Weekly Intelligence Summary

Nov 6, 2020 (TLP: WHITE)

In the spotlight this week:

- The threat actors behind ***Maze ransomware*** have announced their ***retirement***. On November 1, they posted the retirement announcement on the website where they would normally name and shame their victims that were unwilling to pay the ransom. On the other side, the operators of the ***REvil ransomware*** strain have ***"acquired" the source code of the KPOT*** trojan in an auction held on a hacker forum last month.
- Oracle publishes rare out-of-band security update for ***WebLogic servers***. The new patch (tracked as CVE-2020-14750) ***adds additional fixes to a first bug*** (tracked as CVE-2020-14882), originally patched with Oracle's standard quarterly October 2020 security updates. CVE-2020-14882 is a dangerous vulnerability that allows attackers to execute malicious code on an Oracle WebLogic server with elevated privileges before the server's authentication kicks in.
- ***UNC1945 targeted Oracle Solaris*** operating systems, utilized several tools and utilities against Windows and Linux operating systems, loaded and operated custom virtual machines, and employed techniques to evade detection. Mandiant discovered and reported to Oracle ***CVE-2020-14871***. Mandiant said the group downloaded and installed a QEMU virtual machine running a version of the ***Tiny Core Linux OS***. This custom-made Linux VM came pre-installed with several hacking tools like network scanners, password dumpers, exploits, and reconnaissance ***toolkits*** that allowed UNC1945 to scan a company's internal network for weaknesses and move laterally to multiple systems, regardless if they ran Windows or *NIX-based systems.
- Cybereason Nocturnus Team has been tracking various North Korean threat actors known as ***Kimsuky***, (aka: Velvet Chollima, Black Banshee and Thallium), which has been active since at least 2012 and is believed to be operating on behalf of the North Korean regime. One of ***KGH_SPY's components*** is an information stealer that can harvest data from browsers, Windows Credential Manager, WINSCP, and mail clients. At the time of writing the report, no antivirus vendor's products detected the component.

(cisp-id:9461) Nov 4, 2020
REvil ransomware gang 'acquires' KPOT malware.
Ransomware gang who claims to have earned $100 million buys the source code of the KPOT information stealer trojan for $6,500. The sale took place after the KPOT malware author decided to auction off the code, desiring to move off to other projects. The sale was organized as a public auction on a private underground hacking forum for Russian-speaking cyber-criminals, security researcher Pancak3 told ZDNet in an interview last month.
https://www.zdnet.com/article/revil-ransomware-gang-acquires-kpot-malware/#ftag=RSSbaffb68

(cisp-id:9466) Nov 3, 2020
New RegretLocker ransomware targets Windows virtual machines.
RegretLocker was discovered in October and is a simple ransomware in terms of appearance as it does not contain a long-winded ransom note and uses email for communication rather than a Tor payment site. When encrypting files, it will append the innocuous-sounding mouse extension to

encrypted file names. Once the virtual drive is mounted as a physical disk in Windows, the ransomware can encrypt each one individually, which increases the speed of encryption.
https://www.bleepingcomputer.com/news/security/new-regretlocker-ransomware-targets-windows-virtual-machines/

(cisp-id:9452) Nov 3, 2020
Oracle publishes rare out-of-band security update for WebLogic servers.
The new patch (tracked as CVE-2020-14750) adds additional fixes to a first bug (tracked as CVE-2020-14882), originally patched with Oracle's standard quarterly October 2020 security updates. CVE-2020-14882 is a dangerous vulnerability that allows attackers to execute malicious code on an Oracle WebLogic server with elevated privileges before the server's authentication kicks in. Since exploitation is trivial, proof-of-concept (PoC) exploit code was made public within days after the initial Oracle patch.
https://www.zdnet.com/article/oracle-publishes-rare-out-of-band-security-update-for-weblogic-servers/

(cisp-id:9468) Nov 2, 2020
While UNC1945 activity went as far back as 2018, Mandiant said the group caught their eye earlier this year after the threat actor utilized a never-before-seen vulnerability in the Oracle Solaris operating system. Tracked as CVE-2020-14871, the zero-day was a vulnerability in the Solaris Pluggable Authentication Module (PAM) that allowed UNC1945 to bypass authentication procedures and install a backdoor named SLAPSTICK on internet-exposed Solaris servers. Mandiant said the group downloaded and installed a QEMU virtual machine running a version of the Tiny Core Linux OS. This custom-made Linux VM came pre-installed with several hacking tools like network scanners, password dumpers, exploits, and reconnaissance toolkits that allowed UNC1945 to scan a company's internal network for weaknesses and move laterally to multiple systems, regardless if they ran Windows or *NIX-based systems.
https://www.zdnet.com/article/hacker-group-uses-solaris-zero-day-to-breach-corporate-networks/#ftag=RSSbaffb68

(cisp-id:9467) Nov 2, 2020
Google patches second Chrome zero-day in two weeks.
Identified as CVE-2020-16009, the zero-day was discovered by Google's Threat Analysis Group (TAG), a security team at Google tasked with tracking threat actors and their ongoing operations In typical Google fashion, details about the zero-day and the group exploiting the bug have not been made public — as a way to allow Chrome users more time to install the updates and prevent other threat actors from developing their own exploits for the same zero-day. However, in a short changelog published today, Google said the zero-day resides in V8, the Chrome component that handles JavaScript code. Chrome users are advised to update their browser to version 86.0.4240.183 or later.
https://www.zdnet.com/article/google-patches-second-chrome-zero-day-in-two-weeks/#ftag=RSSbaffb68

(cisp-id:9444) Nov 1, 2020
Maze ransomware operators are shutting down their operation
The Maze cybercrime gang is shutting down its operations, it was considered one of the most prominent and active ransomware crew since it began operating in May 2019. The gang was the first to introduce a double-extortion model in the cybercrime landscape at the end of 2019. The double-extortion technique was later adopted by other ransomware gangs, including REvil, DoppelPaymer, Nefilim, and Clop. This week, Maze has started to remove victims from their data leak site except for two organizations that already had all of their data published. At the time it is not clear if Maze operators plan to release the keys to allow its victims to decrypt their files after they shut down the operations.
https://securityaffairs.co/wordpress/110274/cyber-crime/maze-ransomware-shut-down.html

You can build your Threat Intelligence Platform @ https://splunkbase.splunk.com/app/5297/