Weekly Intelligence Summary

Sep 18, 2020 (TLP: WHITE)

In the spotlight this week:

- Researchers at Dutch cybersecurity company ***Secura*** released on Monday a POC exploit for a vulnerability in the ***Netlogon protocol*** that Microsoft employs to authenticate users within a domain. The vulnerability could allow "an attacker with a foothold on your internal network to essentially become [domain administrator] with one click," as Secura analysts put it. Rob Joyce, a longtime National Security Agency official, called the Netlogon exploit "powerful," summing up its ***ease-of-use as "no fuss, no muss***."
- Financial Technology, or ***FinTech***, comprises 'computer programs and other technology used to support or enable banking and financial services'. The first ***ATM*** was opened in 1967. Since then, Fintech has evolved significantly to ***online banking*** and other platforms that facilitate the transfer and lending of money, making banking cheaper and more accessible for people around the globe. However, as easy as this transition has been for banks and as convenient as it has been for customers to be able to manage their money online, these developments have also been linked to an increase in fraud worldwide. Threat actors are easier to conduct ***'bank loading' fraud*** – a method in which illegal funds are transferred through online banking applications.
- ***Lucifer*** is a Windows crypto miner and DDOS hybrid malware. ***CheckPoint*** found evidence that the attackers behind this campaign started their operations in 2018. Attacks have come from a variety of domains including manufacturing, legal, insurance and also the ***Banking Industry***. Further investigation of those strings leads CheckPoint to two campaigns, one that was discovered by ***TrendMicro*** which they called ***BlackSquid***, and another that was discovered by ***Tencent*** and called ***Rudeminer/Spreadminer***.
- Public disclosure didn't stop suspected APT hackers from targeting the Vatican. Hackers with suspected ties to a state government kept up their operations in the weeks after they were caught targeting the Vatican. **RecordedFuture** researchers called out the hacking group's focus on the Vatican and Catholic Diocese in July, after which the hackers appeared to briefly pause their activity, in a likely effort to evade detection. But within 2 weeks, the hackers, ***RedDelta***, had resumed their activities, aiming to infiltrate mail servers of the Vatican and the ***Hong Kong Catholic Diocese***, researchers said.

(cisp-id:9187) Sep 16, 2020
Fintech fraud in 2020.
The increase in innovative online banking applications – such as #Dozens and #BoBank – as well as those from high-street branches such as NatWest, there has been an increase in UK fraud. #BankLoading – the moving of illegal funds through bank transfers between the fraudster and the victim or accomplice – has become prevalent. Following the UK government's imposition of a countrywide lockdown in March 2020, many high-street banks were temporarily closed. Some UK fraudsters used this as an opportunity to increase their focus on FinTech applications such as BO bank, Revolut and Monzo. #OnlineBanking became a target for money laundering due to the ease of

downloading and verifying the apps. Cybercriminals use social media platforms, such as TikTok, to advertise their fraudulent activities which take the form of ordering a Monzo card to cash-out fund.
https://www.cyjax.com/2020/09/16/fintech-fraud-in-2020/

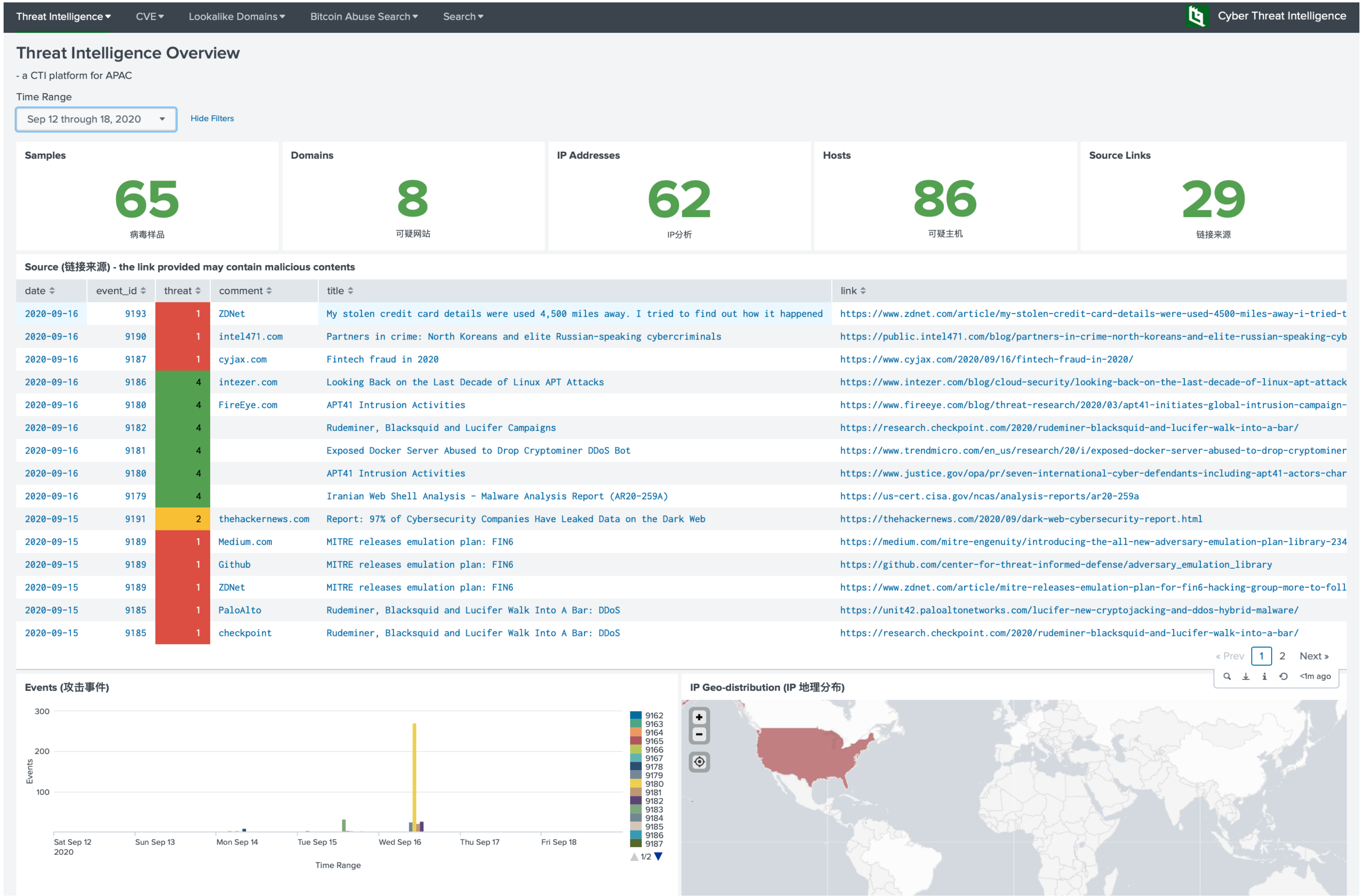
(cisp-id:9186) Sep 16, 2020
Looking Back on the Last Decade of Linux APT Attacks.
More recently there has been a noticeable increase of such discoveries. In addition to the many espionage tools that were recently uncovered (HiddenWasp, Dacls, and MessageTap to name some), older tools such as Penquin Turla have reemerged in new versions. In another high-profile example, BlackBerry recently uncovered a decade-long campaign attributed to the Winniti Group (China), where the attackers utilized multiple cross-platform RATs to target Linux, Windows, and Android platforms, Intezer said.
https://www.intezer.com/blog/cloud-security/looking-back-on-the-last-decade-of-linux-apt-attacks/

(cisp-id:9195) Sep 15, 2020
After researchers test Netlogon exploit, feds tell users to patch now or suffer later.
Researchers at Dutch cybersecurity company Secura released on Monday a POC exploit for a vulnerability in the Netlogon protocol that Microsoft employs to authenticate users within a domain. The vulnerability could allow “an attacker with a foothold on your internal network to essentially become [domain administrator] with one click,” as Secura analysts put it. That means an attacker could “impersonate any computer, including the domain controller itself, and execute remote procedure calls on their behalf.” Rob Joyce, a longtime National Security Agency official, called the Netlogon exploit “powerful,” summing up its ease-of-use as “no fuss, no muss.”
https://www.cyberscoop.com/microsoft-netlogon-exploit-secura/
https://www.secura.com/blog/zero-logon

(cisp-id:9189) Sep 15, 2020
MITRE releases emulation plan for FIN6 hacking group, more to follow.
MITRE and cyber-security industry partners have launched a new project that promises to offer free emulation plans that mimic today's biggest hacking groups in order to help train security teams to defend their networks. Named the Adversary Emulation Library, the project is the work of the MITRE Engenuity's Center for Threat-Informed Defense. The project, hosted on GitHub, aims to provide free-to-download emulation plans. Emulation plans are a collection of step-by-step guides, scripts, and commands that describe and perform malicious operations commonly observed in the playbook of a specific adversary. The goal of an emulation plan is to test network defenses and see if automated security systems or human operators detect attacks before, during, and after they've taken place — and then update security procedures to account for any lapses.
The first entry in MITRE's Adversary Emulation Library is an emulation plan for FIN6, one of today's biggest financially-motivated cybercrime groups.
https://www.zdnet.com/article/mitre-releases-emulation-plan-for-fin6-hacking-group-more-to-follow/

(cisp-id:9184) Sep 15, 2020
Back Despite Disruption: RedDelta Resumes Operations.
In the interim two-month period since previous Insikt Group reporting, RedDelta has largely remained unperturbed by the extensive public reporting on its targeting of the Vatican and other Catholic organizations. Despite taking basic operational security measures through changing the resolution status of command and control (C2) domains in the immediate aftermath of this reporting, the group’s tactics, techniques, and procedures (TTPs) remained consistent. RedDelta’s persistence is exemplified through resuming its targeting of both the Vatican and the Catholic Diocese of Hong Kong mail servers within two weeks of the report publication. More widely, there has been new activity that we attribute to the group in the form of PlugX samples
https://www.recordedfuture.com/reddelta-cyber-threat-operations/

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

Sep 12 through 18, 2020 ▾ Hide Filters

Samples	Domains	IP Addresses	Hosts	Source Links
65 病毒样品	8 可疑网站	62 IP分析	86 可疑主机	29 链接来源

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

date	event_id	threat	comment	title	link
2020-09-16	9193	1	ZDNet	My stolen credit card details were used 4,500 miles away. I tried to find out how it happened	https://www.zdnet.com/article/my-stolen-credit-card-details-were-used-4500-miles-away-i-tried-t
2020-09-16	9190	1	intel471.com	Partners in crime: North Koreans and elite Russian-speaking cybercriminals	https://public.intel471.com/blog/partners-in-crime-north-koreans-and-elite-russian-speaking-cyb
2020-09-16	9187	1	cyjax.com	Fintech fraud in 2020	https://www.cyjax.com/2020/09/16/fintech-fraud-in-2020/
2020-09-16	9186	4	intezer.com	Looking Back on the Last Decade of Linux APT Attacks	https://www.intezer.com/blog/cloud-security/looking-back-on-the-last-decade-of-linux-apt-attack
2020-09-16	9180	4	FireEye.com	APT41 Intrusion Activities	https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-
2020-09-16	9182	4		Rudeminer, Blacksquid and Lucifer Campaigns	https://research.checkpoint.com/2020/rudeminer-blacksquid-and-lucifer-walk-into-a-bar/
2020-09-16	9181	4		Exposed Docker Server Abused to Drop Cryptominer DDoS Bot	https://www.trendmicro.com/en_us/research/20/i/exposed-docker-server-abused-to-drop-cryptominer
2020-09-16	9180	4		APT41 Intrusion Activities	https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-char
2020-09-16	9179	4		Iranian Web Shell Analysis - Malware Analysis Report (AR20-259A)	https://us-cert.cisa.gov/ncas/analysis-reports/ar20-259a
2020-09-15	9191	2	thehackernews.com	Report: 97% of Cybersecurity Companies Have Leaked Data on the Dark Web	https://thehackernews.com/2020/09/dark-web-cybersecurity-report.html
2020-09-15	9189	1	Medium.com	MITRE releases emulation plan: FIN6	https://medium.com/mitre-engenuity/introducing-the-all-new-adversary-emulation-plan-library-234
2020-09-15	9189	1	Github	MITRE releases emulation plan: FIN6	https://github.com/center-for-threat-informed-defense/adversary_emulation_library
2020-09-15	9189	1	ZDNet	MITRE releases emulation plan: FIN6	https://www.zdnet.com/article/mitre-releases-emulation-plan-for-fin6-hacking-group-more-to-foll
2020-09-15	9185	1	PaloAlto	Rudeminer, Blacksquid and Lucifer Walk Into A Bar: DDoS	https://unit42.paloaltonetworks.com/lucifer-new-cryptojacking-and-ddos-hybrid-malware/
2020-09-15	9185	1	checkpoint	Rudeminer, Blacksquid and Lucifer Walk Into A Bar: DDoS	https://research.checkpoint.com/2020/rudeminer-blacksquid-and-lucifer-walk-into-a-bar/

« Prev 1 2 Next »

<1m ago

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>