Weekly Intelligence Summary

Jul 3, 2020 (TLP: WHITE)

In the spotlight this week:

- ***Microsoft*** releases emergency security update to fix two Windows Codecs bugs ***silently***.
- ***DarkLab intelligence*** analysts ***(#HongKong-based***) detected a ***#Loki-Bot*** phishing campaign targeting the maritime and engineering sectors in Europe, Asia and the US from spoofed email addresses of legitimate organizations in Asia.
- ***Trustwave SpiderLabs*** has identified an executable file displaying highly unusual behaviour and sending system information to a suspicious Chinese domain. (Definitely a shitty devs and bad intention ***#Spyware***, but can't agree it's an act of ***#APT***)
- ***US Cyber Command*** said today that foreign state-sponsored hacking groups are likely to exploit a major security bug disclosed today in PAN-OS. ***#PaloAlto***
- Hacking group, "***Korean Hackers***" and "***Team Johnwick***", breach ***E27***, want "donation" to reveal vulnerabilities.

(cisp-id:8220) Jul 1, 2020
Microsoft releases emergency security update to fix two bugs in Windows codecs
Security updates have been silently deployed to customers on Tuesday through the Windows Store app. Tracked as CVE-2020-1425 & CVE-2020-1457, the two bugs only impact Windows 10 and Windows Server 2019 distributions. In security advisories published today, Microsoft said the two security flaws can be exploited with the help of a specially crafted image file. The two bugs, built-in Windows Codecs Library -- described as two remote code execution (RCE) vulnerabilities -- received patches earlier today. The OS maker said it learned of the bugs after a report from Trend Micro's Zero Day Initiative, a program that intermediates communications between security researchers and larger companies.
https://www.zdnet.com/article/microsoft-releases-emergency-security-update-to-fix-two-bugs-in-windows-codecs/#ftag=RSSbaffb68

(cisp-id:8233) Jun 30, 2020
Loki Bot campaign targets maritime industry
DarkLab intelligence analysts detected a Loki Bot phishing campaign targeting the maritime and engineering sectors in Europe, Asia and the US from spoofed email addresses of legitimate organizations in Asia. The earliest phishing email detected dates back to October 2019. The 2019 email was sent from a likely compromised subdomain of an Indonesian company and contained a malicious archive (.rar) attachment purportedly pertaining to a purchase order, a common theme of spam emails. Although the campaign exploits well-known threat vectors, lack of widespread adoption of anti-spoofing technologies like SPF and DMARC, or their incorrect implementation, means that criminals can continue sending credible phishing emails apparently from legitimate domains.
https://blog.darklab.hk/2020/06/29/phishing-vessels/

(cisp-id:8231) Jun 30, 2020
GoldenSpy: Chapter Two – The Uninstaller
Trustwave SpiderLabs has identified an executable file displaying highly unusual behavior and sending system information to a suspicious Chinese domain. Discussions with our client revealed that this was part of their bank's required tax software. They informed us that upon opening operations in China, their local Chinese bank required that they install a software package called Intelligent Tax produced by the Golden Tax Department of Aisino Corporation, for paying local taxes. Trustwave SpiderLabs is still actively investigating and seeking out more telemetry on the GoldenSpy

campaign. Only in their report, Trustwave declared that the GoldenSpy campaign, as detailed in this report, has the characteristics of a coordinated Advanced Persistent Threat (APT) campaign targeting foreign companies operating in China. During their analysis, they found that the GoldenSpy threat actors followed our removal recommendations step by step with their uninstaller.
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-two-the-uninstaller/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-golden-tax-department-and-the-emergence-of-goldenspy-malware/

(cisp-id:8224) Jun 30, 2020
US Cyber Command says foreign hackers will most likely exploit new PAN-OS security bug
US Cyber Command said today that foreign state-sponsored hacking groups are likely to exploit a major security bug disclosed today in PAN-OS, the operating system running on firewalls and enterprise VPN appliances from Palo Alto Networks. In a tweet. US Cyber Command said: "Please patch all devices affected by CVE-2020-2021 immediately, especially if SAML is in use." They appreciate proactive response to this vulnerability.
https://www.zdnet.com/article/us-cyber-command-says-foreign-hackers-will-most-likely-exploit-new-pan-os-security-bug/#ftag=RSSbaffb68

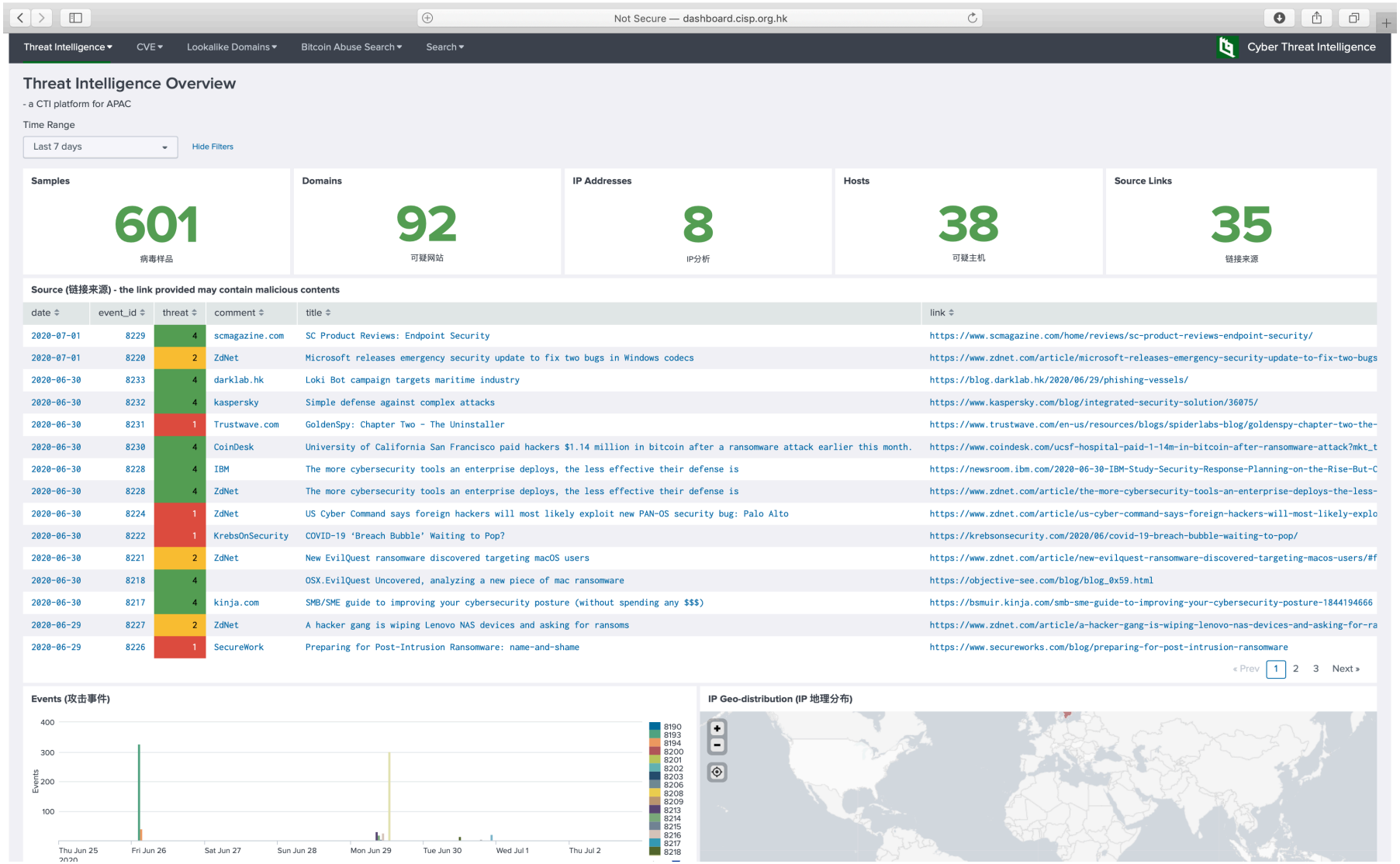
(cisp-id:8227) Jun 29, 2020
A hacker gang is wiping Lenovo NAS devices and asking for ransoms
A hacker group going by the name of 'Cl0ud SecuritY' is breaking into old LenovoEMC (formerly Iomega) network-attached storage (NAS) devices, wiping files, and leaving ransom notes behind asking owners to pay between $200 and $275 to get their data back. Attacks appear to have targeted only LenovoEMC/Iomega NAS devices that are exposing their management interface on the internet without a password. ZDNet was able to identify around 1,000 such devices using a Shodan search.
https://www.zdnet.com/article/a-hacker-gang-is-wiping-lenovo-nas-devices-and-asking-for-ransoms/

(cisp-id:8226) Jun 29, 2020
Preparing for Post-Intrusion Ransomware
Since 2015, Secureworks® Counter Threat Unit™ (CTU) researchers have observed a massive increase in the number and impact of post-intrusion ransomware incidents. In these attacks, (1) a threat actor gains access to a compromised network, (2) moves laterally to other systems and networks, (3) locates the critical business assets, and then (4) chooses a time (which could be days or months after initial access) to deploy ransomware that encrypts the victim’s files. Around the end of 2019, criminals realized they could gain additional leverage by stealing data before encrypting it and then threatening the victim with public disclosure.
https://www.secureworks.com/blog/preparing-for-post-intrusion-ransomware

(cisp-id:8200) Jun 26, 2020
Hackers breach E27, want "donation" to reveal vulnerabilities
Asian media firm E27 has been hacked, and attackers ask for a small "donation" to provide information on the vulnerabilities used in the attack. In an email notification to their members sent today and shared with BleepingComputer by Cyble, E27 CEO Mohan Belani explained that they were victims of a "malicious cyber attack". This cyberattack was conducted by a hacking group identifying themselves as "Korean Hackers" and "Team Johnwick".
https://www.bleepingcomputer.com/news/security/hackers-breach-e27-want-donation-to-reveal-vulnerabilities/

(cisp-id:8242) Jul 1, 2020
Ransomware Gangs Don’t Need PR Help
https://krebsonsecurity.com/2020/07/ransomware-gangs-dont-need-pr-help/

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



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