Weekly Intelligence Summary

Oct 8, 2020 (TLP: WHITE)

In the spotlight this week:

- Many organizations that do hire professionals to test their network security posture unfortunately tend to focus on fixing vulnerabilities hackers could use to break in. But judging from the proliferation of help-wanted ads for ***offensive pentesters*** in the cybercrime underground, today's attackers have exactly zero trouble gaining that initial intrusion, KrebsonSecurity said.
- For almost a year, a threat actor has been using zero-day vulnerabilities to install malware on ***Tenda routers*** and build a so-called IoT botnet. Named ***Ttint***, this botnet was first detailed in a report published on Friday by Netlab. It didn't just infect devices to perform DDoS attacks, but also implemented 12 different remote access methods to the infected routers
- By combining two exploits***, checkm8 exploit*** with the ***Blackbird vulnerability***, initially developed for jailbreaking iPhones, security researchers claim they can also jailbreak Macs and MacBook devices that include Apple's latest line of ***T2 security chips***.
- The past year has been a transition period for dark web markets, as the illicit e-commerce hubs have been forced to adapt after big takedowns in 2019, according to a new ***report by Europol***. After the 2019 takedown of Deep Dot Web — a site that helped users navigate online markets for illegal drugs — ***dark web*** users began setting up other information hubs, including dark.fail and darknetlive.com, Europol say
- Kaspersky plan to present their finding of an ***UEFI malware***, which is particularly unusual—and disturbing—because it's designed to alter a target computer's Unified Extensible Firmware Interface, the firmware that is used to load the computer's operating system. Because the UEFI sits on a chip on the ***computer's motherboard*** outside of its hard drive, infections can persist even if a computer's entire hard drive is wiped or its operating system is reinstalled.
- Four ***JavaScript npm packages*** contained malicious code that collected user details and uploaded the information to a public GitHub page. The four packages where this malicious code was identified included:(a) electorn, (b) lodashsm (c) loadyaml and (d) loadym. ***#Supply-chain-attack***
- ***Emotet*** is an advanced Trojan primarily spread via phishing email attachments and then attempts to proliferate within a network by brute forcing user credentials and writing to shared drives. Emotet is difficult to combat because of its "worm-like" features that enable network-wide infections. CISA has seen increased activity involving Emotet-associated indicators.

(cisp-id:9316) Oct 8, 2020

Amid an Embarrassment of Riches, Ransom Gangs Increasingly Outsource Their Work.

"Every company gets penetration tested, whether or not they pay someone for the pleasure." Many organizations that do hire professionals to test their network security posture unfortunately tend to focus on fixing vulnerabilities hackers could use to break in. But judging from the proliferation of help-wanted ads for offensive pentesters in the cybercrime underground, today's attackers have

exactly zero trouble gaining that initial intrusion: The real challenge seems to be hiring enough people to help everyone profit from the access already gained.
https://krebsonsecurity.com/2020/10/amid-an-embarrassment-of-riches-ransom-gangs-increasingly-outsource-their-work/

(cisp-id:9314) Oct 6, 2020
Emotet is an advanced Trojan primarily spread via phishing email attachments and links that, once clicked, launch the payload. The malware then attempts to proliferate within a network by brute forcing user credentials and writing to shared drives. Emotet is difficult to combat because of its "worm-like" features that enable network-wide infections. Additionally, Emotet uses modular Dynamic Link Libraries to continuously evolve and update its capabilities. Since July 2020, CISA has seen increased activity involving Emotet-associated indicators.
https://us-cert.cisa.gov/ncas/alerts/aa20-280a

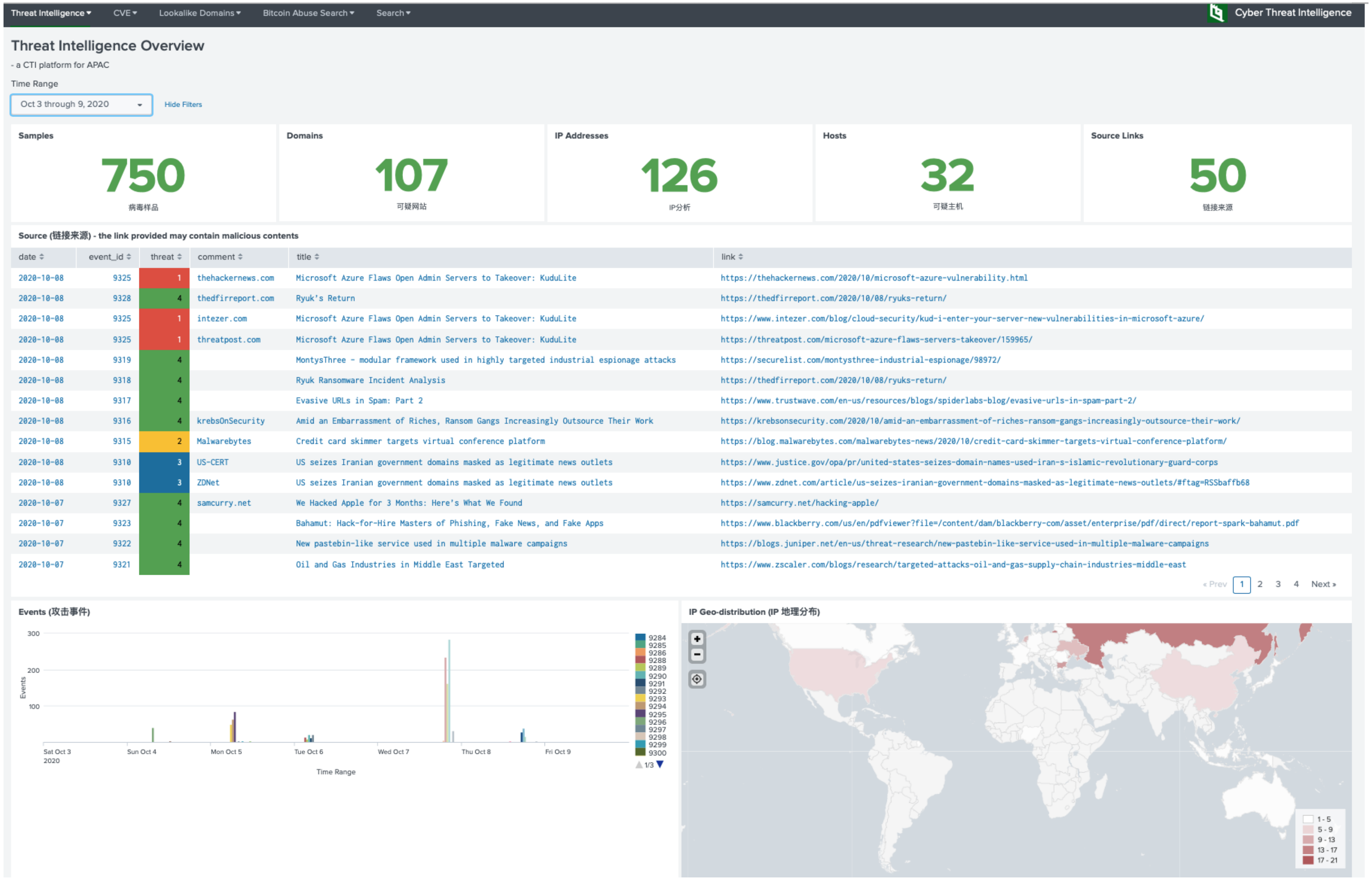
(cisp-id:9298) Oct 6, 2020
Ransomware threat surge, Ryuk attacks about 20 orgs per week.
Malware researchers monitoring ransomware threats noticed a sharp increase over the past months. At the top of the list are Maze, Ryuk, and REvil (Sodinokibi) ransomware families, according to recently published data from Check Point and IBM Security X-Force Incident Response team. Both companies observed a surge in ransomware incidents at a global level between June and September, with some threats being more active than others.
https://www.bleepingcomputer.com/news/security/ransomware-threat-surge-ryuk-attacks-about-20-orgs-per-week/

(cisp-id:9285) Oct 6, 2020
Dark web markets continue to evolve after big takedowns, Europol says.
The past year has been a transition period for dark web markets, as the illicit e-commerce hubs have been forced to adapt after big takedowns in 2019, according to a new report by Europol. After the 2019 takedown of Deep Dot Web — a site that helped users navigate online markets for illegal drugs — dark web users began setting up other information hubs, including dark.fail and darknetlive.com, Europol says. While criminals try to keep dark web markets as user-friendly as possible, they also appear to be conscious of the risks of allowing any single brand to become too big.
https://www.cyberscoop.com/dark-web-markets-europol/

(cisp-id:9305) Oct 5, 2020
Chinese hacker group spotted using a UEFI bootkit in the wild.
At an online version of the Kaspersky Security Analyst Summit this week, researchers Mark Lechtik and Igor Kuznetsov plan to present their findings about that mysterious malware sample, which they detected on the PCs of two of Kaspersky's customers earlier this year. The malware is particularly unusual—and disturbing—because it's designed to alter a target computer's Unified Extensible Firmware Interface, the firmware that is used to load the computer's operating system. Because the
https://www.wired.com/story/hacking-team-uefi-tool-spyware/

(cisp-id:9306) Oct 5, 2020
Four npm packages found uploading user details on a GitHub page.
Four JavaScript npm packages contained malicious code that collected user details and uploaded the information to a public GitHub page. The four packages where this malicious code was identified included:(a) electorn, (b) lodashsm (c) loadyaml and (d) loadym. All four packages were developed by the same user (simplelive12) and uploaded on the npm portal in August. Two packages (lodashs, loadyml) were removed by the author shortly after publication, but not before they infected some users.
https://www.zdnet.com/article/four-npm-packages-found-uploading-user-details-on-a-github-page/#ftag=RSSbaffb68

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 3 through 9, 2020 ▾   Hide Filters

Samples	Domains	IP Addresses	Hosts	Source Links
750 病毒样品	107 可疑网站	126 IP分析	32 可疑主机	50 链接来源

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

date ⇕	event_id ⇕	threat ⇕	comment ⇕	title ⇕	link ⇕
2020-10-08	9325	1	thehackernews.com	Microsoft Azure Flaws Open Admin Servers to Takeover: KuduLite	https://thehackernews.com/2020/10/microsoft-azure-vulnerability.html
2020-10-08	9328	4	thedfirreport.com	Ryuk's Return	https://thedfirreport.com/2020/10/08/ryuks-return/
2020-10-08	9325	1	intezer.com	Microsoft Azure Flaws Open Admin Servers to Takeover: KuduLite	https://www.intezer.com/blog/cloud-security/kud-i-enter-your-server-new-vulnerabilities-in-microsoft-azure/
2020-10-08	9325	1	threatpost.com	Microsoft Azure Flaws Open Admin Servers to Takeover: KuduLite	https://threatpost.com/microsoft-azure-flaws-servers-takeover/159965/
2020-10-08	9319	4		MontysThree - modular framework used in highly targeted industrial espionage attacks	https://securelist.com/montysthree-industrial-espionage/98972/
2020-10-08	9318	4		Ryuk Ransomware Incident Analysis	https://thedfirreport.com/2020/10/08/ryuks-return/
2020-10-08	9317	4		Evasive URLs in Spam: Part 2	https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/evasive-urls-in-spam-part-2/
2020-10-08	9316	4	krebsOnSecurity	Amid an Embarrassment of Riches, Ransom Gangs Increasingly Outsource Their Work	https://krebsonsecurity.com/2020/10/amid-an-embarrassment-of-riches-ransom-gangs-increasingly-outsource-their-work/
2020-10-08	9315	2	Malwarebytes	Credit card skimmer targets virtual conference platform	https://blog.malwarebytes.com/malwarebytes-news/2020/10/credit-card-skimmer-targets-virtual-conference-platform/
2020-10-08	9310	3	US-CERT	US seizes Iranian government domains masked as legitimate news outlets	https://www.justice.gov/opa/pr/united-states-seizes-domain-names-used-iran-s-islamic-revolutionary-guard-corps
2020-10-08	9310	3	ZDNet	US seizes Iranian government domains masked as legitimate news outlets	https://www.zdnet.com/article/us-seizes-iranian-government-domains-masked-as-legitimate-news-outlets/#ftag=RSSbaffb68
2020-10-07	9327	4	samcurry.net	We Hacked Apple for 3 Months: Here's What We Found	https://samcurry.net/hacking-apple/
2020-10-07	9323	4		Bahamut: Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps	https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-spark-bahamut.pdf
2020-10-07	9322	4		New pastebin-like service used in multiple malware campaigns	https://blogs.juniper.net/en-us/threat-research/new-pastebin-like-service-used-in-multiple-malware-campaigns
2020-10-07	9321	4		Oil and Gas Industries in Middle East Targeted	https://www.zscaler.com/blogs/research/targeted-attacks-oil-and-gas-supply-chain-industries-middle-east

Events (攻击事件)

IP Geo-distribution (IP 地理分布)

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