Weekly Intelligence Summary

Aug 21, 2020 (TLP: WHITE)

In the spotlight this week:

- ***Google*** has patched on Wednesday a major security ***bug impacting the Gmail and G Suite*** email servers. The bug (***DMARC/SPF policy***) could have allowed a threat actor to send spoofed emails mimicking any Gmail or G Suite customer.
- Group of crooks is taking your standard phishing attack to the next level, marketing a ***voice phishing*** service that uses a combination of one-on-one phone calls and custom ***phishing sites to steal VPN credentials*** from employees. The phishers will explain that they're calling from the employer's IT department to help troubleshoot issues with the company's virtual private networking (VPN) technology. (Source: KrebOnSecurity)
- ***Akamai's Security Intelligence Research Team*** (SIRT) has been investigating a series of recent ***DDoS attacks*** targeting businesses across multiple sectors within the last week or so. The extortion demands are similar to those used by DDoS ransom groups in the past. DATC can confirm, a ***Hong Kong domestic bank*** has been threatened in Oct 2019 for a DDoS attack. The attackers claimed they are from an actor group called "Fancy Bear".
- Emotet also has bugs. In the cyber-security industry, there's a very dangerous moral line when it comes to exploiting bugs in malware, a line many security companies won't cross. The kill-switch was in Emotet's "persistence mechanism," the part of the code that allows the malware to survive PC reboots. James Quinn finished the first version of the ***killswitch/vaccine*** that eventually became ***EmoCrash***.. (Source: Binary Defense)

(cisp-id:8535) Aug 21, 2020
ATM makers Diebold and NCR deploy fixes for 'deposit forgery' attacks.
Two of today's biggest ATM manufacturers, Diebold Nixdorf and NCR, have released software updates to address bugs that could have been exploited for "deposit forgery" attacks.
Deposit forgery bugs are rare, but two have been discovered last year and patched this year. Diebold Nixdorf patched CVE-2020-9062, an issue impacting ProCash 2100xe USB ATMs running Wincor Probase software, while NCR patched CVE-2020-10124, a bug in SelfServ ATMs running APTRA XFS software. CERT/CC says the ATMs do not encrypt, authenticate, or verify the integrity of messages sent between the ATM cash deposit boxes and the host computer.
https://www.zdnet.com/article/atm-makers-diebold-and-ncr-deploy-fixes-for-deposit-forgery-attacks/#ftag=RSSbaffb68

(cisp-id:8537) Aug 20, 2020
IBM Db2 Shared Memory Vulnerability (CVE-2020-4414).
Developers forgot to put explicit memory protections around the shared memory used by the Db2 trace facility. This allows any local users to read and write access to that memory area. In turn, this allows accessing critically sensitive data as well as the ability to change how the trace subsystem functions, resulting in a denial of service condition in the database. Needless to say, both shouldn't be possible for regular users. Please update ASAP. (Source: Trustwave)
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/ibm-db2-shared-memory-vulnerability-cve-2020-4414/

(cisp-id:8536) Aug 20, 2020
Google fixes major Gmail bug seven hours after exploit details go public.
Due to missing verification when configuring mail routes, both Gmail's and any G Suite customer's strict DMARC/SPF policy may be subverted by using G Suite's mail routing rules to relay and grant authenticity to fraudulent messages. This issue is a bug unique to Google which allows an attacker to

send mail as any other user or G Suite customer while still passing even the most restrictive SPF and DMARC rules.
https://ezh.es/blog/2020/08/the-confused-mailman-sending-spf-and-dmarc-passing-mail-as-any-gmail-or-g-suite-customer/

(cisp-id:8519) Aug 20, 2020
Voice Phishers Targeting Corporate VPNs.
Group of crooks is taking your standard phishing attack to the next level, marketing a voice phishing service that uses a combination of one-on-one phone calls and custom phishing sites to steal VPN credentials from employees. This hybrid phishing gang has a remarkably high success rate, and operates primarily through paid requests or “bounties,” where customers seeking access to specific companies or accounts can hire them to target employees working remotely at home.
https://krebsonsecurity.com/2020/08/voice-phishers-targeting-corporate-vpns/

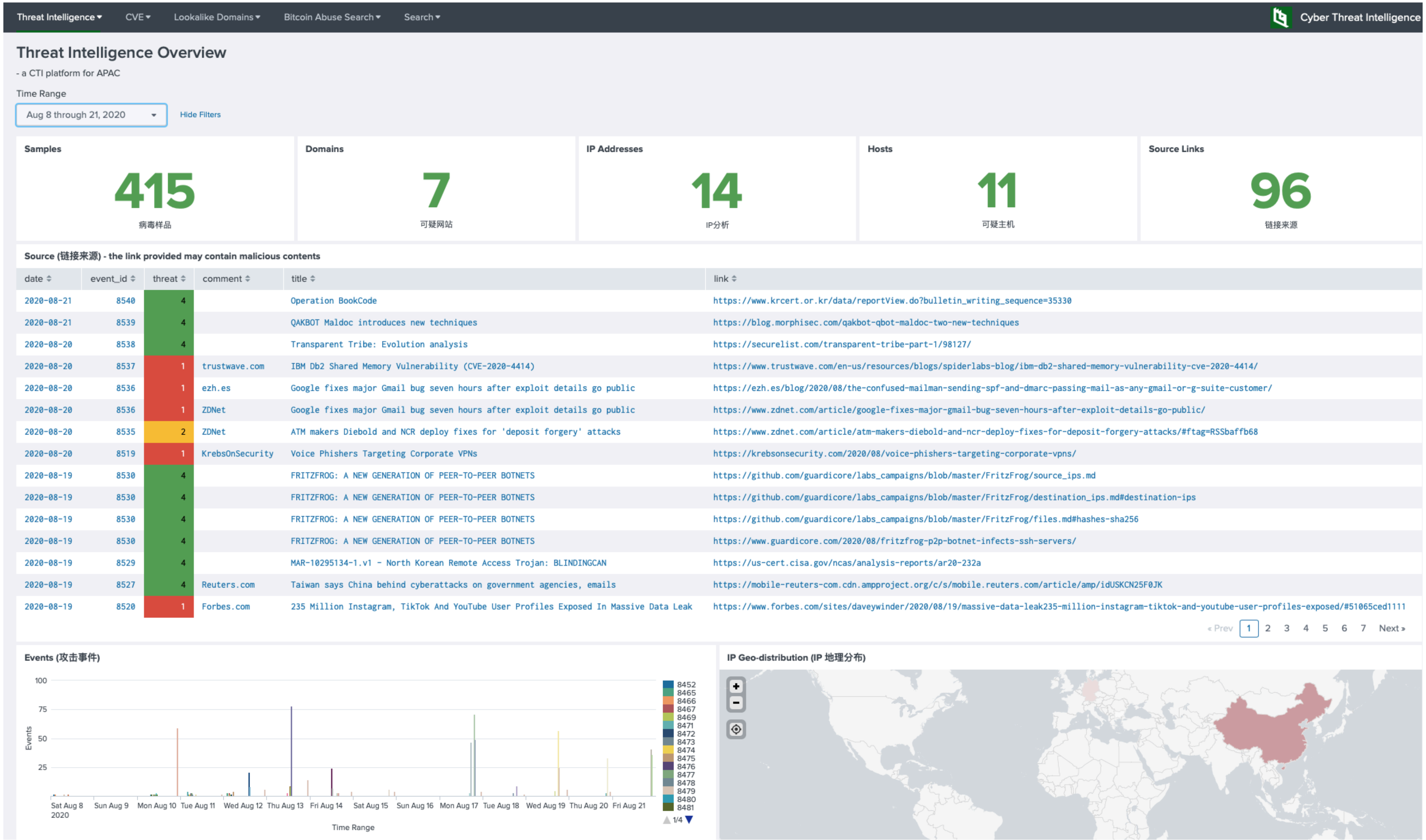
(cisp-id:8517) Aug 19, 2020
CISA warns of BLINDINGCAN, a new strain of North Korean malware.
The US Cybersecurity and Infrastructure Security Agency (CISA) has published a security alert today containing details about a new strain of malware that was seen this year deployed by North Korean government hackers. This new malware was spotted in attacks that targeted US and foreign companies active in the military defense and aerospace sectors, sources in the infosec community have told ZDNet, with the attacks being documented in reports from McAfee (Operation North Star) and ClearSky (Operation DreamJob).
https://www.zdnet.com/article/cisa-warns-of-blindingcan-a-new-strain-of-north-korean-malware/#ftag=RSSbaffb68
https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a

(cisp-id:8522) Aug 17, 2020
Ransom demands return: New DDoS Extortion Threats from old actors targeting finance and retail.
Akamai's Security Intelligence Research Team (SIRT) has been investigating a series of recent DDoS attacks targeting businesses across multiple sectors within the last week or so. The extortion demands are similar to those used by DDoS ransom groups in the past.
The letters identify targeted assets at the victim's organization and promise a small "test" attack to prove the seriousness of the situation.
https://blogs.akamai.com/sitr/2020/08/ransom-demands-return-new-ddos-extortion-threats-from-old-actors-targeting-finance-and-retail.html

(cisp-id:8515) Aug 14, 2020
Yesterday, SANS released the indicators of compromise (IOCs) for their phishing attack so that other organizations can make sure they were not affected. According to SANS, the initial attack started with a phishing email pretending to be a file shared by a SANS SharePoint service. The file pretending to be shared was called "Copy of July Bonus 24JUL2020.xls," and the email prompted the user to click on the 'Open' button to access the file. When clicked on, the button would open the default browser to "https://officei6zq49rv2p5a4xbq8ge41f1enjjczo.s3.us-east-2.amazonaws[.]com/index.html," which would immediately prompt the user to enter their ***Office 365 credentials***.
https://www.sans.org/blog/sans-data-incident-2020-indicators-of-compromise/
https://www.bleepingcomputer.com/news/security/sans-shares-details-on-attack-that-led-to-their-data-breach/

(cisp-id:85012) Aug 14, 2020
The fact that James Quinn, an analyst of Binary Defense, discovered the bug was no accident. While trawling through the daily Emotet updates in February, Quinn spotted a change in the Emotet code -- in one of the recent payloads the Emotet botnet was mass-spamming across the internet.
https://www.binarydefense.com/emocrash-exploiting-a-vulnerability-in-emotet-malware-for-defense/

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



Threat Intelligence Overview

- a CTI platform for APAC

Time Range

Aug 8 through 21, 2020

Samples	Domains	IP Addresses	Hosts	Source Links
415 病毒样品	7 可疑网站	14 IP分析	11 可疑主机	96 链接来源

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

date	event_id	threat	comment	title	link
2020-08-21	8540	4		Operation BookCode	https://www.krcert.or.kr/data/reportView.do?bulletin_writing_sequence=35330
2020-08-21	8539	4		QAKBOT Maldoc introduces new techniques	https://blog.morphisec.com/qakbot-qbot-maldoc-two-new-techniques
2020-08-20	8538	4		Transparent Tribe: Evolution analysis	https://securelist.com/transparent-tribe-part-1/98127/
2020-08-20	8537	1	trustwave.com	IBM Db2 Shared Memory Vulnerability (CVE-2020-4414)	https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/ibm-db2-shared-memory-vulnerability-cve-2020-4414/
2020-08-20	8536	1	ezh.es	Google fixes major Gmail bug seven hours after exploit details go public	https://ezh.es/blog/2020/08/the-confused-mailman-sending-spf-and-dmarc-passing-mail-as-any-gmail-or-g-suite-customer/
2020-08-20	8536	1	ZDNet	Google fixes major Gmail bug seven hours after exploit details go public	https://www.zdnet.com/article/google-fixes-major-gmail-bug-seven-hours-after-exploit-details-go-public/
2020-08-20	8535	2	ZDNet	ATM makers Diebold and NCR deploy fixes for 'deposit forgery' attacks	https://www.zdnet.com/article/atm-makers-diebold-and-ncr-deploy-fixes-for-deposit-forgery-attacks/#ftag=RSSbaffb68
2020-08-20	8519	1	KrebsOnSecurity	Voice Phishers Targeting Corporate VPNs	https://krebsonsecurity.com/2020/08/voice-phishers-targeting-corporate-vpns/
2020-08-19	8530	4		FRITZFROG: A NEW GENERATION OF PEER-TO-PEER BOTNETS	https://github.com/guardicore/labs_campaigns/blob/master/FritzFrog/source_ips.md
2020-08-19	8530	4		FRITZFROG: A NEW GENERATION OF PEER-TO-PEER BOTNETS	https://github.com/guardicore/labs_campaigns/blob/master/FritzFrog/destination_ips.md#destination-ips
2020-08-19	8530	4		FRITZFROG: A NEW GENERATION OF PEER-TO-PEER BOTNETS	https://github.com/guardicore/labs_campaigns/blob/master/FritzFrog/files.md#hashes-sha256
2020-08-19	8530	4		FRITZFROG: A NEW GENERATION OF PEER-TO-PEER BOTNETS	https://www.guardicore.com/2020/08/fritzfrog-p2p-botnet-infects-ssh-servers/
2020-08-19	8529	4		MAR-10295134-1.v1 – North Korean Remote Access Trojan: BLINDINGCAN	https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a
2020-08-19	8527	4	Reuters.com	Taiwan says China behind cyberattacks on government agencies, emails	https://mobile-reuters-com.cdn.ampproject.org/c/s/mobile.reuters.com/article/amp/idUSKCN25F0JK
2020-08-19	8520	1	Forbes.com	235 Million Instagram, TikTok And YouTube User Profiles Exposed In Massive Data Leak	https://www.forbes.com/sites/daveywinder/2020/08/19/massive-data-leak235-million-instagram-tiktok-and-youtube-user-profiles-exposed/#51065ced1111

Events (攻击事件)

IP Geo-distribution (IP 地理分布)

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