Cyber Threat Intelligence insights

Who knows his enemy and himself, won't fear the result of a hundred battles

Sun Tzu (544 – 496 av.JC)

Cyber-Weather

Monthly News Roundup

July

sogeti
Part of Capgemini

Weak signals for Strategic CTI

USA, Five Eyes and EU publicly shame China for Microsoft Exchange massive hack

https://therecord.media/white-house-formally-blames-chinas-ministry-of-state-security-for-microsoft-exchange_hack/
https://media.defense.gov/2021/Jul/19/2002805003/-1/-1/1/CSA_CHINESE_STATE-SPONSORED_CYBER_TTPS.PDF

On Monday, July 19, 2021, the #United States, allied international organizations (NATO and the Council of the European Union) and partner states (United Kingdom, Japan, New Zealand, Australia and Canada) issued several joint statements accusing the People's Republic of #China of massively exploiting the #Microsoft Exchange vulnerability dubbed Proxylogon. Moreover, **a joint advisory has been published by CISA, NSA and FBI with more than 50 TTPs most employed by china-backed APT groups**.

Several chinese ambassadors of the countries concerned have refuted these allegations as "unfounded" and "malicious smears". On the same day, the #DoJ (Department of Justice) made public **the indictment of four Chinese citizens charging them with unauthorized computer intrusions, theft of intellectual property, trade secrets and information related to infectious disease research**. Three of the individuals are identified as working for the #MSS (Ministry of State Security), and one is identified as working for a company suspected of acting on behalf of the MSS. These four citizens have been linked to the #APT40 group (aka Kryptonite Panda) and #APT31 (aka Judgement Panda) **the two belonging to the MSS cyber activity according to DoJ**.

Interestingly, on July 21st, the French national cybersecurity agency #ANSSI shared IoCs and a statement claiming **members of APT31 (aka Judgment Panda) are actively targeting French enterprises**. The White House statement precisely blamed this group and the APT40 one for belonging to the Chinese MSS even though we don't know at this point if these statements are linked.
As far as APT31, **the group had access to infamous NSA alleged Equation Group exploit three years before the Shadow Brokers bought this case to light**. Thus, APT31 performs cyberespionage operations leveraging #0-days. One can conjecture that Judgment Panda could have accessed and exploited the Exchange flaws.

CERT Sogeti ESEC hypothesizes that the absence of international cyberspace law and the generalization of name-and-shame could **lead to less restraint in future cyberespionage operations**. Indeed, based on the Russian model, **Chinese APT ecosystem could have more recourse to mercenary groups** (*privateers*, see the June edition of the Cyber-Weather) who would act on its behalf in return of funding. This would have the advantage of maintaining a sufficiently thick fog over their operations to avoid name-and-shame and geopolitical consequences slowing down China's desire to become a global power.

Additionnaly, **this is one of the first time the ANSSI publicly attributes a campaign to state-backed APT group targeting French interests**. This doctrinal evolution is consistent with our above hypothesis. However, and as of writing, contrary to Russia we have no indication that China could leverage eCrime ransomware operators to support their strategic goals.

USA, China, Microsoft Exchange, MSS, APT31, APT40, DoJ, ANSSI, 0-days

Weak signals for Strategic CTI

USA, Five Eyes and EU publicly shame China for Microsoft Exchange massive hack

APT31 and APT40 are respectively specialized in high-value intellectual property theft and cyberespionage operations directed to defense and government entities in Western countries.

- Intensive **reuse of same tools** (i.e : PlugX, Icefog, RoyalRoad)
- High degree of **persistence** combined to high-skilled efforts to evade detections
- Supply-chain *zero-days* exploits to increase the attack surface and the compromise potential

The generalization of ***name-and-shame*** could lead to less restraint in future Chinese cyberespionage operations. Based on the Russian model, **Chinese APT ecosystem could have more recourse to privateers groups** who would act on its behalf in return of funding.

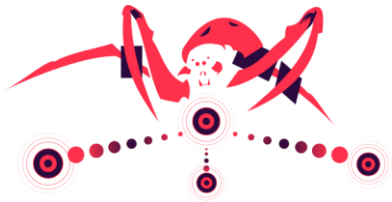
- **Be prepared** : capitalize on whitepapers, Threat Advisories and Flash-News produced by CTI Team about the Exchange hack by Chinese actors
- **Learn more about Chinese APTs** : the CTI team maintains up-to-date actors identity cards on our TIP with latest TTPs associated
- **Focus efforts** of patching/monitoring **on your VPN servers**
  - Use whitelists if possible / ban specific countries you are not interacting with
  - **Audit** the network for systems using **RDP**
- **Train your teams** to phishing and social-engineering methods, widely used by Chinese actors

USA, China, Microsoft Exchange, MSS, APT31, APT40, DoJ, ANSSI, 0-days

Kaseya hit by a Sodinokibi-backed supply-chain attack

- Alleged to be the successor of the notorious #GandCrab, #REvil (aka #Sodinokibi or #Sodin) is a ransomware-as-a-service operated by #Pinchy Spider.

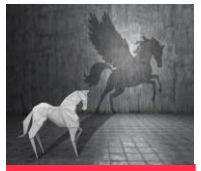
- Pinchy Spider stand on its own feet at the beginning of **April 2019** and became rapidly an infamous financially driven #ransomware gang. #Talos proposed recently to designate the latter as of privateers not only because of their sophisticated and impactful attacks pursuing Big Game Hunting but also they are allegedly supported or at least indulged by the state(s) that host their infrastructures (in Kaseya' case, i.e., by the **Russian government**).
- **Since February**, Revil' operator appetizes its brand and capabilities (#DDoS and **anonymized phone calls to victims' business associates and media**) on top-tier Russian language cybercrime #forums (#XSS & #Exploit) under the alias 'Unknown'. The latter also recruited new partners with English-language negotiation skills.



- **On July 2**, several #Kaseya VSA servers were abused to spread Revil ransomware-as-a-service. Kaseya is a Miami software supplier and its VSA agents are widely used by Managed Service Providers (#MSP) for network system monitoring of their clients.
- A #Zero-Day exploit was employed against vulnerable on-premise VSA software to **get initial access** (none of their #SaaS customers were compromised). The attackers then spread #Revil payloads towards MSP's final customers via fake updates.
- None of the victims' data were #doxed on its dedicated leak site and backups failed to be deleted thus decreasing by a lot the impact of this attack. According to Kaseya and #Huntress, 60 MSP customers (with about 1,500 downstream businesses impacted) could have been let with encrypted data. #Pinchy Spider demands a $70 million ransom payment to release a "universal decryptor" but also addressed victims individually with lower customized ransom amounts.
- We strongly recommend following Kaseya guidance amongst which is strongly advised to shut down on-premise instances till a patch is released the **11h of June** to mitigate the flaw and to use the **Kaseya Detection Tool** to fasten investigations.

GandCrab, Revil, Sodinokibi, Sodin, Pinchy Spider, ransomware, Talos, DDoS, Zero-Day exploit, doxware, XSS, Exploit, Huntress, Talos, Kaseya VSA

NSO Group's Pegasus spyware activity revealed



- **Pegasus is a spyware created by the Israeli company NSO Group and active since at least 2014**.
- Strictly reserved for government use in order to fight "terrorism and crime" according to its creators, #Project Pegasus, bringing together both NGOs and international media consortium, has just demonstrated a misuse of the #spyware for political surveillance and interference in the affairs of humanitarian workers or media.
- The states suspected of using #NSO Group's solutions are all regimes that have been criticized for the **authoritarian nature of their government**, such as: the Kingdom of Morocco, Hungary, India, Mexico, Saudi Arabia or Rwanda

- Amnesty International and Forbidden Stories, the organizations coordinating the investigation project, point to the #surveillance of nearly 50,000 mobiles (both Android and iOS) through the exploitation of **vulnerabilities that allow the recording and tracing of any data sent or received on these devices**. A victim could be infected without realizing it or without noticing any warning signs due to so-called #zero-click attacks that do not require any interaction with the user to infect them.

- Victimology shows a precise targeting of individuals whose activities are likely to pose a risk to the stability of Pegasus user regimes such as: critical or investigative journalists, lawyers, humanitarian workers or politicians.
- The Pegasus case is symptomatic of the increasingly problematic threats known as #mobile APTs. States that may not have the resources to benefit from effective APT groups are **turning to private NSO Group-like companies to contract surveillance and cyber espionage operations**. The Candiru mAPT, not related with Pegasus, is another illustration of this growing phenomenon.

- **Be prepared** : Monitor as much as possible mobile logs of C-levels employees if they use their personal devices for professional purposes
- **Focus efforts** on teams sensibilization about social-engineering/phishing techniques.
- **In case of suspicious mobile behaviours**, you can check whether you've been targeted by Pegasus with the Mobile Verification Toolkit developed by Amnesty International.

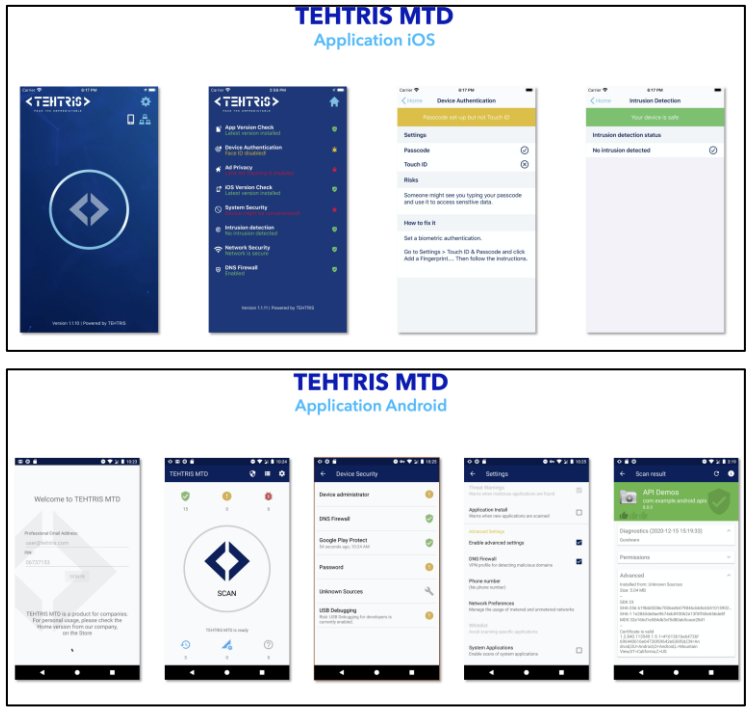
Project Pegasus, spyware, NSO Group, surveillance, zero-click, mobile APTs

NSO Group's Pegasus spyware activity revealed

TEHTRIS Mobile Threat Defense solution allows enterprises to protect either iOS or Android mobile phones fleets from mAPT such as Pegasus :

Since 2018, TEHTRIS offers a mobile agent, named **TEHTRIS MTD**. Its role is to **protect mobile fleets**, it can analyse system configurations, low-level attacks and applications as they are installed or updated. By linking devices in the fleet to the **TEHTRIS XDR** Platform console, TEHTRIS MTD also ensures that **each device is set up in accordance with the company's security policy**.

TEHTRIS MTD interfaces for iOS and Android



An XDR console is systematically deployed in the cloud allowing the customer to monitor the mobile fleet. In case of alerts, these are forwarded from MTD to the XDR platform for analysis. These include, in the case of a **Pegasus infection**, for example:

- **Detection of unknown or potentially malicious apps**
- **Trafic detection through malicious domains**
- **Abnormal behaviour detections** (injection of dynamic libraries into softwares, low-level injections called Stealth Hooking or Swizzling attacks, attempts to hide a malicious presence)

To face mobile, usual APT threats and eCrime modus operandi, Capgemini and Tehtris announced on June, 17th a partnership agreement to provide public and private sectors entities efficient cybersecurity solution

Project Pegasus, spyware, NSO Group, surveillance, zero-click, mobile APTs

sogeti
Part of Capgemini

Cyber-Weather Spotlight

APT

APT31 (aka Zirconium / Judgment Panda)

China

- Defense
- Government
- Aerospace
- International Finance
- Medias & Tel.comm

- Sogu
- Luckybird
- Equation Group leaked exploit

#APT31 is a **Chinese state-sponsored APT group** first seen in 2016. **APT31** primarily **targets the Western countries**, and is specialized on intellectual property theft.

In 2020, APT31 has been accused by national intelligence services to have tried to infiltrate the Finnish Parliament in a intelligence collection oriented operation. Judgment Panda is a **highly sophisticated actor** that in the past have been capable to leverage one of the American APT Equation Group #zero-days years before the #Shadows Brokers made the case public.

Recently, members of APT31 have been pointed out by White House and Allies to belonging to the Chinese #Ministry of State Security and accused of targeting French enterprises by the national cybersecurity agency #ANSSI.

#APT31, zero-days, Shadow Brokers, Ministry of State Security, ANSSI

E-crime

Pinchy Spider

C.I.S/ Russia

- Global

- Sodinokibi
- Gootkit loader
- CVE-2021-30116 exploit

#Pinchy Spider is a Russian speaking eCrime group that performs **Big Game Hunting** (BGH) ops first spotted in January 2018 and believed to be the developer of **Sodinokibi** (aka Revil) #ransomware. Pinchy Spider rapidly adopted #doxing tactics and ranked itself on the Tier I of ransomware operators in terms of sophistication and attack potential.

Following a Ransomware as a Service scheme, **Pinchy Spider turned heavily challenging targeting major enterprises** such as JBS, Acer or Quanta. This targeting is consistent with the possible affiliation of Pinchy Spider to the Russian #privateers groups (i.e financially motivated groups but acting under the protection of Russian authorities). On the beginning of July 2021, Pinchy Spider claimed the #supply-chain attack against #Kaseya showing one more time the growing sophistication of this kind of threats groups.

Pinchy Spider, ransomware, doxing, privateers, supply-chain, Kaseya

sogeti
Part of Capgemini

Cyber-Weather
Spotlight

Vulnerability

PrintNightmare

A #vulnerability nicknamed #PrintNightmare has been discovered in Windows Operating System. A 0-day variant of the previous vulnerability tracked as CVE-2021-34527 was unleashed by mistake by a group of Chinese infosec researchers and affects not only Domain Controllers but also all #Windows servers and workstations and all Windows versions.

Any system in which at least a #print spooler service is accessible will allow an attacker to run arbitrary code with SYSTEM privileges. This CVE is exploited in the wild along with the presence of several public exploits available and has been already embedded in a couple of pentesting tools/frameworks.

Microsoft has released the 6th of July an out-of-band (OOB) fix to address this vulnerability, but the patch does not cover all cases of exploitation of the vulnerability. Besides, the OOB security update now allows customers to restrict installation of new printer drivers after applying the July 6, 2021, updates.

Course of action

Microsoft has released an update for several versions of Window to address this vulnerability. The Out-of Band (OOB) security update allows customers to restrict installation of new printer drivers after applying the July 6, 2021 updates.
If the #patch is not yet available for your Windows version or cannot be applied, we recommend to disable the Print spooler service on all critical assets (possibly via GPO or PowerShell command line on servers).

If this mitigation is not applicable, please apply the workaround below:

- Disable inbound remote printing by #GPO for workstations and/or #ACLs for print servers
- Apply ACLs for print servers developed by Trusec to add deny rules for driver's directory and all subdirectories. As it can still impact printing functionality use the rollback script if necessary.
- Enable PrintService-Operational event logging (not default) for detecting exploitation attempts
- Detecting and responding to exploitation attempts is recommended one can also leverage this #Sigma rule
- Apply upcoming stable version of the patch for the vulnerability CVE-2021-34527

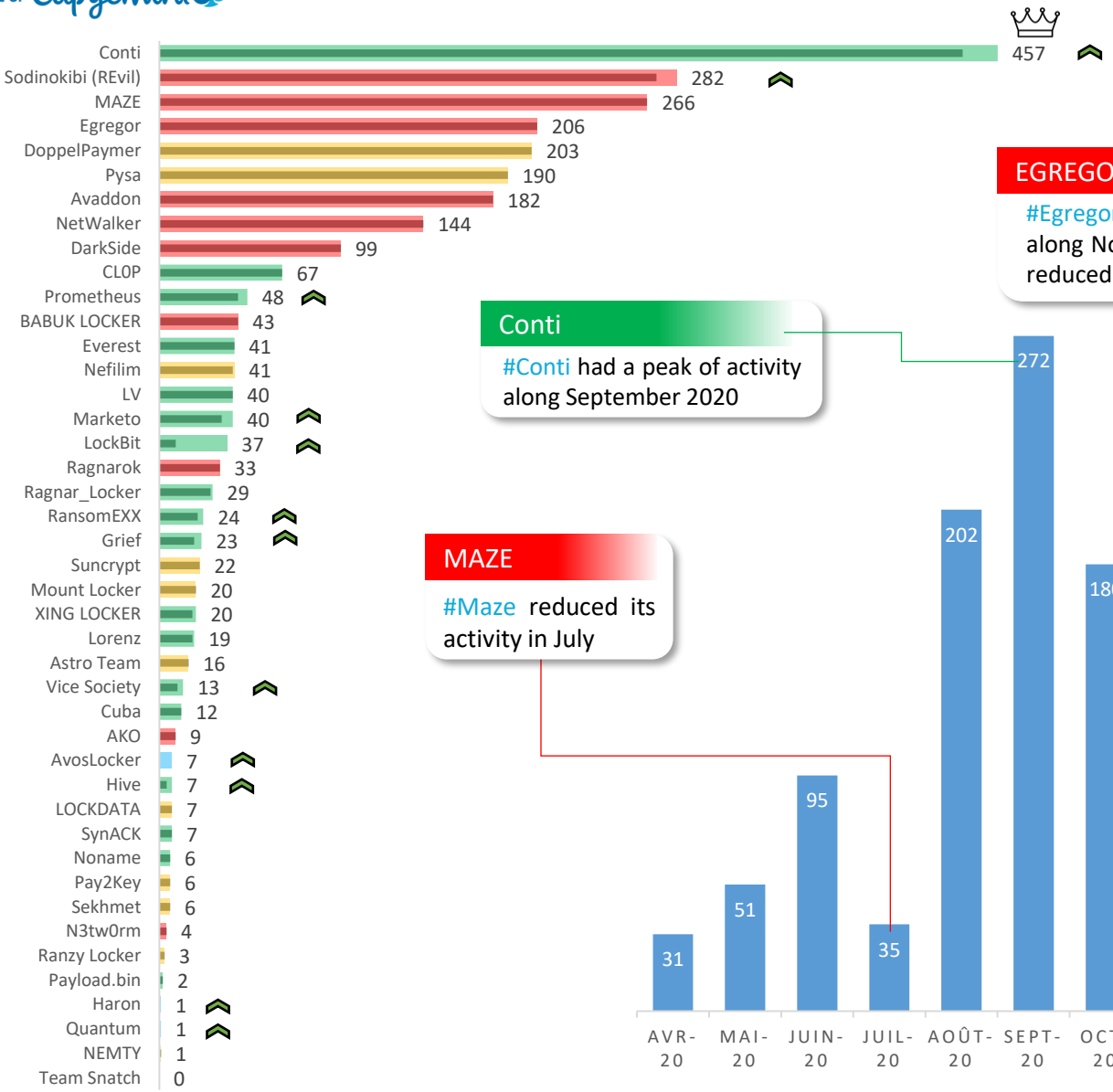
Vulnerability, Windows, Printspooler, PrintNightmare

Patch, ACL, GPO, Sigma

Cyber-Weather

Evolution of Doxwares

Total number of victims (June VS July)



Conti

#Conti had a peak of activity along September 2020

EGREGOR

#Egregor had a peak of activity along November 2020 and then reduced its activity in **January**

MAZE

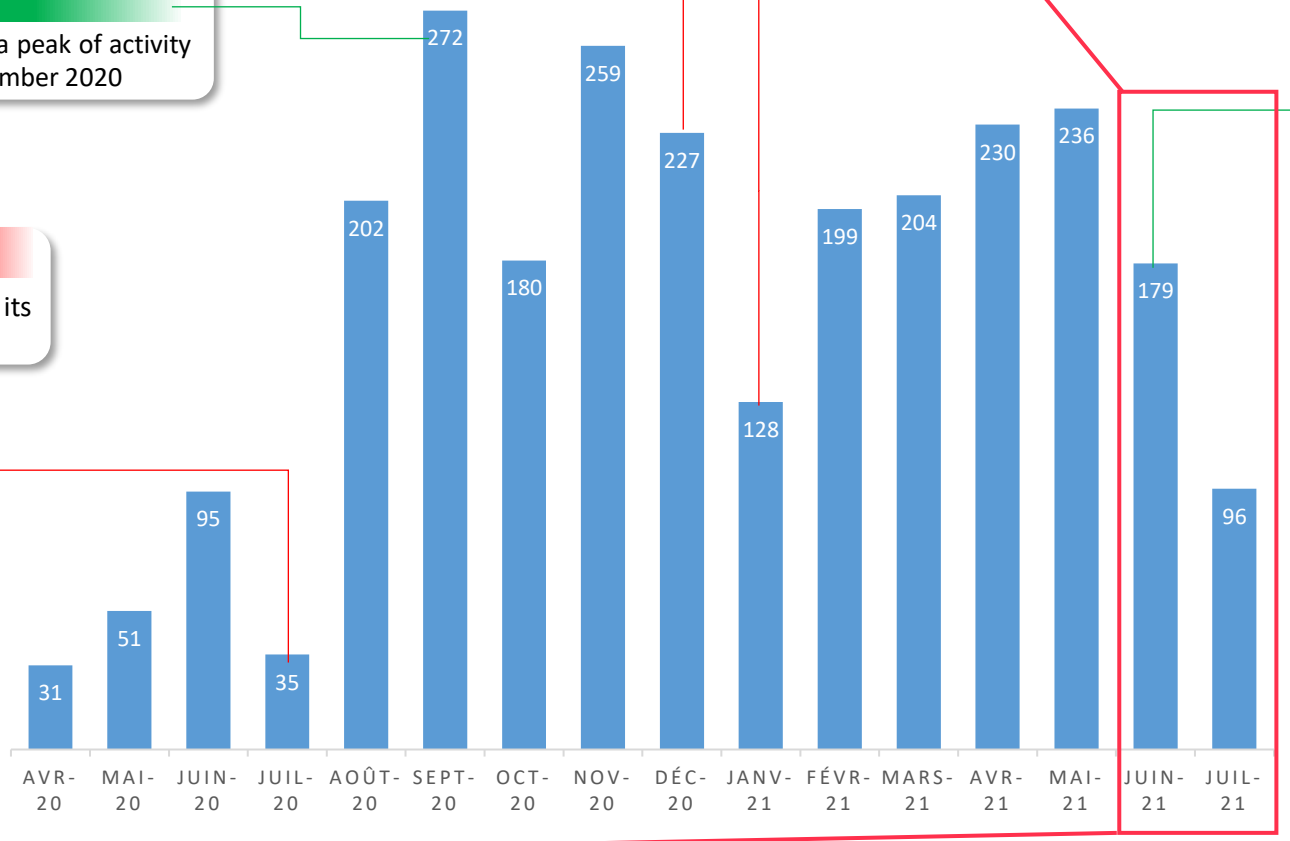
#Maze reduced its activity in July

Darkside | Avaddon | Babuk

Decrease explained by the decreased activity of #Darkside & #Avaddon & #Babuk

Conti | LokBit | REvil

Global decrease explained by summer break of a lot of groups except #Conti & #LokBit . #REvil disappears after a potential end of activity during July



Changes in the number of victims

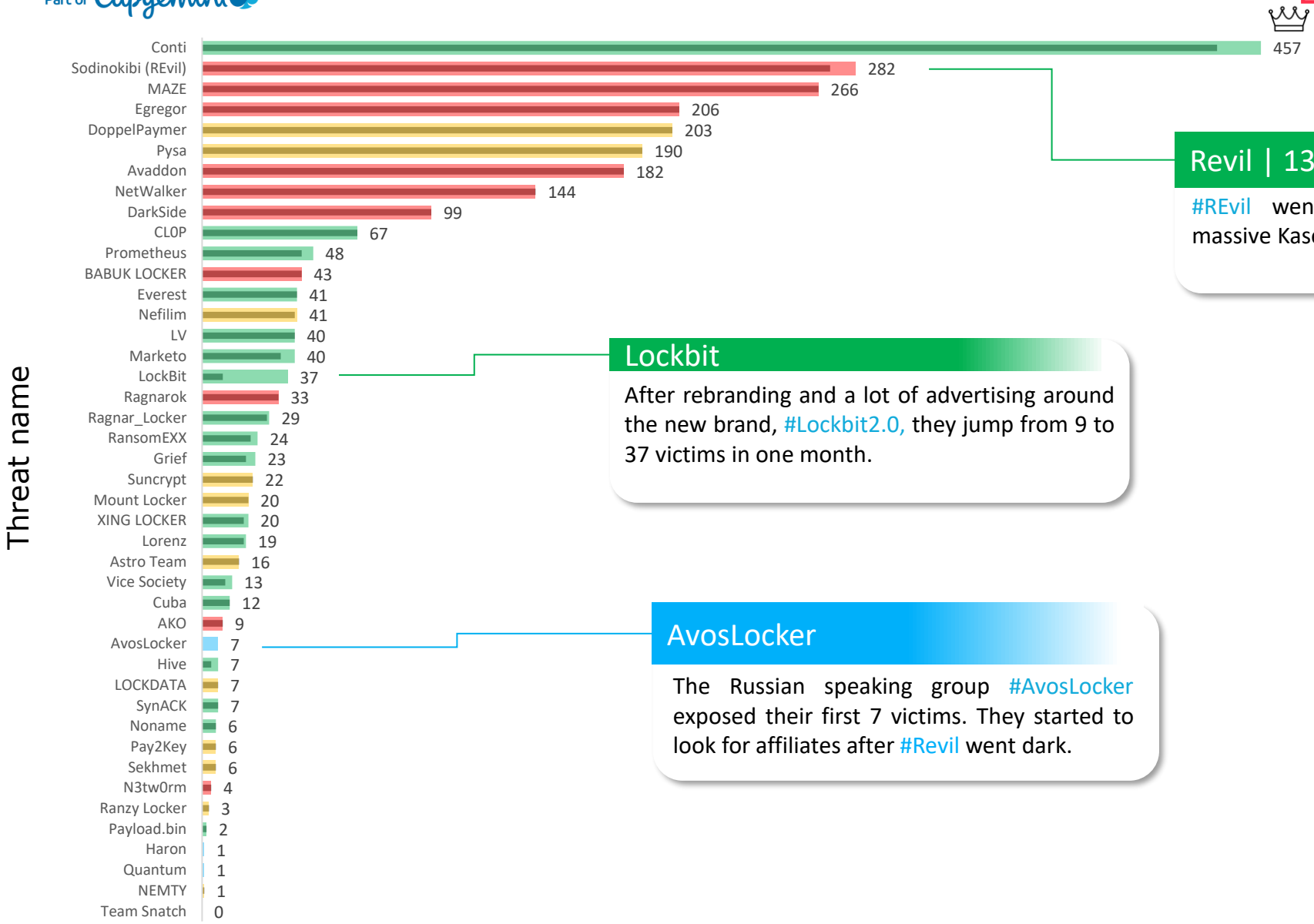
Legend

- Shutdown/Ceased
- Online & active
- Online & inactive
- New this month

Cyber-Weather

Evolution of Doxwares

Total number of victims



Revil | 13th of July

#REvil went offline after the massive Kaseya attack

Lockbit

After rebranding and a lot of advertising around the new brand, #Lockbit2.0, they jump from 9 to 37 victims in one month.

AvosLocker

The Russian speaking group #AvosLocker exposed their first 7 victims. They started to look for affiliates after #Revil went dark.

Legend

- Shutdown/Ceased
- Online & active
- Online & inactive
- New this month