Weekly Intelligence Summary

Dec 4, 2020 (TLP: WHITE)

In the spotlight this week:

- This summer, Red Canary Intel detected a cluster of malicious activity executing ***a .NET RAT across multiple industries***. Here's what to look out for. They've been tracking this threat since June 2020. Yellow Cockatoo has targeted a range of victims across multiple industries and company sizes, and they continue to see it, as recently as this week. Other than a tweet from June referencing a related ***PowerShell script***, ***Yellow Cockatoo*** mostly evaded public notice until November 2020, when researchers from Morphisec published a detailed overview of a threat they call Jupyter Infostealer. Jupyter Infostealer overlaps significantly with the threat they call Yellow Cockatoo.
- Eclypsium has discovered that the ***TrickBot malware now*** has functionality designed to ***inspect the UEFI/BIOS firmware*** of targeted systems. This new functionality, which we have dubbed "TrickBoot," makes use of readily available tools to check devices for well-known vulnerabilities that can allow attackers to read, write, or erase the UEFI/BIOS firmware of a device. At the time of writing, their research uncovered TrickBot performing reconnaissance for firmware vulnerabilities. This activity sets the stage for TrickBot operators to perform more active measures such as the installation of ***firmware implants and backdoors*** or the destruction (bricking) of a targeted device. It is quite possible that threat actors are already exploiting these vulnerabilities against high-value targets.
- FBI: "The ***web-based client's forwarding rules*** often do ***not sync with the desktop client***, limiting the rules' visibility to cyber security administrators." Threat actors absolutely love email auto-forwarding rules as they allow them to receive copies of all incoming emails without having to log into an account each day -- and be at risk of triggering a ***security warning for a suspicious login***. FBI officials say that the technique is still making victims in corporate environments because some companies don't forcibly sync email settings for the web-based accounts with desktop clients.

(cisp-id:9652) Dec 4, 2020

Yellow Cockatoo: Search engine redirects, in-memory remote access trojan, and more.

This summer, Red Canary Intel detected a cluster of malicious activity executing a .NET RAT across multiple industries. Here's what to look out for. Yellow Cockatoo is our name for a cluster of activity involving the execution of a .NET remote access trojan (RAT) that runs in memory and drops other payloads. Yellow Cockatoo has targeted a range of victims across multiple industries and company sizes, and we continue to see it, as recently as this week. Other than a tweet from June referencing a related PowerShell script, Yellow Cockatoo mostly evaded public notice until November 2020, when researchers from Morphisec published a detailed overview of a threat they call Jupyter Infostealer.
https://redcanary.com/blog/yellow-cockatoo/

(cisp-id:9661) Dec 3, 2020

TrickBot Offers New "TrickBoot" UEFI-Focused Functionality.

Eclypsium has discovered that the TrickBot malware now has functionality designed to inspect the UEFI/BIOS firmware of targeted systems. This new functionality, which we have dubbed "TrickBoot," makes use of readily available tools to check devices for well-known vulnerabilities that can allow attackers to read, write, or erase the UEFI/BIOS firmware of a device. At the time of writing, their research uncovered TrickBot performing reconnaissance for firmware vulnerabilities. This activity sets the stage for TrickBot operators to perform more active measures such as the installation of firmware implants and backdoors or the destruction (bricking) of a targeted device.

https://eclypsium.com/2020/12/03/trickbot-now-offers-trickboot-persist-brick-profit/

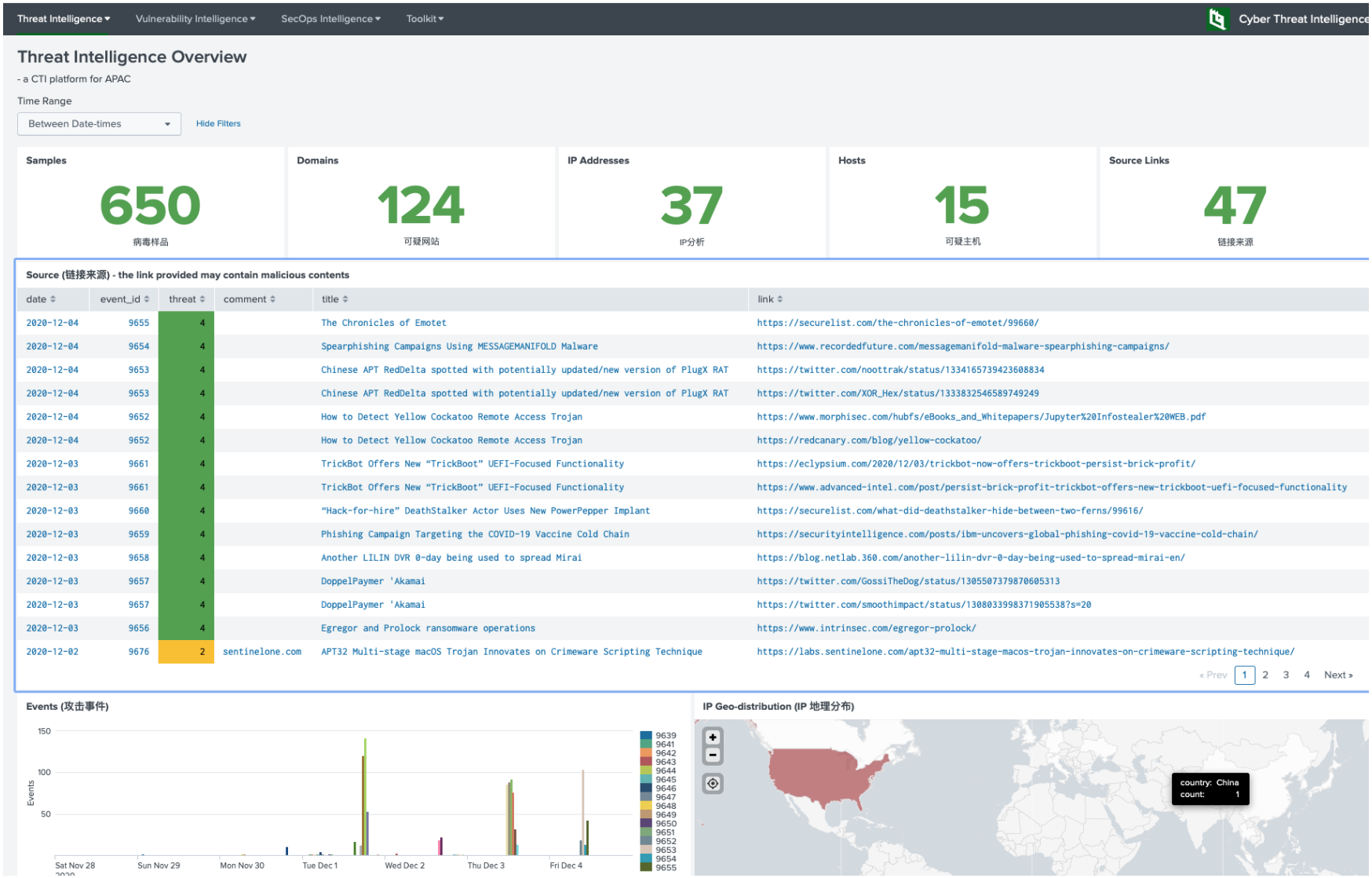
(cisp-id:9676) Dec 2, 2020
APT32 Multi-stage macOS Trojan Innovates on Crimeware Scripting Technique.
In the same week as Microsoft disclosed the Vietnamese-linked APT32 (aka “OceanLotus”, “Bismuth”, “SeaLotus”) group deploying Cryptominer software like a common crimeware adversary, researchers at Trend Micro released details of an update to an APT32 macOS backdoor that also appears to have been taking lessons from commodity malware authors. In this post, SentinelOne review some of the details in the earlier report but also add some new IoCs and observations that have not yet been mentioned. In this case, the script aggressively attempts to remove all quarantine bits and, in the event any of those fail and the malware finds itself translocated to a read-only filepath, it then undertakes a hunt for the original downloaded file via its MD5 hash and attempts to execute it from its non-translocated path on disk. The second stage payload, once dumped from the encoded base64, is a universal FAT binary containing Mach-Os for i386 and x86_64 architectures.
https://labs.sentinelone.com/apt32-multi-stage-macos-trojan-innovates-on-crimeware-scripting-technique/

(cisp-id:9672) Dec 2, 2020
Open source software security vulnerabilities exist for over four years before detection.
GitHub research suggests there is a need to reduce the time between bug detection and fixes.
GitHub launched a deep-dive into the state of open source security, comparing information gathered from the organization's dependency security features and the six package ecosystems supported on the platform. Only active repositories have been included, not including forks or 'spam' projects. The package ecosystems analyzed are Composer, Maven, npm, NuGet, PyPi, and RubyGems On average, vulnerabilities can go undetected for over four years in open source projects before disclosure. A fix is then usually available in just over a month, which GitHub said.
https://www.zdnet.com/article/open-source-software-security-vulnerabilities-exist-for-over-four-years-before-detection-study/#ftag=RSSbaffb68

(cisp-id:9646) Dec 1, 2020
Cryptocurrency miners were 'distraction technique' in APT's espionage campaigns, Microsoft says.
Cryptocurrency miners are typically associated with cybercriminal operations, not sophisticated nation state actor activity. They are not the most sophisticated type of threats, which also means that they are not among the most critical security issues that defenders address with urgency. Recent campaigns from the nation-state actor BISMUTH take advantage of the low-priority alerts coin miners cause to try and fly under the radar and establish persistence. BISMUTH, which shares similarities with OceanLotus or APT32, has been running increasingly complex cyberespionage attacks as early as 2012, using both custom and open-source tooling to target large multinational corporations, governments, financial services, educational institutions, and human and civil rights organizations. But in campaigns from July to August 2020, the group deployed Monero coin miners
https://www.zdnet.com/article/microsoft-links-vietnamese-state-hackers-to-crypto-mining-malware-campaign/#ftag=RSSbaffb68

(cisp-id:9644) Dec 1, 2020
FBI warns of email forwarding rules being abused in recent hacks.
FBI: "The web-based client's forwarding rules often do not sync with the desktop client, limiting the rules' visibility to cyber security administrators." Threat actors absolutely love email auto-forwarding rules as they allow them to receive copies of all incoming emails without having to log into an account each day -- and be at risk of triggering a security warning for a suspicious login. FBI officials say that the technique is still making victims in corporate environments because some companies don't forcibly sync email settings for the web-based accounts with desktop clients.
https://www.zdnet.com/article/fbi-warns-of-email-forwarding-rules-being-abused-in-recent-hacks/#ftag=RSSbaffb68

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



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