Weekly Intelligence Summary

Oct 30, 2020 (TLP: WHITE)

In the spotlight this week:

- Attacks targeting ***CVE-2020-14882*** were observed last week, soon after a Vietnamese researcher published POC. Successful exploitation of the flaw could lead to takeover of ***Oracle WebLogic***, an advisory published by the MITRE. “The vulnerability exists due to improper input validation. A remote attacker can send a specially crafted request and execute arbitrary code on the target system. Successful exploitation of this vulnerability may result in complete compromise of vulnerable system,” Czech vulnerability company Cybersecurity Help says.
- Eastern European criminals are targeting dozens of ***U.S. hospitals*** with ransomware, and federal officials on Wednesday urged healthcare facilities to beef up preparations rapidly in case they are next. “***UNC1878*** is one of most brazen, heartless, and disruptive threat actors I’ve observed over my career,” said U.S. cyber incident response firm Mandiant. Mandiant Threat Intelligence has tracked several loader and backdoor campaigns that lead to the post-compromise deployment of ransomware (***Ryuk***), sometimes within 24 hours of initial compromise. Effective and fast detection of these campaigns is key to mitigating this threat.
- A cyber intelligence firm Hold Security to KrebsOnSecurity in March that a Swedish security giant Gunnebo Group that hackers had broken into its network and sold the access to a criminal group which specializes in deploying ransomware. In August, Gunnebo said it had successfully ***thwarted a ransomware*** attack, but this week it emerged that the intruders stole and published online tens of thousands of sensitive documents — including schematics of client ***bank vaults*** and ***surveillance systems***.
- In August and early September, ***New Zealand Stock Exchange*** (NZX), was hit, which was taken offline for several days. Also among the victims were the ***Indian bank YesBank***, PayPal, Worldpay, Braintree, and other financial companies. Another DDoS wave of bitcoin ransom demands affected a number of European ISPs; however, it’s not known for sure whether this was the work of the same group. At the end of September, financial and telecommunications companies in Hungary were rocked by a powerful DDoS attack. According to Magyar Telekom, the junk traffic came from Russia, China, and Vietnam. Source: SecureList
- The KashmirBlack botnet mainly infects popular ***CMS platforms***. It utilizes dozens of known vulnerabilities on its victims’ servers, performing millions of attacks per day on average, on thousands of victims in more than ***30 different countries*** around the world. It uses sophisticated methods to camouflage itself, stay undetected, and protect its operation. It has a complex operation managed by one C&C (Command and Control) server and uses more than 60 – mostly innocent surrogate – servers as part of its infrastructure. Source: Imperva

(cisp-id:9429) Oct 30, 2020

Oracle Warns of Critical WebLogic Flaw Exploited in Attacks.

Attacks targeting CVE-2020-14882 were observed last week, soon after a Vietnamese researcher published proof-of-concept code. Successful exploitation of the flaw could lead to takeover of Oracle WebLogic, an advisory published by the MITRE Corporation reads. “The vulnerability exists due to improper input validation. A remote attacker can send a specially crafted request and execute arbitrary code on the target system. Successful exploitation of this vulnerability may result in complete compromise of vulnerable system,” Czech vulnerability intelligence company

Cybersecurity Help says. Oracle Commends that customers apply the available patches as soon as possible, after installing the October 2020 CPU.
https://www.securityweek.com/oracle-warns-weblogic-flaw-related-exploited-vulnerability

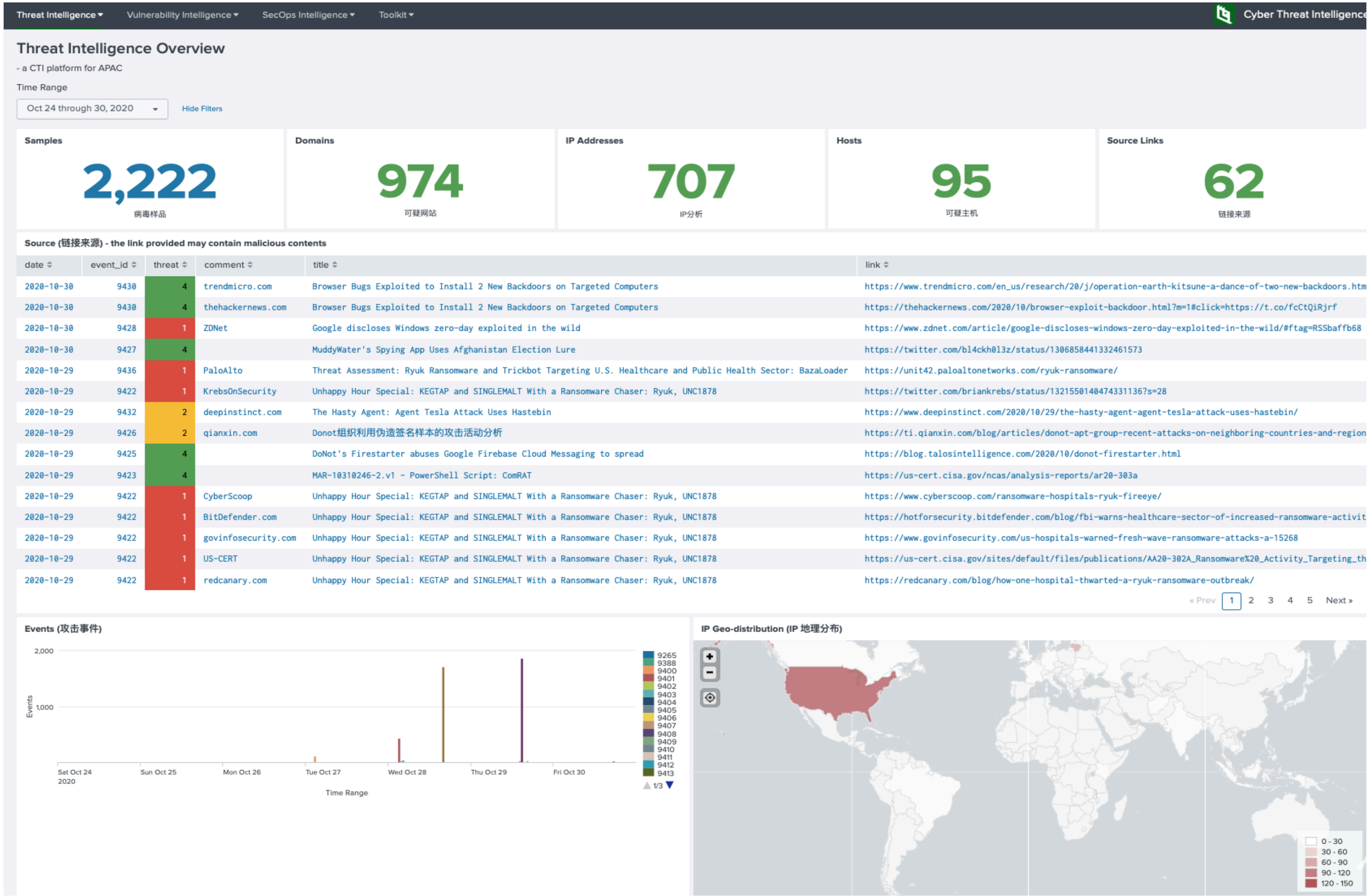
(cisp-id:9422) Oct 29, 2020
Ryuk ransomware outbreak.
Eastern European criminals are targeting dozens of U.S. hospitals with ransomware, and federal officials on Wednesday urged healthcare facilities to beef up preparations rapidly in case they are next. "UNC1878 is one of most brazen, heartless, and disruptive threat actors I've observed over my career," said Mandiant. CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats. The ransomware attacks against several facilities owned by St. Lawrence Health System in New York and an incident involving the Sky Lakes Medical Center in Oregon. The motive behind this recent rash of ransomware attacks appears to be financial gain, according to the joint alert
https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html
https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/

(cisp-id:9412) Oct 28, 2020
DDoS attacks in Q3 2020.
The Lucifer botnet, which first appeared on researchers' radar last quarter, and knows all about DDoS attacks and cryptocurrency mining, got an update, and now infects not only Windows, but also Linux devices. In DDoS attacks, the new version can use all major protocols (TCP, UDP, ICMP, HTTP) and spoof the IP address of the traffic source. In August and early September, several organizations in New Zealand were hit, including the New Zealand Stock Exchange (NZX), which was taken offline for several days. At the end of September, financial and telecommunications companies in Hungary were rocked by a powerful DDoS attack. According to Magyar Telekom, the junk traffic came from Russia, China, and Vietnam. The cybercriminals sent ransom messages of the attack is unknown.
https://securelist.com/ddos-attacks-in-q3-2020/99171/

(cisp-id:9408) Oct 28, 2020
Security Blueprints of Many Companies Leaked in Hack of Swedish Firm Gunnebo
In March 2020, KrebsOnSecurity alerted Gunnebo Group that hackers had broken into its network and sold the access to a criminal group which specializes in deploying ransomware. In August, Gunnebo said it had successfully thwarted a ransomware attack, but this week it emerged that the intruders stole and published online of sensitive documents — including schematics of client bank vaults and surveillance systems. Wis.-based cyber intelligence firm Hold SecurityThat transaction included credentials to a Remote Desktop Protocol (RDP) account apparently set up by a Gunnebo Group employee who wished to access the company's internal network remotely.
https://krebsonsecurity.com/2020/10/security-blueprints-of-many-companies-leaked-in-hack-of-swedish-firm-gunnebo/

(cisp-id:9420) Oct 26, 2020
KashmirBlack botnet behind attacks on CMSs like WordPress, Joomla, Drupal, others.
The KashmirBlack botnet mainly infects popular CMS platforms. It utilizes dozens of known vulnerabilities on its victims' servers, performing millions of attacks per day on average, on thousands of victims in more than 30 different countries around the world. Its well-designed infrastructure makes it easy to expand and add new exploits or payloads without much effort, and it uses sophisticated methods to camouflage itself, stay undetected, and protect its operation. It has a complex operation managed by one C&C (Command and Control) server and uses more than 60 – mostly innocent surrogate – servers as part of its infrastructure.
https://www.imperva.com/blog/crimeops-of-the-kashmirblack-botnet-part-i/

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



Threat Intelligence Overview

- a CTI platform for APAC

Time Range

Oct 24 through 30, 2020 ▾ Hide Filters

Samples	Domains	IP Addresses	Hosts	Source Links
2,222 病毒样品	974 可疑网站	707 IP分析	95 可疑主机	62 链接来源

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

date ⬍	event_id ⬍	threat ⬍	comment ⬍	title ⬍	link ⬍
2020-10-30	9430	4	trendmicro.com	Browser Bugs Exploited to Install 2 New Backdoors on Targeted Computers	https://www.trendmicro.com/en_us/research/20/j/operation-earth-kitsune-a-dance-of-two-new-backdoors.htm
2020-10-30	9430	4	thehackernews.com	Browser Bugs Exploited to Install 2 New Backdoors on Targeted Computers	https://thehackernews.com/2020/10/browser-exploit-backdoor.html?m=1#click=https://t.co/fcCtQiRjrf
2020-10-30	9428	1	ZDNet	Google discloses Windows zero-day exploited in the wild	https://www.zdnet.com/article/google-discloses-windows-zero-day-exploited-in-the-wild/#ftag=RSSbaffb68
2020-10-30	9427	4		MuddyWater's Spying App Uses Afghanistan Election Lure	https://twitter.com/bl4ckh0l3z/status/1306858441332461573
2020-10-29	9436	1	PaloAlto	Threat Assessment: Ryuk Ransomware and Trickbot Targeting U.S. Healthcare and Public Health Sector: BazaLoader	https://unit42.paloaltonetworks.com/ryuk-ransomware/
2020-10-29	9422	1	KrebsOnSecurity	Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser: Ryuk, UNC1878	https://twitter.com/briankrebs/status/1321550140474331136?s=28
2020-10-29	9432	2	deepinstinct.com	The Hasty Agent: Agent Tesla Attack Uses Hastebin	https://www.deepinstinct.com/2020/10/29/the-hasty-agent-agent-tesla-attack-uses-hastebin/
2020-10-29	9426	2	qianxin.com	Donot组织利用伪造签名样本的攻击活动分析	https://ti.qianxin.com/blog/articles/donot-apt-group-recent-attacks-on-neighboring-countries-and-region
2020-10-29	9425	4		DoNot's Firestarter abuses Google Firebase Cloud Messaging to spread	https://blog.talosintelligence.com/2020/10/donot-firestarter.html
2020-10-29	9423	4		MAR-10310246-2.v1 - PowerShell Script: ComRAT	https://us-cert.cisa.gov/ncas/analysis-reports/ar20-303a
2020-10-29	9422	1	CyberScoop	Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser: Ryuk, UNC1878	https://www.cyberscoop.com/ransomware-hospitals-ryuk-fireeye/
2020-10-29	9422	1	BitDefender.com	Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser: Ryuk, UNC1878	https://hotforsecurity.bitdefender.com/blog/fbi-warns-healthcare-sector-of-increased-ransomware-activit
2020-10-29	9422	1	govinfosecurity.com	Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser: Ryuk, UNC1878	https://www.govinfosecurity.com/us-hospitals-warned-fresh-wave-ransomware-attacks-a-15268
2020-10-29	9422	1	US-CERT	Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser: Ryuk, UNC1878	https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_th
2020-10-29	9422	1	redcanary.com	Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser: Ryuk, UNC1878	https://redcanary.com/blog/how-one-hospital-thwarted-a-ryuk-ransomware-outbreak/

« Prev 1 2 3 4 5 Next »

Events (攻击事件)

IP Geo-distribution (IP 地理分布)

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