Weekly Intelligence Summary

Aug 7, 2020 (TLP: WHITE)

In the spotlight this week:

- BleepingComputer confirmed that Garmin has received the decryption key by paying US$10m. We expect more ransomware attacks and ransom leaks in near future and the financial losses will be jump bigger than BEC cases. In Hong Kong, we found IT teams usually hide the impact of the incidents from the management and management does not want to believe they are having data breach when ransomeware hit the network.
- FBI has high confidence that Chinese government actors are using Taidoor in conjunction with proxy servers to maintain a presence on victim networks and to further network exploitation.
- SME are actively targeted by LockBit ransomware operators according to an Interpol report. LockBit partnered with Maze ransomware's operators to create an extortion cartel that allows them to share the same data leak platform during their operations and to exchange tactics and intelligence.
- Pulse Secure VPN servers that are running a firmware version vulnerable to the CVE-2019-11510 vulnerability. DATC believe attackers (including human-operated ransomware actors group, such as Evil and Netwalker) are actively scanning all Internet facing devices using online scanner like shodan to locate the vulnerable VPN, then compromise the victims networks. Micorsoft believes behind the Travelex ransomware attack was caused by Pulse VPN and Hong Kong Pwc Darklab blog also disclosed two HK companies were compromised because of the same vulnerability.

(cisp-id:8414) Aug 3, 2020

DOD, FBI, DHS release info on malware used in Chinese government-led hacking campaigns.

The Chinese government has been using malware, referred to as Taidoor, to target government agencies, entities in the private sector, and think tanks since 2008, according to a joint announcement from DOD, DHS, and the FBI. The Chinese Communist Party has been using the malware, in conjunction with proxy servers, “to maintain a presence on victim networks and to further network exploitation,” according to the U.S. government’s MAR. Cyber Command has been uploading malware samples to VirusTotal since 2018 in an effort to help the private sector better protect against foreign adversaries. But it appeared to be the first time in the program’s approximately two-year history that the Pentagon has chosen to identify malware that looks to be Chinese in origin. It wasn’t immediately clear if Taidoor was being used in any recent or ongoing espionage campaigns from China.

https://www.cyberscoop.com/taidoor-malware-report-china-cisa-dod-fbi/

https://us-cert.cisa.gov/ncas/analysis-reports/ar20-216a

(cisp-id:8417) Jul 30, 2020

45 devices won't be patched with vulnerable despite live proof-of-concept code.

The vuln was revealed publicly in June by Trend Micro's Zero Day Initiative (ZDI) following six months spent chivvying Netgear behind the scenes to take it seriously. Stung by pressure from infosec researchers that came to a head in June when ZDI went public, Netgear began issuing patches. It had sorted out 28 of the 79 vulnerable product lines by the end of that month. With today's revelation that 45 largely consumer and SME-grade items will never be patched, Netgear faces questions over its commitment to older product lines. Such questions have begun to be addressed in Britain by calls from government agencies for new laws forcing manufacturers to reveal devices' design lifespans at the point of purchase. Today Netgear's advisory page for the patches shows 45 devices' fix status as "none; outside security support period"

https://www.theregister.com/2020/07/30/netgear_abandons_45_routers_vuln_patching/

(cisp-id:8419) Aug 1, 2020
Confirmed: Garmin received decryptor for WastedLocker ransomware.
BleepingComputer can confirm that Garmin has received the decryption key to recover their files encrypted in the WastedLocker Ransomware attack. Employees later shared with BleepingComputer that the ransom demand was $10 million. After a four day outage, Garmin suddenly announced that they were starting to restore services, and it made us suspect that they paid the ransom to receive a decryptor. Garmin's script contains a timestamp of '07/25/2020', which indicates that the ransom was paid either on July 24th or July 25th.
As Evil Corp has been attributed as the creator of WastedLocker and was placed on the US sanctions list for using Dridex to cause more than $100 million in financial damages, paying this ransomware could lead to hefty fines from the government.
https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/confirmed-garmin-received-decryptor-for-wastedlocker-ransomware/amp/

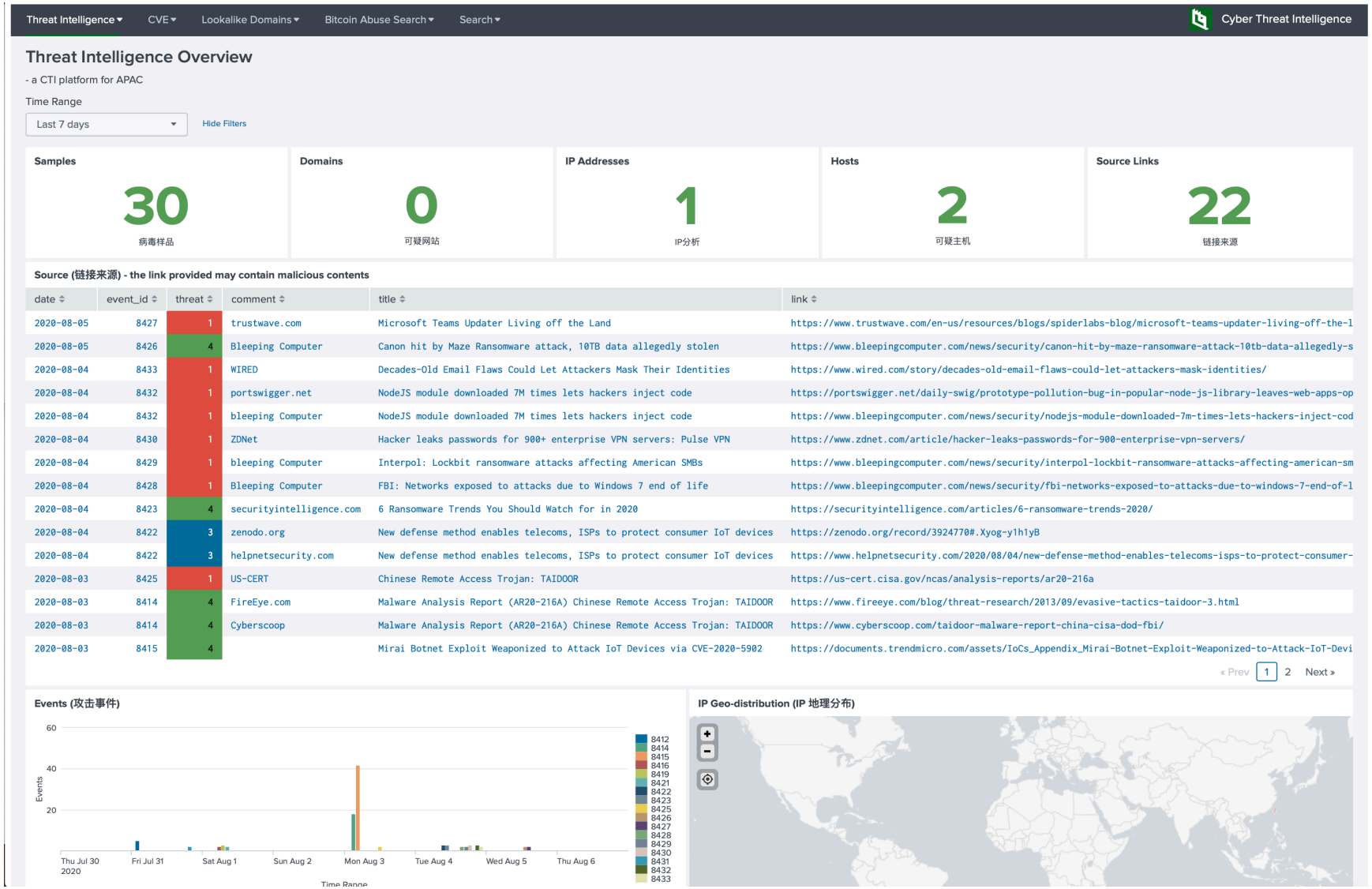
(cisp-id:8425) Aug 3, 2020
Chinese Remote Access Trojan: TAIDOOR.
FBI has high confidence that Chinese government actors are using malware variants in conjunction with proxy servers to maintain a presence on victim networks and to further network exploitation. CISA, FBI, and DoD are distributing this MAR to enable network defense and reduce exposure to Chinese government malicious cyber activity. Malicious binaries identified as a x86 and x64 version of Taidoor were submitted for analysis. Taidoor is installed on a target's system as a service dynamic link library (DLL) and is comprised of two files. The first file is a loader, which is started as a service. The loader decrypts the second file, and executes it in memory, which is the main RAT.
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-216a

(cisp-id:8429) Aug 4, 2020
Interpol: Lockbit ransomware attacks affecting American SMBs.
American medium-sized companies are actively targeted by LockBit ransomware operators according to an Interpol report on the impact the COVID-19 pandemic had on cybercrime around the world. LockBit, a human-operated Ransomware-as-a-Service (RaaS) operation that surface in September 2019 as a private operation targeting enterprises and later observed by Microsoft while targeting healthcare and critical services. Two months ago, LockBit partnered with Maze ransomware's operators to create an extortion cartel that allows them to share the same data leak platform during their operations and to exchange tactics and intelligence.
https://www.bleepingcomputer.com/news/security/interpol-lockbit-ransomware-attacks-affecting-american-smbs/

(cisp-id:8430) Aug 4, 2020
A hacker has published today a list of plaintext usernames and passwords, along with IP addresses for more than 900 Pulse Secure VPN enterprise servers. ZDNet, which obtained a copy of this list with the help of threat intelligence firm KELA, verified its authenticity with multiple sources in the cyber-security community. The security researcher noted that all the Pulse Secure VPN servers included in the list were running a firmware version vulnerable to the CVE-2019-11510 vulnerability.
https://www.zdnet.com/article/hacker-leaks-passwords-for-900-enterprise-vpn-servers/

(cisp-id:8443) Aug 2, 2020
According to data collected by Google's Project Zero security team, there have been 11 zero-day vulnerabilities exploited in the wild in the first half of the year.
https://www.zdnet.com/article/google-eleven-zero-days-detected-in-the-wild-in-the-first-half-of-2020/#ftag=RSSbaffb68

Our Threat Intelligence Platform (http://dashboard.cisp.org.hk/) is ready for public access.



Get access? please send an email to: admin@dragonadvancetech.com