Weekly Intelligence Summary

Oct 23, 2020 (TLP: WHITE)

In the spotlight this week:

- Banking injects are popular and powerful tools for performing fraud. They are usually used with banking trojans to inject malicious HTML or JavaScript code into a web page before it is redirected to a legitimate bank website. Banking trojans, like ***Lokbot***, serves as an overlay, resembling a legitimate bank login web page that requests a user to input additional confidential data such as payment card data, Social Security numbers (SSN), PINs, credit card verification codes (CVV), or additional PII. On Oct 22, a Lokibot using ***HSBC themed decoy loan email*** were found in the wild. The eml file was first uploaded from Singapore.
- US officials identified the Russian hacker group as ***Energetic Bear***, TEMP.Isotope, Berserk Bear, TeamSpy, ***Dragonfly***, ***Havex***, Crouching Yeti, and Koala. According to the technical advisory, Russian hackers used publicly known vulnerabilities to breach networking gear, pivot to internal networks, elevate privileges, and steal sensitive data.
- Named ***T-RAT***, the malware is available for ***only $45***, and its primary selling point is the ability to control infected systems via a Telegram channel. The RAT's Telegram channel supports 98 commands that, allow the RAT owner to retrieve browser passwords and cookies, navigate the victim's filesystem and search for sensitive data, deploy a keylogger, record audio via the microphone, take screenshots of the victim's desktop, take pictures via webcam, and retrieve clipboard contents.
- Earlier this summer, ***Orange Tsai*** discovered three major vulnerabilities in MobileIron's MDM solutions, which he reported to the vendor, and which the company patched in July. MDM servers of ***MobileIron,*** multiple threat actors are now exploiting these bugs to take over crucial enterprise servers and even orchestrate intrusions inside company networks. BlackArrow, published on October 13, breaks down a threat actor's attempts to hack into MobileIron MDM systems and install the ***Kaiten DDoS malware***.
- The ***WordPress*** security team has taken a rare step last week and used a lesser-known internal capability to forcibly push a security update for a popular plugin. WordPress sites running ***the Loginizer plugin*** were forcibly updated this week.

(cisp-id:9380) Oct 22, 2020
FBI, CISA: Russian hackers breached US government networks, exfiltrated data
The US government said today that a Russian state-sponsored hacking group has targeted and successfully breached US government networks. US officials identified the Russian hacker group as Energetic Bear, a codename used by the cybersecurity industry. Other names for the same group also include TEMP.Isotope, Berserk Bear, TeamSpy, Dragonfly, Havex, Crouching Yeti, and Koala. Targeted devices included Citrix access gateways (CVE-2019-19781), Microsoft Exchange email servers (CVE-2020-0688), Exim mail agents (CVE 2019-10149), and Fortinet SSL VPNs (CVE-2018-13379). To move laterally across compromised networks, CISA and the FBI said the Russian hackers used the Zerologon vulnerability in Windows Servers (CVE-2020-1472) to access and steal Windows Active Directory (AD) credentials.
https://us-cert.cisa.gov/ncas/alerts/aa20-296a

(cisp-id:9381) Oct 22, 2020
New Windows RAT can be controlled via a Telegram channel.
Named T-RAT, the malware is available for only $45, and its primary selling point is the ability to control infected systems via a Telegram channel, rather than a web-based administration panel. The RAT's Telegram channel supports 98 commands that, when typed inside the main chat window, allow the RAT owner to retrieve browser passwords and cookies, navigate the victim's filesystem and search for sensitive data, deploy a keylogger, record audio via the microphone, take screenshots of the victim's desktop, take pictures via webcam, and retrieve clipboard contents.
https://www.zdnet.com/article/new-windows-rat-can-be-controlled-via-a-telegram-channel/#ftag=RSSbaffb68

(cisp-id:9382) Oct 21, 2020
WordPress deploys forced security update for dangerous bug in popular plugin
The WordPress security team has taken a rare step last week and used a lesser-known internal capability to forcibly push a security update for a popular plugin. WordPress sites running the Loginizer plugin were forcibly updated this week to Loginizer version 1.6.4. This version contained a security fix for a dangerous SQL injection bug that could have allowed hackers to take over WordPress sites running older versions of the Loginizer plugin.
https://www.zdnet.com/article/wordpress-deploys-forced-security-update-for-dangerous-bug-in-popular-plugin/#ftag=RSSbaffb68

(cisp-id:9379) Oct 19, 2020
MobileIron enterprise MDM servers under attack from DDoS gangs, nation-states.
Earlier this summer, Orange Tsai discovered three major vulnerabilities in MobileIron's MDM solutions, which he reported to the vendor, and which the company patched in July. Tsai eventually published a detailed write-up about the three bugs in September, after he used one of the bugs to hack into Facebook's MDM server and pivot to the company's internal network as part of Facebook's bug bounty program. MDM servers of MobileIron, multiple threat actors are now exploiting these bugs to take over crucial enterprise servers and even orchestrate intrusions inside company networks.
https://www.zdnet.com/article/mobileiron-enterprise-mdm-servers-under-attack-from-ddos-gangs-nation-states/#ftag=RSSbaffb68

(cisp-id:9371) Oct 19, 2020
US charges Russian hackers behind NotPetya, KillDisk, OlympicDestroyer attacks.
The US Department of Justice has unsealed charges today against six Russian nationals believed to be members of one of Russia's elite hacking and cyberwar units — known as Sandworm. US officials said all six suspects are officers in Unit 74455 of the Russian Main Intelligence Directorate (GRU). US officials said the six conducted "destructive" cyber-attacks on behalf and under orders of the Russian government with the intent to destabilize other countries, interfere in their internal politics, and cause havoc and monetary losses. Cases include: (1) Ukrainian Government & Critical Infrastructure, (2) French Elections, (3)The NotPetya Ransomware Outbreak, (4) PyeongChang Winter Olympics, (5) PyeongChang Olympic Destroyer, (6) Novichok Poisoning Investigations, (7) Georgian Companies and Government Entities
https://securelist.com/iamtheking-and-the-slothfulmedia-malware-family/99000/

(cisp-id:9399) Oct 17, 2020
Banking trojans, like ***Lokbot***, serves as an overlay, resembling a legitimate bank login web page that requests a user to input additional confidential data such as payment card data, Social Security numbers (SSN), PINs, credit card verification codes (CVV), or additional PII. On Oct 22, a Lokibot using ***HSBC themed decoy loan email*** were found in the wild. The eml file was first uploaded from Singapore.
https://www.recordedfuture.com/banking-web-injects/

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

Threat Intelligence ▾ Vulnerability Intelligence ▾ SecOps Intelligence ▾ Toolkit ▾ Cyber Threat Intelligence

Threat Intelligence Overview

- a CTI platform for APAC

Time Range

Last 7 days ▾ Hide Filters

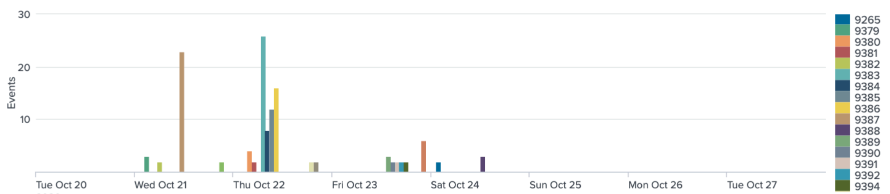
Samples	Domains	IP Addresses	Hosts	Source Links
47	7	13	3	27
病毒样品	可疑网站	IP分析	可疑主机	链接来源

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

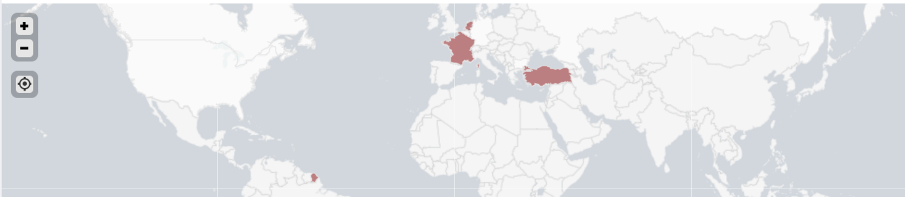
date	event_id	threat	comment	title	link
2020-10-24	9388	4	vice.com	Security News This Week: Did a Security Researcher Guess Trump's Twitter Password?	https://www.vice.com/en/article/epd4x7/twitter-trump-hack-evidence
2020-10-24	9388	4	WIRED	Security News This Week: Did a Security Researcher Guess Trump's Twitter Password?	https://www.wired.com/story/donald-trump-twitter-password-china-vulnerabilities-among-us-security-news/
2020-10-24	9265	4	cyberscoop	US Army combines fake hacks, natural disaster simulation to test municipal responses	https://www.cyberscoop.com/army-savannah-charleston-cyber-test/
2020-10-23	9398	4		New Abaddon RAT malware gets commands via Discord, has ransomware feature	https://twitter.com/malwrhunterteam/status/1319236824070500353
2020-10-23	9398	4		New Abaddon RAT malware gets commands via Discord, has ransomware feature	https://www.bleepingcomputer.com/news/security/new-rat-malware-gets-commands-via-discord-has-ransomware-feature
2020-10-23	9394	4	f-secure.com	Catching Lazarus: Threat Intelligence to Real Detection Logic - Part Two	https://labs.f-secure.com/blog/catching-lazarus-threat-intelligence-to-real-detection-logic-part-two
2020-10-23	9389	4	treasury.gov	US sanctions Russian government institution in connection with Trisis malware	https://home.treasury.gov/news/press-releases/sm1162
2020-10-23	9392	4	WIRED	How Police Can Crack Locked Phones—and Extract Information	https://www.wired.com/story/how-police-crack-locked-phones-extract-information/
2020-10-23	9391	2	WIRED	How 30 Lines of Code Blew Up a 27-Ton Generator	https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/
2020-10-23	9390	4	vice.com	Regulators and Telecoms Are Refusing to Release Data About SIM Swapping In Canada	https://www.vice.com/en/article/qjp4bx/regulators-and-telecoms-are-refusing-to-release-data-about-sim-swapping-
2020-10-23	9389	4	cyberscoop	US sanctions Russian government institution in connection with Trisis malware	https://www.cyberscoop.com/us-sanctions-russia-trisis-malware/
2020-10-22	9396	1	securityweek.com	QNAP Issues Advisory on Zerologon Vulnerability	https://www.securityweek.com/qnap-issues-advisory-zerologon-vulnerability
2020-10-22	9395	4	Kasperky	On the trail of the XMRig miner	https://securelist.com/miner-xmrig/99151/
2020-10-22	9386	4		On the trail of the XMRig miner	https://securelist.com/miner-xmrig/99151/
2020-10-22	9385	4		TrickBot Droppers and Downloaders: Detecting a Stealthy COVID-19-themed Campaign using Toolmarks	https://threatresearch.ext.hp.com/detecting-a-stealthy-trickbot-campaign/

« Prev 1 2 Next »

Events (攻击事件)



IP Geo-distribution (IP 地理分布)



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