Weekly Intelligence Summary

Jun 12, 2020 (TLP: WHITE)

In the spotlight this week:

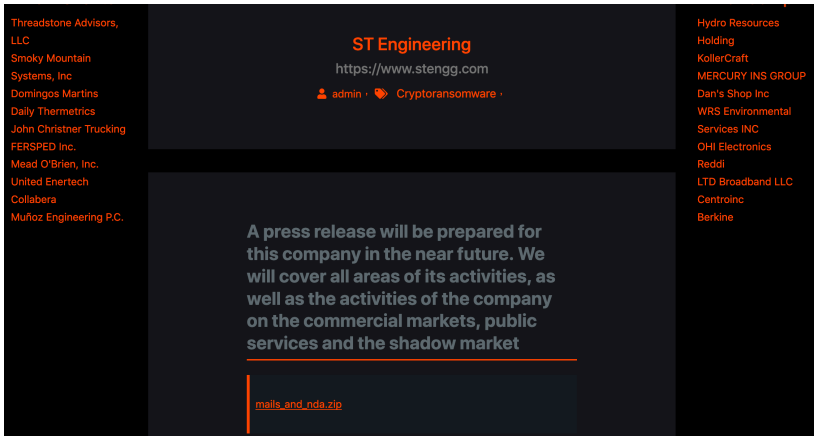
- Maze ransomware gang hit against #Singapore-based **defense contractor** ST Engineering and leaks is found in dark web. Last week Maze and Netwalker gangs also released partial leaks of two #HongKong business entities.
- A1 Telekom, the largest **internet service provider** in Austria, has admitted to a security breach this week, following a whistleblower's expose. They needed more than six months to kick the hackers off its network. Not bad, #CX needs 8-months.
- New Ransomware-as-a-Service (**RaaS**) Tool Thanos is offering for sale on exploit forum. Recorded Future found connections of a threat actor called Nosophoros who is found links to Hakbit Group.
- Crowdstrike found Internet-as-a-service (**IaaS**) API key theft has opened a vast new attack surface. Cadosecurity also identified an on-going campaign to steal AWS accounts through phishing.

(cisp-id:8097) Jun 8, 2020

Maze Ransomware Gang Hits Defense Contractor ST Engineering

The prolific Maze ransomware gang has been tied to yet more attacks, including against Singapore-based defense contractor ST Engineering. ST Engineering is a global aerospace, maritime, smart city and defense contractor with about 23,000 employees worldwide. "Upon discovering the incident, the company says it took immediate action, including disconnecting certain systems from the network, retaining third-party forensic advisors to help investigate and notifying appropriate law enforcement authorities," according to VT San Antonio Aerospace. The company also has begun informing any potentially affected customers and is continuing to conduct an investigation into the incident.

https://www.bankinfosecurity.com/maze-ransomware-gang-hits-defense-contractor-st-engineering-a-14399



Post to Maze's "news" site names ST Engineering as a victim (source: dark web)

(cisp-id:8099) Jun 19, 2020

CrowdStrike found attackers are targeting cloud service providers.

Internet-as-a-service (IaaS) API key theft has opened a vast new attack surface, giving adversaries easy access to critical controls and data assets when appropriate protection is

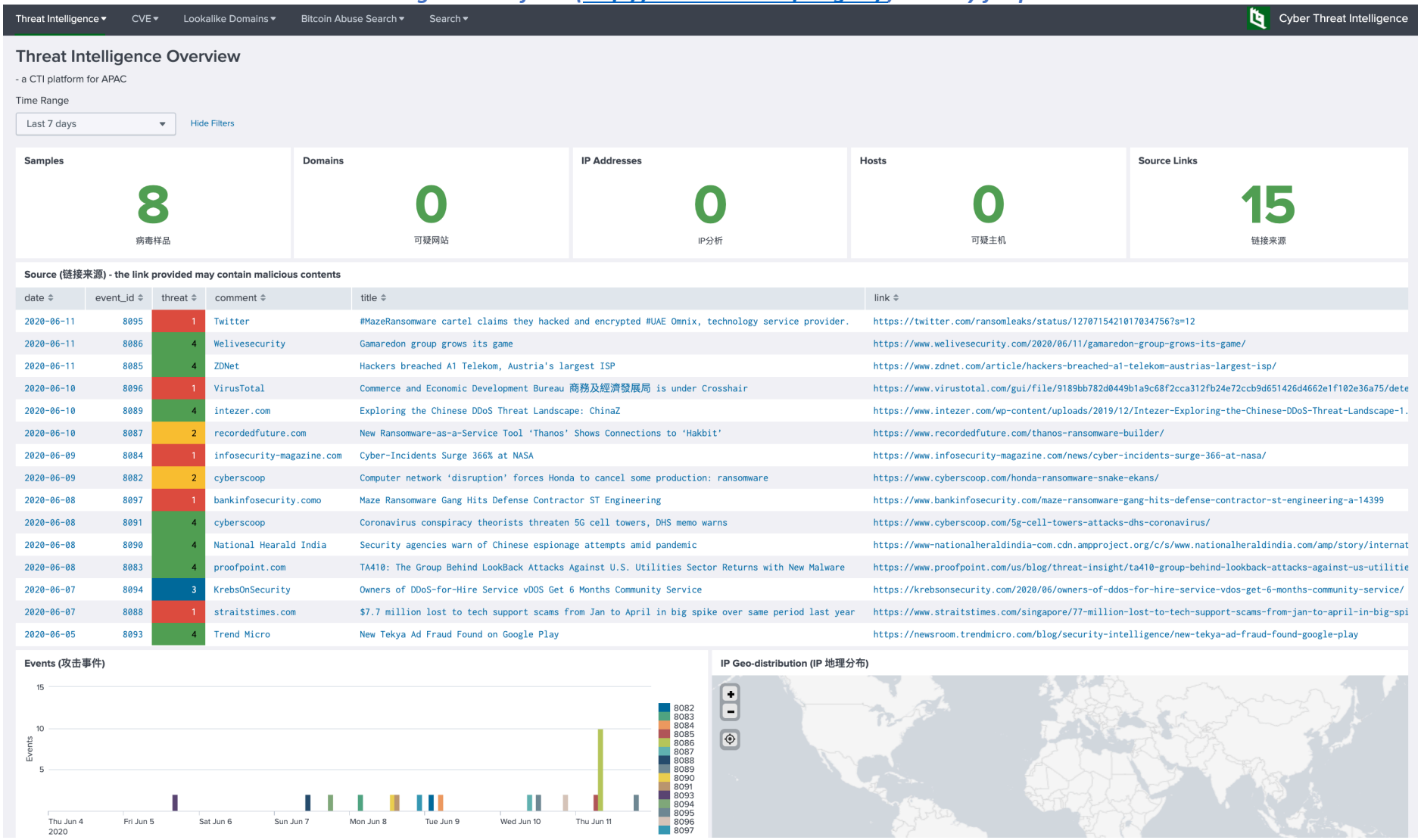
not in place. As discussed in the latest CrowdStrike Services Cyber Front Lines Report, many recent cases have involved static credentials that were not protected by multi-factor authentication (MFA), IP address-based restrictions or automatic rotation. Previously, when threat actors harvested API keys from public source code repositories, it was typically a crime of opportunity. Now, it's become targeted, and CrowdStrike has responded to multiple cases in which attackers actively sought cloud IaaS API keys in client and third-party infrastructure. In virtually all cases, these long-lived API keys were an unnecessary liability as they could have been replaced with ephemeral credentials issued through the underlying cloud infrastructure.
https://www.crowdstrike.com/blog/crowdstrike-observes-increase-in-iaas-api-key-theft/
https://www.cadosecurity.com/2020/06/11/an-ongoing-aws-phishing-campaign/

(cisp-id:8085) Jun 11, 2020
Hackers breached A1 Telekom, Austria's largest ISP.
A1 Telekom, the largest internet service provider in Austria, has admitted to a security breach this week, following a whistleblower's exposé. The company admitted to suffering a malware infection in November 2019. A1 said its security team detected the malware a month later, but that removing the infection was more problematic than it initially anticipated. A1 needed more than six months to kick the hackers off its network. Whsitleblower claims the intruders were Chinese hackers. A1, which didn't disclose the nature of the malware, didn't say if the intruders were financially focused cybercrime gang or a nation-state hacking group.
https://www.zdnet.com/article/hackers-breached-a1-telekom-austrias-largest-isp/

(cisp-id:8087) Jun 10, 2020
New Ransomware-as-a-Service Tool 'Thanos' Shows Connections to 'Hakbit'
Insikt Group uncovered a new family of ransomware for sale on Exploit Forum called Thanos, developed by a threat actor with the alias "Nosophoros." Nosophoros offered Thanos as a private ransomware builder with the ability to generate new Thanos ransomware clients based on 43 different configuration options. Recorded Future analyzed the Thanos ransomware builder to detect, understand, and exercise the breadth of functionality that the Thanos ransomware can support. The Thanos client is simple in its overall structure and functionality. It is written in C# and is straightforward to understand even with obfuscation, though it does incorporate some more advanced features such as the RIPlace technique.
https://www.recordedfuture.com/thanos-ransomware-builder/

(cisp-id:8083) Jun 8, 2020
The Group Behind LookBack Attacks Against U.S. Utilities Sector Returns with New Malware
In August 2019, Proofpoint researchers reported that LookBack malware was targeting the United States (U.S.) utilities sector between July and August 2019. Proofpoint researchers identified a new, additional malware family named FlowCloud that was also being delivered to U.S. utilities providers. Analysis found similarities between TA410 and TA429 (APT10) delivery tactics. Specifically, we have seen attachment macros that are common to both actors. TA410 campaigns detected in November 2019 included TA429 (APT10)-related infrastructure used in phishing attachment delivery macros. However, Proofpoint analysts believe that intentional reuse of well-publicized TA429 (APT10) techniques and infrastructure may be an attempt by threat actors to create a false flag.
https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new

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



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