Weekly Intelligence Summary

Sep 4, 2020 (TLP: WHITE)

In the spotlight this week:

- The Iranian hackers group, which Crowdstrike believes is a contractor for the Iranian regime, has spent 2019 and 2020 hacking into corporate networks via vulnerabilities in VPNs and networking equipment, such as: ***Pulse Secure*** "Connect" enterprise VPNs (CVE-2019-11510), ***Fortinet VPN*** servers running FortiOS (CVE-2018-13379) , ***Palo Alto*** Networks "***Global Protect***" VPN servers (CVE-2019-1579), ***Citrix "ADC" servers*** and Citrix network gateways (CVE-2019-19781), ***F5 Networks BIG-IP*** load balancers (CVE-2020-5902). Those products are so familiar which I have mentioned them in the past few Summary reports.
- More than a ***dozen ISPs*** have reported DDoS attacks that targeted their DNS infrastructure. "Most of [the attacks] were ***DNS amplification*** and ***LDAP-type of attacks***. Some of the attacks took longer than 4 hours and hit close to ***300Gbit/s in volume***," NBIB said. The DDoS attacks against European ISPs all took place starting after ZDNet exposed a criminal gang engaging in DDoS extortion ***against financial institutions*** across the world, with victims like MoneyGram, YesBank India, Worldpay, PayPal, Braintree, and Venmo.
- In March 2020, Proofpoint researchers observed a phishing campaign impersonating the World Health Organization's (WHO) guidance on COVID-19 critical preparedness to deliver a new malware family that researchers have dubbed "***Sepulcher***". Operator email accounts identified in this campaign have been publicly linked to historic Chinese APT campaigns targeting the Tibetan community ***delivering ExileRAT malware***.
- Unidentified hackers are trying to exploit critical vulnerabilities in the ***router software*** made by Cisco while the networking giant scrambles to address the issues. The Department of Homeland Security's Agency encouraged users to check for "indicators of compromise' or signs of malicious cyber activity.
- A recent update to Windows 10's ***Microsoft Defender*** antivirus solution ironically allows it to download malware and other files to a Windows computer. Legitimate operating system files that can be abused for malicious purposes are known as living-off-the-land binaries or LOLBINs. This directive allows a local user to use the Microsoft Antimalware Service Command Line Utility (***MpCmdRun.exe***) to download a file from a remote location.

(cisp-id:8592) Sep 3, 2020
More than a dozen internet service providers (ISPs) across Europe have reported DDoS attacks that targeted their DNS infrastructure. Attacks lasted no longer than a day and were all eventually mitigated, but ISP services were down while the DDoS was active. NBIP, a non-profit founded by Dutch ISPs to collectively fight DDoS attacks and government wiretapping attempts, provided ZDNet with additional insights into the past week's incidents. "Multiple attacks were aimed towards routers and DNS infrastructure of Benelux based ISPs," a spokesperson said. "Most of [the attacks] were DNS amplification and LDAP-type of attacks. Some of the attacks took longer than 4 hours and hit close to 300Gbit/s in volume," NBIB said.
https://www.zdnet.com/article/european-isps-report-mysterious-wave-of-ddos-attacks/#ftag=RSSbaffb68

(cisp-id:8596) Sep 2, 2020
Microsoft Defender can ironically be used to download malware.

Legitimate operating system files that can be abused for malicious purposes are known as living-off-the-land binaries or LOLBINs. In a recent Microsoft Defender update, the command-line MpCmdRun.exe tool has been updated to include the ability to download files from a remote location. This directive allows a local user to use the Microsoft Antimalware Service Command Line Utility (MpCmdRun.exe) to download a file from a remote location.
https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-can-ironically-be-used-to-download-malware/

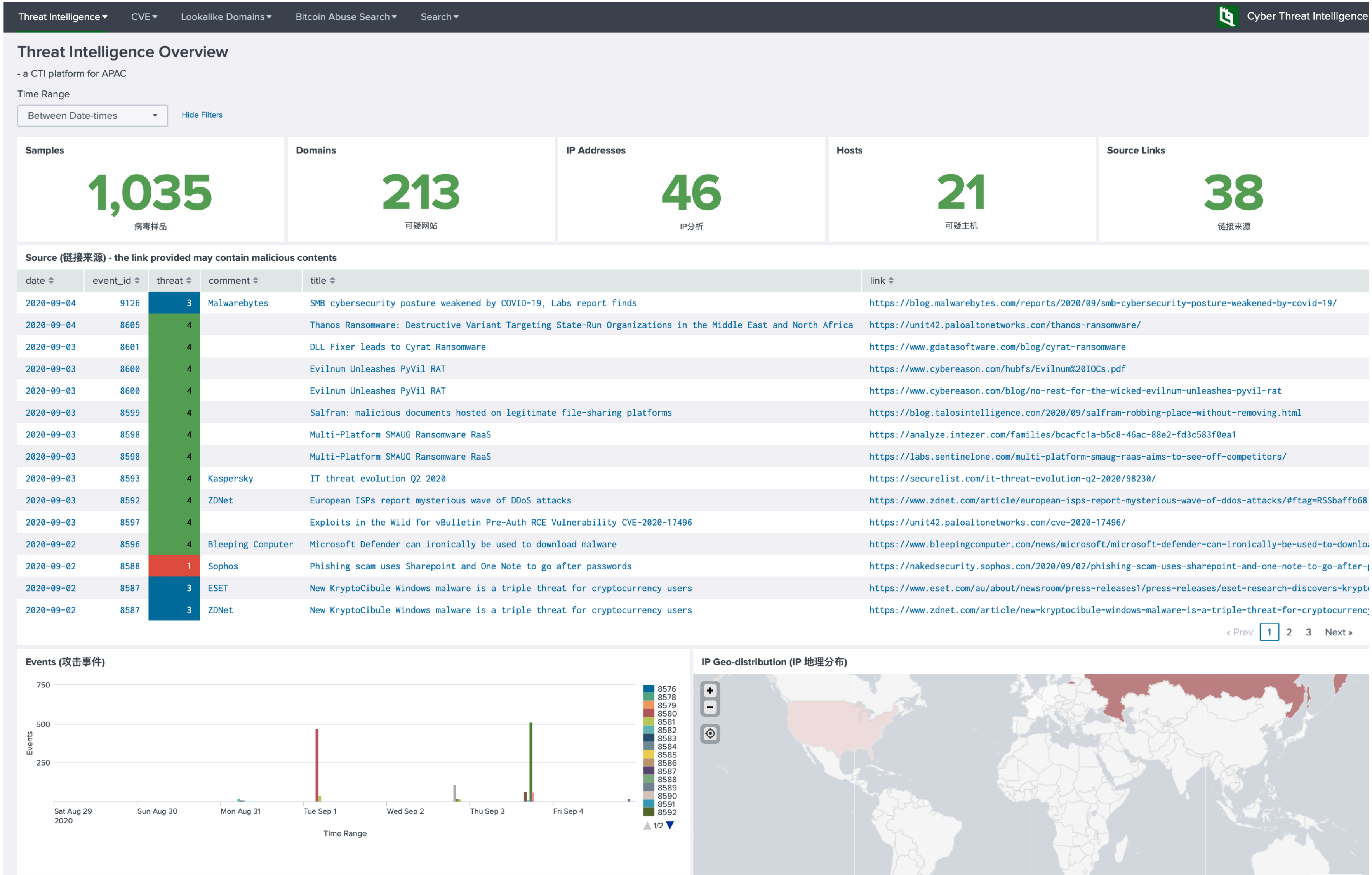
(cisp-id:8588) Sep 2, 2020
Phishing scam uses Sharepoint and One Note to go after passwords.
Sophos said: The crooks deliberately target the CEO's or the CFO's account so they can issue fake payment instructions, apparently from the most senior level. In this case, however, the crooks had clearly set out to use one compromised account as a starting point to compromise as many more as they could. The Sharepoint link you're expected to click to access the One Note file does look suspicious because there's no clear connection between the sender's company and the location of the One Note lure.
https://nakedsecurity.sophos.com/2020/09/02/phishing-scam-uses-sharepoint-and-one-note-to-go-after-passwords/

(cisp-id:8595) Sep 1, 2020
Unidentified hackers are trying to exploit critical vulnerabilities in router software made by Cisco while the networking giant scrambles to address the issues. The bugs could allow an attacker to remotely deny service to a device running the software or exhaust the memory on the device. That could destabilize “interior and exterior routing protocols” on an affected network, Cisco said in an advisory. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency encouraged users to check for “indicators of compromise' or signs of malicious cyber activity.
https://www.cyberscoop.com/cisco-ios-xr-vulnerabilities-patch/

(cisp-id:8594) Sep 1, 2020
In March 2020, Proofpoint researchers observed a phishing campaign impersonating the World Health Organization's (WHO) guidance on COVID-19 critical preparedness to deliver a new malware family that researchers have dubbed “Sepulcher”. This campaign targeted European diplomatic and legislative bodies, non-profit policy research organizations, and global organizations dealing with economic affairs. A phishing campaign from July 2020 targeting Tibetan dissidents was identified delivering the same strain of Sepulcher malware. Operator email accounts identified in this campaign have been publicly linked to historic Chinese APT campaigns targeting the Tibetan community delivering ExileRAT malware. Proofpoint researchers have attributed both campaigns to the APT actor TA413, which has previously been documented in association with ExileRAT. The usage of publicly known Tibetan-themed sender accounts to deliver Sepulcher malware demonstrates a short-term realignment of TA413's targets of interest.
https://www.proofpoint.com/us/blog/threat-insight/chinese-apt-ta413-resumes-targeting-tibet-following-covid-19-themed-economic

(cisp-id:8576) Sep 1, 2020
Iranian hackers are selling access to compromised companies on an underground forum.
One of Iran's state-sponsored hacking groups has been spotted selling access to compromised corporate networks on an underground hacking forum. The group, which Crowdstrike believes is a contractor for the Iranian regime, has spent 2019 and 2020 hacking into corporate networks via vulnerabilities in VPNs and networking equipment, such as:Pulse Secure "Connect" enterprise VPNs (CVE-2019-11510), Fortinet VPN servers running FortiOS (CVE-2018-13379) ,Palo Alto Networks "Global Protect" VPN servers (CVE-2019-1579), Citrix "ADC" servers and Citrix network gateways (CVE-2019-19781), F5 Networks BIG-IP load balancers (CVE-2020-5902).
https://www.crowdstrike.com/blog/who-is-pioneer-kitten/

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



Threat Intelligence Overview

- a CTI platform for APAC

Time Range

Samples	Domains	IP Addresses	Hosts	Source Links
1,035 病毒样品	213 可疑网站	46 IP分析	21 可疑主机	38 链接来源

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

date ⬍	event_id ⬍	threat ⬍	comment ⬍	title ⬍	link ⬍
2020-09-04	9126	3	Malwarebytes	SMB cybersecurity posture weakened by COVID-19, Labs report finds	https://blog.malwarebytes.com/reports/2020/09/smb-cybersecurity-posture-weakened-by-covid-19/
2020-09-04	8605	4		Thanos Ransomware: Destructive Variant Targeting State-Run Organizations in the Middle East and North Africa	https://unit42.paloaltonetworks.com/thanos-ransomware/
2020-09-03	8601	4		DLL Fixer leads to Cyrat Ransomware	https://www.gdatasoftware.com/blog/cyrat-ransomware
2020-09-03	8600	4		Evilnum Unleashes PyVil RAT	https://www.cybereason.com/hubfs/Evilnum%20IOCs.pdf
2020-09-03	8600	4		Evilnum Unleashes PyVil RAT	https://www.cybereason.com/blog/no-rest-for-the-wicked-evilnum-unleashes-pyvil-rat
2020-09-03	8599	4		Salfram: malicious documents hosted on legitimate file-sharing platforms	https://blog.talosintelligence.com/2020/09/salfram-robbing-place-without-removing.html
2020-09-03	8598	4		Multi-Platform SMAUG Ransomware RaaS	https://analyze.intezer.com/families/bcacfc1a-b5c8-46ac-88e2-fd3c583f0ea1
2020-09-03	8598	4		Multi-Platform SMAUG Ransomware RaaS	https://labs.sentinelone.com/multi-platform-smaug-raas-aims-to-see-off-competitors/
2020-09-03	8593	4	Kaspersky	IT threat evolution Q2 2020	https://securelist.com/it-threat-evolution-q2-2020/98230/
2020-09-03	8592	4	ZDNet	European ISPs report mysterious wave of DDoS attacks	https://www.zdnet.com/article/european-isps-report-mysterious-wave-of-ddos-attacks/#ftag=RSSbaffb68
2020-09-03	8597	4		Exploits in the Wild for vBulletin Pre-Auth RCE Vulnerability CVE-2020-17496	https://unit42.paloaltonetworks.com/cve-2020-17496/
2020-09-02	8596	4	Bleeping Computer	Microsoft Defender can ironically be used to download malware	https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-can-ironically-be-used-to-downlo
2020-09-02	8588	1	Sophos	Phishing scam uses Sharepoint and One Note to go after passwords	https://nakedsecurity.sophos.com/2020/09/02/phishing-scam-uses-sharepoint-and-one-note-to-go-after-
2020-09-02	8587	3	ESET	New KryptoCibule Windows malware is a triple threat for cryptocurrency users	https://www.eset.com/au/about/newsroom/press-releases1/press-releases/eset-research-discovers-krypt
2020-09-02	8587	3	ZDNet	New KryptoCibule Windows malware is a triple threat for cryptocurrency users	https://www.zdnet.com/article/new-kryptocibule-windows-malware-is-a-triple-threat-for-cryptocurrenc

Events (攻击事件)

IP Geo-distribution (IP 地理分布)

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