Weekly Intelligence Summary

Oct 2, 2020 (TLP: WHITE)

In the spotlight this week:

- ***QNAP*** urged customers last week to update the firmware and apps installed on their network-attached storage (NAS) devices to avoid infections with a new strain of ransomware named ***AgeLocker***. Last week, QNAP said it identified two sources of how AgeLocker gains access to QNAP devices.
- ***It's not the ships! It's the shore-based networks***. Security analyst Munro points out that it's not the ships that are usually getting attacked in the major incidents. ***Maritime industry*** groups have responded to these increasing reports of malware aboard ships by publishing two sets of IT security guidelines to address maritime security aboard ocean-bound vessels. With today's news that French shipping giant ***CMA CGM*** has been hit by a ransomware attack. Previous incidents included: (a) ***APM-Maersk*** (b) ***Mediterranean Shipping Company*** (3***) COSCO***.
- The Department of Defense and the Department of Homeland Security are calling out an unspecified "sophisticated cyber actor" for using malware to launch cyberattacks against targets in India, Kazakhstan, Kyrgyzstan, ***Malaysia***, Russia and Ukraine. The malware, which the military's Cyber Command has dubbed "***SlothfulMedia***," is an information-stealer capable of logging keystrokes of victims and modifying files.
- HHS released important updates on the Ryuk ransomware, which is suspected in the recent cyberattack at King of Prussia, Pa.-based Universal Health Systems hospital. They provided 10 things to known about #Ryuk. Here is one of them: ***Ryuk originated in North Korea and has links to Russian cybercriminal groups, according to HHS and based on reporting by CrowdStrike and FireEye which are cybersecurity firms. #LOL***
- Active since 2011 but only discovered this year, the XDSpy hacker group targeted government and private companies in Belarus, Moldova, Russia, Serbia, and Ukraine. Slovak cyber-security firm ESET has discovered a new state-sponsored hacking group (also known as an APT). Named ***XDSpy***, the group is a rarity in the cyber-security landscape as it managed to remain ***undetected for nearly nine years*** before its hacking spree was discovered earlier this year.

(cisp-id:9278) Oct 2, 2020
ESET discovers a rare APT that stayed undetected for nine years.
Active since 2011 but only discovered this year, the XDSpy hacker group targeted government and private companies in Belarus, Moldova, Russia, Serbia, and Ukraine. Slovak cyber-security firm ESET has discovered a new state-sponsored hacking group (also known as an APT). Named XDSpy, the group is a rarity in the cyber-security landscape as it managed to remain undetected for nearly nine years before its hacking spree was discovered earlier this year.
https://www.zdnet.com/article/eset-discovers-a-rare-apt-that-stayed-undetected-for-nine-years/

(cisp-id:9267) Oct 1, 2020
DOD, DHS expose hacking campaign in Russia, Ukraine, India, Malaysia.
The Department of Defense and the Department of Homeland Security are calling out an unspecified "sophisticated cyber actor" Thursday for using malware to launch cyberattacks against targets in India, Kazakhstan, Kyrgyzstan, Malaysia, Russia and Ukraine. The malware, which the military's Cyber Command has dubbed "SlothfulMedia," is an information-stealer capable of logging keystrokes of

victims and modifying files, according to an analysis shared early with CyberScoop. ***#sdvro.net*** domain registrar is named ***#Chengdu***
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-275a

(cisp-id:9287) Oct 1, 2020
HHS tells hospitals to guard against Ryuk ransomware attack: 10 things to know.
HHS released important updates on the Ryuk ransomware, which is suspected in the recent cyberattack at King of Prussia, Pa.-based Universal Health Systems hospital. Ryuk ransomware is an encryption used by individuals to lock information within an organization's computer system. They provided 10 thinks to known about. Here is one of them: 9. Ryuk originated in North Korea and has links to Russian cybercriminal groups, according to HHS and based on reporting by CrowdStrike and FireEye which are cybersecurity firms. https://www.beckershospitalreview.com/cybersecurity/hhs-tells-hospitals-to-guard-against-ryuk-ransomware-attack-10-thinks-to-know.html

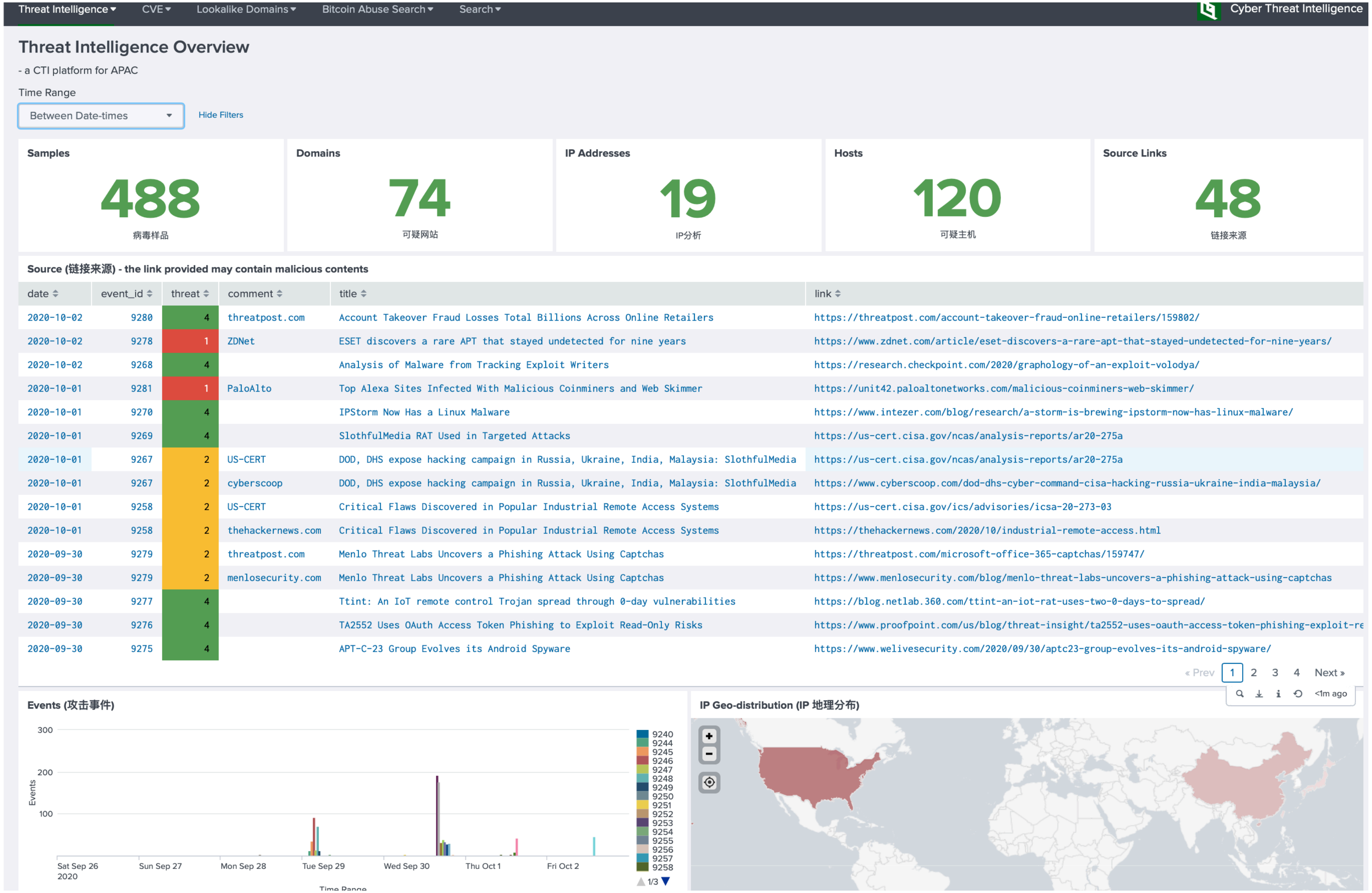
(cisp-id:9251) Sep 30, 2020
Craig Hays outlined a recent phishing attempt which went far beyond the usual spray-and-pray tactics and basic attempts to compromise a network, to become "the greatest password theft he had ever seen." The team locked the impacted account down and began to investigate the incident in order to find the root cause and any potential damage. Within minutes, several more alerts pinged their inbox. This, in itself, isn't unusual. As Hayes noted, "emails that made it through the filtering rules tended to hit a number of people at the same time." A typical phishing email comes from an email address you've never seen before. In this attack, however, all of the phishing links were sent as replies to emails in the compromised account's mailbox. This gave every email an inherited sense of trust.
https://medium.com/swlh/phishing-with-worms-the-greatest-password-theft-ive-ever-seen-26d6ad4658f9

(cisp-id:9262) Sep 29, 2020
BLINDINGCAN - Malware Used by Lazarus.
In the previous article, we introduced one type of malware that Lazarus (also known as Hidden Cobra) uses after network intrusion. It is confirmed that this attack group uses multiple types of malware including BLINDINGCAN, which CISA recently introduced in its report. This article summarises the result of our analysis on BLINDINGCAN. The malware runs when a loader loads a DLL file. Figure 1 shows the flow of events until BLINDINGCAN runs. JPCERT/CC has confirmed that the DLL file is encoded in some samples (which requires decoding by the loader before execution).
https://blogs.jpcert.or.jp/en/2020/09/BLINDINGCAN.html

(cisp-id:9256) Sep 29, 2020
QNAP tells NAS users to update firmware to avoid new type of ransomware
QNAP urged customers last week to update the firmware and apps installed on their network-attached storage (NAS) devices to avoid infections with a new strain of ransomware named AgeLocker. Last week, QNAP said it identified two sources of how AgeLocker gains access to QNAP devices. The first is the QNAP device firmware (known as QTS), while the second is one of the default apps that come preinstalled with recent QNAP systems (named PhotoStation). Older versions of the PhotoStation app are known to contain security flaws.
https://www.zdnet.com/article/qnap-tells-nas-users-to-update-firmware-to-avoid-new-type-of-ransomware/#ftag=RSSbaffb68

(cisp-id:9257) Sep 28, 2020
All four of the world's largest shipping companies have now been hit by cyber-attacks.
With today's news that French shipping giant (a) CMA CGM has been hit by a ransomware attack. Previous incidents included: (b) APM-Maersk, (c) Mediterranean Shipping Company, (d) COSCO
https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/#ftag=RSSbaffb68

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



Threat Intelligence Overview

- a CTI platform for APAC

Time Range

Samples	Domains	IP Addresses	Hosts	Source Links
488	74	19	120	48
病毒样品	可疑网站	IP分析	可疑主机	链接来源

Source (链接来源) - the link provided may contain malicious contents

date	event_id	threat	comment	title	link
2020-10-02	9280	4	threatpost.com	Account Takeover Fraud Losses Total Billions Across Online Retailers	https://threatpost.com/account-takeover-fraud-online-retailers/159802/
2020-10-02	9278	1	ZDNet	ESET discovers a rare APT that stayed undetected for nine years	https://www.zdnet.com/article/eset-discovers-a-rare-apt-that-stayed-undetected-for-nine-years/
2020-10-02	9268	4		Analysis of Malware from Tracking Exploit Writers	https://research.checkpoint.com/2020/graphology-of-an-exploit-volodya/
2020-10-01	9281	1	PaloAlto	Top Alexa Sites Infected With Malicious Coinminers and Web Skimmer	https://unit42.paloaltonetworks.com/malicious-coinminers-web-skimmer/
2020-10-01	9270	4		IPStorm Now Has a Linux Malware	https://www.intezer.com/blog/research/a-storm-is-brewing-ipstorm-now-has-linux-malware/
2020-10-01	9269	4		SlothfulMedia RAT Used in Targeted Attacks	https://us-cert.cisa.gov/ncas/analysis-reports/ar20-275a
2020-10-01	9267	2	US-CERT	DOD, DHS expose hacking campaign in Russia, Ukraine, India, Malaysia: SlothfulMedia	https://us-cert.cisa.gov/ncas/analysis-reports/ar20-275a
2020-10-01	9267	2	cyberscoop	DOD, DHS expose hacking campaign in Russia, Ukraine, India, Malaysia: SlothfulMedia	https://www.cyberscoop.com/dod-dhs-cyber-command-cisa-hacking-russia-ukraine-india-malaysia/
2020-10-01	9258	2	US-CERT	Critical Flaws Discovered in Popular Industrial Remote Access Systems	https://us-cert.cisa.gov/ics/advisories/icsa-20-273-03
2020-10-01	9258	2	thehackernews.com	Critical Flaws Discovered in Popular Industrial Remote Access Systems	https://thehackernews.com/2020/10/industrial-remote-access.html
2020-09-30	9279	2	threatpost.com	Menlo Threat Labs Uncovers a Phishing Attack Using Captchas	https://threatpost.com/microsoft-office-365-captchas/159747/
2020-09-30	9279	2	menlosecurity.com	Menlo Threat Labs Uncovers a Phishing Attack Using Captchas	https://www.menlosecurity.com/blog/menlo-threat-labs-uncovers-a-phishing-attack-using-captchas
2020-09-30	9277	4		Ttint: An IoT remote control Trojan spread through 0-day vulnerabilities	https://blog.netlab.360.com/ttint-an-iot-rat-uses-two-0-days-to-spread/
2020-09-30	9276	4		TA2552 Uses OAuth Access Token Phishing to Exploit Read-Only Risks	https://www.proofpoint.com/us/blog/threat-insight/ta2552-uses-oauth-access-token-phishing-exploit-re
2020-09-30	9275	4		APT-C-23 Group Evolves its Android Spyware	https://www.welivesecurity.com/2020/09/30/aptc23-group-evolves-its-android-spyware/

Events (攻击事件)

IP Geo-distribution (IP 地理分布)

Get access? please send an email to: <u>admin@dragonadvancetech.com</u>