Weekly Intelligence Summary

Sep 11, 2020 (TLP: WHITE)

In the spotlight this week:

- ***TeamTNT*** is a cybercrime group that has been previously documented using several tools including ***crypto-miners*** and Amazon Web Services (AWS) credential stealing worms. TeamTNT has also been spotted using a malicious ***Docker image*** which can be found on Docker Hub to infect its victims' servers. In a recent attack observed by Intezer, TeamTNT uses a new technique by abusing ***Weave Scope***, a trusted tool which gives the user full access to their cloud environment and is integrated with Docker, Kubernetes, the Distributed Cloud Operating System (DC/OS), and AWS Elastic Compute Cloud (ECS).
- Welivesecuerity discovered that CDRThief is designed to target a ***very specific VoIP*** platform, used by ***two China-produced soft switches*** (software switches): Linknat VOS2009 and VOS3000. A soft switch is a core element of a VoIP network that provides call control, billing, and management. The primary goal of the malware is to exfiltrate various private data from a compromised soft switch, including call detail records (CDR). Its ELF binary was produced by the Go compiler with the ***debug symbols left*** unmodified, which is always helpful for the analysis. **2 samples were uploaded from HongKong on 23/7. #HongKong #Telcos need helps?**
- ***Equinix***, a multibillion-dollar data center company, is grappling with a ransomware incident affecting its internal computer systems. The California-based company, which claims nearly 10,000 clients and has offices around the world, said the incident hadn't impacted its support for customers, and that its data centers "remain fully operational."
- The ***critical Intel vulnerability*** could allow unauthenticated attackers gain escalated privileges on ***Intel vPro corporate systems***. Intel patched a critical privilege escalation vulnerability in its Active Management Technology (AMT), which is used for remote out-of-band management of PCs. The flaw can be exploited by an unauthenticated attacker on the same network, in order to gain escalated privileges. The issue (***CVE-2020-8758***), found internally by Intel employees, ranks 9.8 out of 10 on the CVSS scale, making it critical severity, according to Intel's security advisory.

(cisp-id:9155) Sep 10, 2020

Multibillion-dollar Equinix is the latest data-center firm to face ransomware incident.

Equinix, a multibillion-dollar data center company, is grappling with a ransomware incident affecting its internal computer systems, the company announced late Wednesday. The California-based company, which claims nearly 10,000 clients and has offices around the world, said the incident hadn't impacted its support for customers, and that its data centers "remain fully operational."

https://www.cyberscoop.com/equinix-ransomware-data-centers/

(cisp-id:9154) Sep 10, 2020

Who is calling? CDRThief targets Linux VoIP softswitches.

This new malware that we have discovered and named CDRThief is designed to target a very specific VoIP platform, used by two China-produced softswitches (software switches): Linknat VOS2009 and VOS3000. A softswitch is a core element of a VoIP network that provides call control, billing, and management. These softswitches are software-based solutions that run on standard Linux servers. The primary goal of the malware is to exfiltrate various private data from a compromised softswitch, including call detail records (CDR).

https://www.welivesecurity.com/2020/09/10/who-callin-cdrthief-linux-voip-softswitches/

(cisp-id:9137) Sep 8, 2020
Chinese cyber power is neck-and-neck with US, Harvard research finds.
A lot of people, Americans in particular, will think that the U.S., the U.K., France, Israel are more advanced than China when it comes to cyber power," Eric Rosenbach, the Co-Director of Harvard's Belfer Center, told CyberScoop. "Our study shows it's just not the case and that China is very sophisticated and almost at a peer level with the U.S." Overall, China's cyber power is only second to the U.S., according to the research, which was shared exclusively with CyberScoop.
https://www.cyberscoop.com/chinese-cyber-power-united-states-harvard-belfer-research/

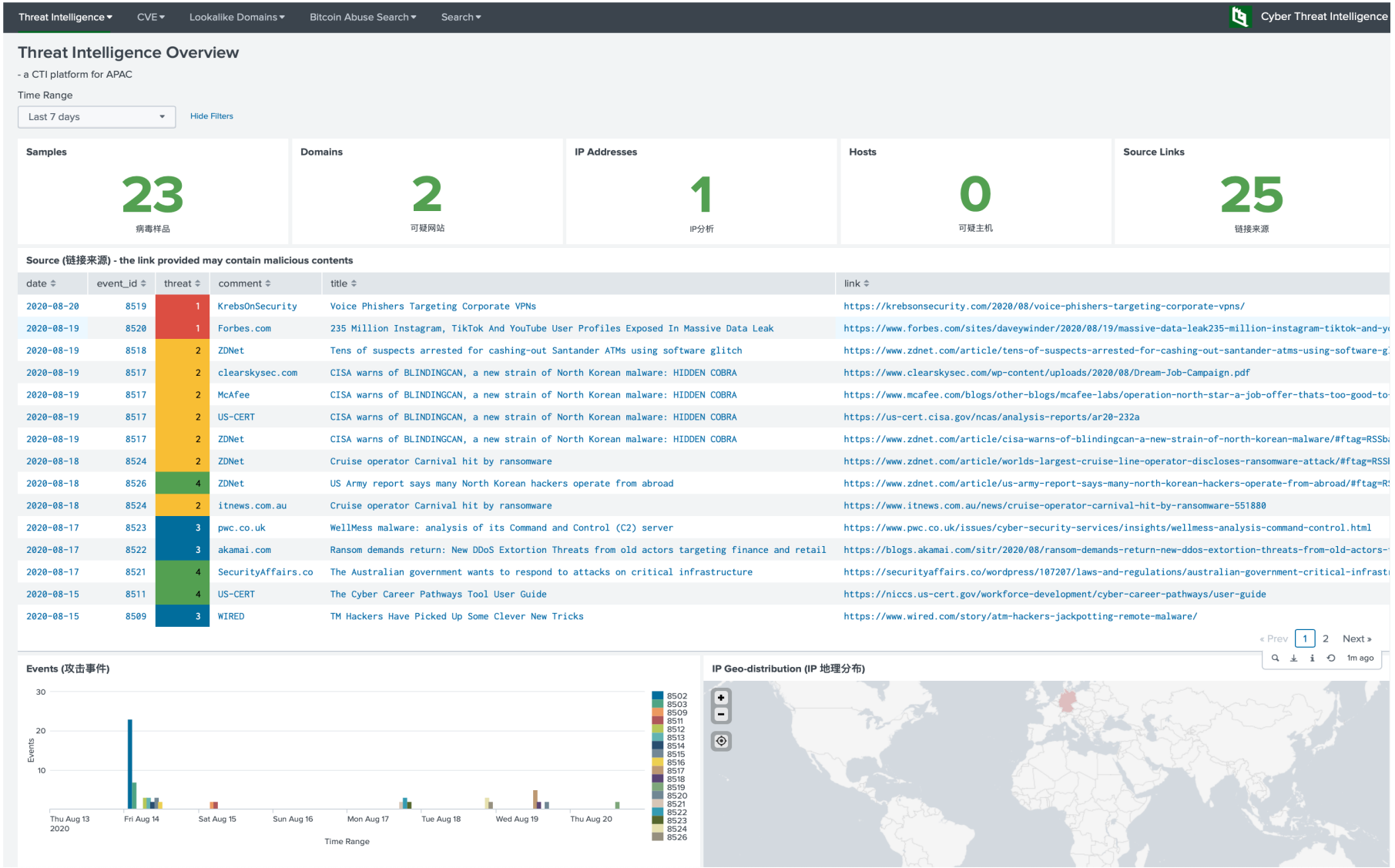
(cisp-id:9135) Sep 8, 2020
Attackers Abusing Legitimate Cloud Monitoring Tools to Conduct Cyber Attacks.
TeamTNT is a cybercrime group that targets cloud environments including Docker and Kubernetes instances. The group has been previously documented using several tools including crypto-miners and Amazon Web Services (AWS) credential stealing worms. Now the group is evolving. In a recent attack observed by Intezer, TeamTNT uses a new technique by abusing Weave Scope, a trusted tool which gives the user full access to their cloud environment and is integrated with Docker, Kubernetes, the Distributed Cloud Operating System (DC/OS), and AWS Elastic Compute Cloud (ECS).
https://www.intezer.com/blog/cloud-workload-protection/attackers-abusing-legitimate-cloud-monitoring-tools-to-conduct-cyber-attacks/

(cisp-id:9120) Sep 6, 2020
Millions of WordPress sites are being probed and attacked with recent plugin bug
Millions of WordPress sites have been probed and attacked this week, Defiant, the company behind the Wordfence web firewall said on Friday. The sudden spike in attacks happened after hackers discovered and started exploiting a zero-day vulnerability in "File Manager," a popular WordPress plugin installed on more than 700,000 sites. The zero-day was an unauthenticated file upload vulnerability that allowed an attacker to upload malicious files on a site.
https://www.zdnet.com/article/millions-of-wordpress-sites-are-being-probed-attacked-with-recent-plugin-bug/#ftag=RSSbaffb68

(cisp-id:9132) Sep 5, 2020
Visa warns of new Baka credit card JavaScript skimmer.
Visa issued a warning regarding a new JavaScript e-commerce skimmer known as Baka that will remove itself from memory after exfiltrating stolen data. The credit card stealing script was discovered by researchers with Visa's Payment Fraud Disruption (PFD) initiative in February 2020 while examining a command and control (C2) server that previously hosted an ImageID web skimming kit.
https://www.bleepingcomputer.com/news/security/visa-warns-of-new-baka-credit-card-javascript-skimmer/

(cisp-id:9143) Sep 4, 2020
Thanos Ransomware: Targeting State-Run Organizations in the Middle East and North Africa.
A strain of ransomware designed to disrupt computers' booting processes hit government-run organizations in the Middle East and North Africa in July, researchers said Friday, in the latest example of data-wiping tools being aimed at key organizations in the region. The ransomware attacks used Thanos, a type of malware that surfaced earlier this year and has gained traction on underground forums, according to analysts at Palo Alto Networks. In an increasingly popular tactic among ransomware gangs, Thanos is sold "as a service" to other hackers interested in deploying it. That can make the attacks harder to trace and allow users to develop their own custom features.
https://unit42.paloaltonetworks.com/thanos-ransomware/

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



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