CYBER **NEWSLETTER**

EXPLOITS GALORE!

ANDROID MMRAT

By exploiting a rarely used method of communication, protobuf serialization, the malware MMRat allows attackers to more efficiently steal your data. The malware was spotted first by Trend Micro in late June 2023. The good news here is that the exploit primarily targets users in Southeast Asia as of now. The bad news is that it tends to go undetected by antivirus software. With a long list of data sets that the attackers can gain access to, refer to the bleeping computer article for more information on this.

WORDPRESS

Tracked as CVE-2023-40004, the exploit affects third-party plugs-ins used to facilitate data migration. The vulnerable code includes a lack of permission and nonce validation within the init function. While this is minimized because of the fact that it is only using this during migrations, the result when exploited is the exfiltration of data. As this can include user details, critical website data and proprietary information, ensuring that the patch released on July 26th is applied before any data migration is of paramount importance. Applications that include the flawed code can be seen in Box, Google Drive, OneDrive, and Dropbox.

SNEAKY CONTAINER

Disclosed by findings from Deep Instinct security at the Def Con security conference, the POC shows how attackers can leverage malware detection evasion techniques to bypass endpoint security. By redirecting the links in the Windows Container, attackers can obfuscate attacks and help bypass endpoint detection. Using the minifilter driver withing the Windows container instance, which operates at a lower altitude of 180000-189999 and most antivirus filters function in the 320000-329999 range. Since this results in the antivirus not getting the full picture, the payload is able to bypass detection. There is some good news as it would take an attacker having administrative privileges to pull of this type of attack.

"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked." -Richard Clarke

INTERNET SHOPPING ATTACK

While attacks on e-commerce sites are nothing new, they are definitely on the rise in 2023. With companies using more and more APIs for the platform, attackers have constantly been testing more exploits to this type of infrastructure. Common threats to the e-commerce platforms include spam/phishing, malware/ransomware, e-skimming, cross-site scripting and SQL Injection. Thes types of attacks are generally found if the company does regular penetration testing. While a full pen test can become expensive, companies have started to offer PTaaS, penetration test as a service. The need to have regular testing performed becomes extremely important as the threat landscape is constantly changing.

As we wrap this week's cyber round up, the main take away is to stay vigilant. While many attack vectors can be fixed with regular patching, there will always be the ones that are able to evade detection.