**, attack cycle comprises of following three components:-

(1) **Dropper.** Downloads the malware.

(2) **Launcher.** A file named "**pplauncher**" that installs and launches the malware. It is activated by a **launch daemon (com.pplauncher.plist)**.

(3) **Miner "mshelper.** Which is based on **XMRig**, an open-source **Monero** miner.

b. Analysis reveals that **fake Adobe Flash Player installers** infected files in **phishing emails** or downloads from **unauthentic piracy platforms**.

3. **Affected Products.** The malware is affecting devices running on Mac operating systems.

4. **Mitigation Method.**

a. To remove **malicious files** following steps are recommended:-

(1) To delete "**mshelper**", install an **antivirus** or an **anti-miner** program.

(2) In order to remove "**mshelper**" manually, delete these below mentioned files and reboot your device:-

(a) /Library/LaunchDaemons/com.pplauncher.plist.

(b) /Library/Application Support/pplauncher/pplauncher.

b. Following **best practices** are recommended for **MAC users** against cyber- attacks:-

(1) It is recommended to use a **standard user account** or everyday activities and the **administrator** user accounts system configuration.

(2) **Turn Off Java And Auto Download** In Safari Browser.

(3) Remove **Standalone Flash Player**.

(4) Apple has given the 'option to allow other devices to **remotely: access** your Mac, it is advised **disable remote login**.

(5) Install **Gatekeeper**, a **malware check app** which protects

SECRET

your Mac from malware and misbehaving apps downloaded from the internet.

- (6) To ensure your network security and online privacy use **VPN**.
- (7) It is strongly recommended to Update Your Mac OS X Regularly.

5. **Recommendations.**

- a. Strictly follow all mitigation measures mentioned at para 4.
- b. **It is Strongly recommended Install and regularly update ;Mac Anti- Virus Software.**
- c. Download and install applications only form **App store** and avoid third-party sources.
- d. Don't **download attachments** from **emails** unless you are sure about the source.
- e. Be vigilant on **social media** groups and **don't click** on any **link** being , shared by any known/ unknown group member.