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

June

sogeti

Part of Capgemini

Weak signals for Strategic CTI

"Privateers" groups : towards a new state-sponsored threats scheme

https://blog.talosintelligence.com/2021/05/privateer-groups.html
https://www.welivesecurity.com/2021/06/21/state-sponsored-financially-motivated-is-there-any-difference-anymore/

The Samsam ransomware (Boss Spider actor) in 2018 and #Maze (TA2101/Graceful Spider) in 2019 were the first ransomware variants involved in the **Big Game Hunting** *(i.e large enterprise or governmental organizations)* accompanied by the phenomenon of **double-extortion** by not only encrypting files but also exposing data on dedicated sites and ultimately forcing the board to pay.

The #eCrime ecosystem has shown a strong mimicry and currently 37 groups offer doxxing sites. The most impactful ones (*i.e.*, Conti, Maze, Sodinokibi, Egregor, DopplePaymer) are characterized by a relatively **high level of sophistication and strength, a powerful affiliate system with an overall organizational structure close to the one of big corporations**.

In the infosec culture, #APT groups are usually linked to nation-states tasking them of cyber espionage and disruption operations. These groups are usually characterized by the use of custom toolsets and a sustained effort in terms of OPSEC.

In contrast, eCrime groups are generally financially motivated, act on their own behalf and often rely on open-source tools. Currently, a growing portion of the infosec community believes that many eCrime groups no longer meet these criteria. Talos proposes a new taxonomy of the cyber threat landscape via the designation of #privateers for sophisticated and impactful **cybercriminal groups pursuing Big Game Hunting and being allegedly supported or at least indulged by the states that host their infrastructures**.

CERT Sogeti ESEC is in line with this naming evolution: groups such as #Ryuk, #Conti, #Clop, #Pay2Key or #Netw0rm meet several of these criteria. **Thus, it is reasonable to assume that nation-states will continue to be lenient towards these cartels as long as they do not target domestic companies**. Moreover, while state cyber espionage groups are likely to remain, **privateers are likely to grow significantly**, as their operators take advantage of non-existent international cyberspace laws. Adversary states that rely on #privateers can thus deny having links with them while benefiting from the geopolitical consequences of their attacks (see #Darkside involvement in #Colonial Pipeline). In our opinion, the threat of #privateers, which is more hybrid and involves more money, **should be put on the same footing as that represented by state-run cyber espionage groups**.

Maze, eCrime, APT, Privateers, Ryuk, Conti, Cl0p, Pay2Key, Netw0rm, Darkside, Colonial Pipeline

#

Weak signals for Strategic CTI

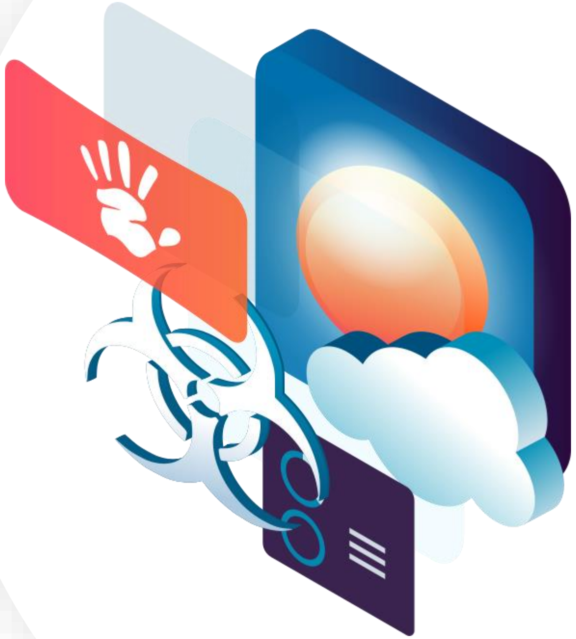
"Privateers" groups : towards a new state-sponsored threats scheme

Privateers actors distinguish themselves by their Big Game Hunting (targeting large companies) ops or by extremely targeted ones (*i.e.*, #Networm|#Pay2Key)

- Intensive use of **loaders as access-brokers**
- Often checks the target's keyboard configuration to **avoid any user whose keyboard is in the Cyrillic language** to get impacted; if the user is located in the C.I.S area the payload stops itself before encryption begins.

The high **profitability** of privateers coupled with their **legal safety** in their countries can (with **high confidence**) lead other malicious actors to engage in this type of activity

- **Be prepared** : capitalize on whitepapers produced by CTI Team about doxwares closely linked to privateers and I3S (Initial Access as a Service) malwares
- **Regularly test your backups; maintain them offline**
  - In particular before using a decryptor
  - Maintain "gold images" of critical systems
- Apply known **vaccines shared by CTI** on specific threats
- **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 access-brokers threats in which phishing is used as an entry vector



Maze, eCrime, APT, Privateers, Ryuk, Conti, Cl0p, Pay2Key, Netw0rm, Darkside, Colonial Pipeline #

RedEpsilon (aka BlackCocaine) Ransomware

- #RedEpsilon (aka #BlackCocaine) is a #ransomware instance written in #Golang first spotted in the wild by security researchers **in May 2021**. Pretty new in the #doxware ecosystem, Epsilon Red came to light targeting Nucleus Software Exports (an Indian company that provides lending software to banks and retail stores) by the end of May

- The name "Red Epsilon" is **a reference to an obscure enemy character in the X-men Larvek comics**. The super soldier is alleged to be **Russian** in origin (former KGB agent) provided with four mechanical tentacles that could be a parable of the way the ransomware deploys itself in a network. Also, Epsilon Red is known to be a highly trained cosmonaut, which implies a solid background in science and technology

- **Epsilon's operators seem to target vulnerable** #Microsoft #Exchange servers by exploiting the infamous #ProxyLogon (#vulnerabilities)

- Once a foothold has been established onto the network of the victim **the attacker(s) deployed needed softwares** and #PowerShell scripts **via Remote Desktop Protocol** (#RDP) and **Windows Management Instrumentation** (#WMI) towards the reachable machines being accessible from the vulnerable Exchange server

- A first #PowerShell script extracts other one as well as a Red Epsilon strain for **further encryption**. Once executed, the additional scripts perform **a series of tasks to prepare the system for a successful attack**. Of note is **the lack of encryption whitelists** usually encountered on other ransomware families. As a result, executables and DLLs could also be encrypted by the Red Epsilon strains and let the **system disrupted**

- Even if Epsilon's has several **anti-VM and anti-debugging functions**, developers seem **to lack of sophistication according to researchers**

RedEpsilon (aka BlackCocaine) Ransomware

- **Ransomware operators let the extensions** ".epsilonred" and ".Blackcocaine" to the encrypted files
- It should be noted that a resemblance in the ransom note as compared as the one of #Sodinokibi/REvil ransomware was reported in the literature. **However, it could be opportunistically borrowed by the operator of Epsilon Red and does not constitute a strong adherence per se**. We found no TTPs in common with Sodinokibi/REvil (see MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs))

- As of writing, **only U.S. and India were targeted** but generally, eCrime actors involved in double-extorsion schemes follow the money so we can expect wealthy Western countries to be targeted (i.e North America, Western Europe). Sectors involved were (at the time of writing) mostly Healthcare and IT companies.

- **Be prepared** : create, maintain and exercise a basic cyber incident response plan against ransomwares/doxwares

- Regularly test your backups; maintain them offline
  - In particular before using a decryptor
  - Maintain "gold images" of critical systems

- Apply our python **vaccines/detection rules whenever provided**

- **Focus efforts** of patching/monitoring **on your VPN/Exchange servers**
  - use whitelists if possible / ban specific countries you are not interacting with
  - **Audit** the network for systems using **RDP**

- One can deobfuscate Powershell scripts via a python script available on Github

APT

Red Foxtrot (aka Temp.Trident / Nomad Panda)

China

- Defense
- Government
- Telecommunications
- Mining
- Think Tanks

- PlugX
- Icefog
- Poison Ivy

#RedFoxtrot is a **Chinese state-sponsored APT group** first seen in 2014. Researchers link the group to the Unit 69010 of the #People's Liberation Army – **Strategic Support Forces** (SSF) responsible for spatial, cyber and electronic warfare, located in Ürümqi (capital of Xinjiang autonomous region). **RedFoxtrot** primarily **targets the Chinese near-abroad area**, particularly Turkish peoples in a military-driven intelligence effort. Defense and government entities are the main targets of RedFoxtrot. The toolset leveraged by the threat group indicates a **strong affiliation pattern to China-nexus APT groups** with RATs and backdoors such as #Icefog, #Poison Ivy, #Quickheal but also with C2 infrastructure known as #PlugX or Axiomaticasymptote.

RedFoxtrot, PLA, Icefog, Poison Ivy, Quickheal, PlugX

E-crime

## Cl0p

C.I.S

- Global

- SDBot loader
- Get2 loader
- Flawed Ammyy

#Cl0p is a ransomware that leverages doxing tactics first spotted in February 2019 and believed to be operated by the infamous eCrime group #TA505 aka Graceful Spider. Cl0p is **one of the oldest** #doxware with the launching of the "Cl0p^_- Leaks" site in March 2020.

On June 16th 2021, a joint #law enforcement operation of Ukraine, United States and South-Korea led to the **arrest of six individuals allegedly involved in Cl0p operations in Ukraine**. Although more than 185.000$ were seized and although the seizure of the Cl0p network' infrastructure were announced by Ukraine, since this operation, two new victims has appeared on the #data leak site, **Cl0p is thus still alive**

Clop, TA505, Doxware, Law enforcement, Data leak site #

sogeti
Part of Capgemini

Cyber-Weather
Spotlight

Vulnerability

PyPI repository targeted by supply chain attack

#Sonatype has identified malicious packages that pulled in #cryptominers on affected machines. Those **typosquatted** packages lured victims to impersonate legitimate python libraries, like **mplatlib** and **matplatlib-plus** being close enough to **matplotlib**. The package analysed by Sonatype pulls bash scripts hosted on #Github, which download #cryptominers referred to as #Ubqminer or #T-Rex.
Those packages were uploaded by the same author (“**nedog123**”), reached more than 5000 downloads since April of this year. Supply chain attack is a fast-growing threat since the end of 2020 as #PHPProject, #RubyGems and #NPM were all targets of this kind of attack hoping to spread malicious packages all around the world.

Course of action

- Developers should perform preventive verification steps such as:
  - Check library signatures
  - Look for a suspicious code in CI / CD Pipeline
- Maintainers of public repositories must:
  - search for any new package that may be typosquatting a legitimate package
  - Communicate about and block any suspicious user or package found

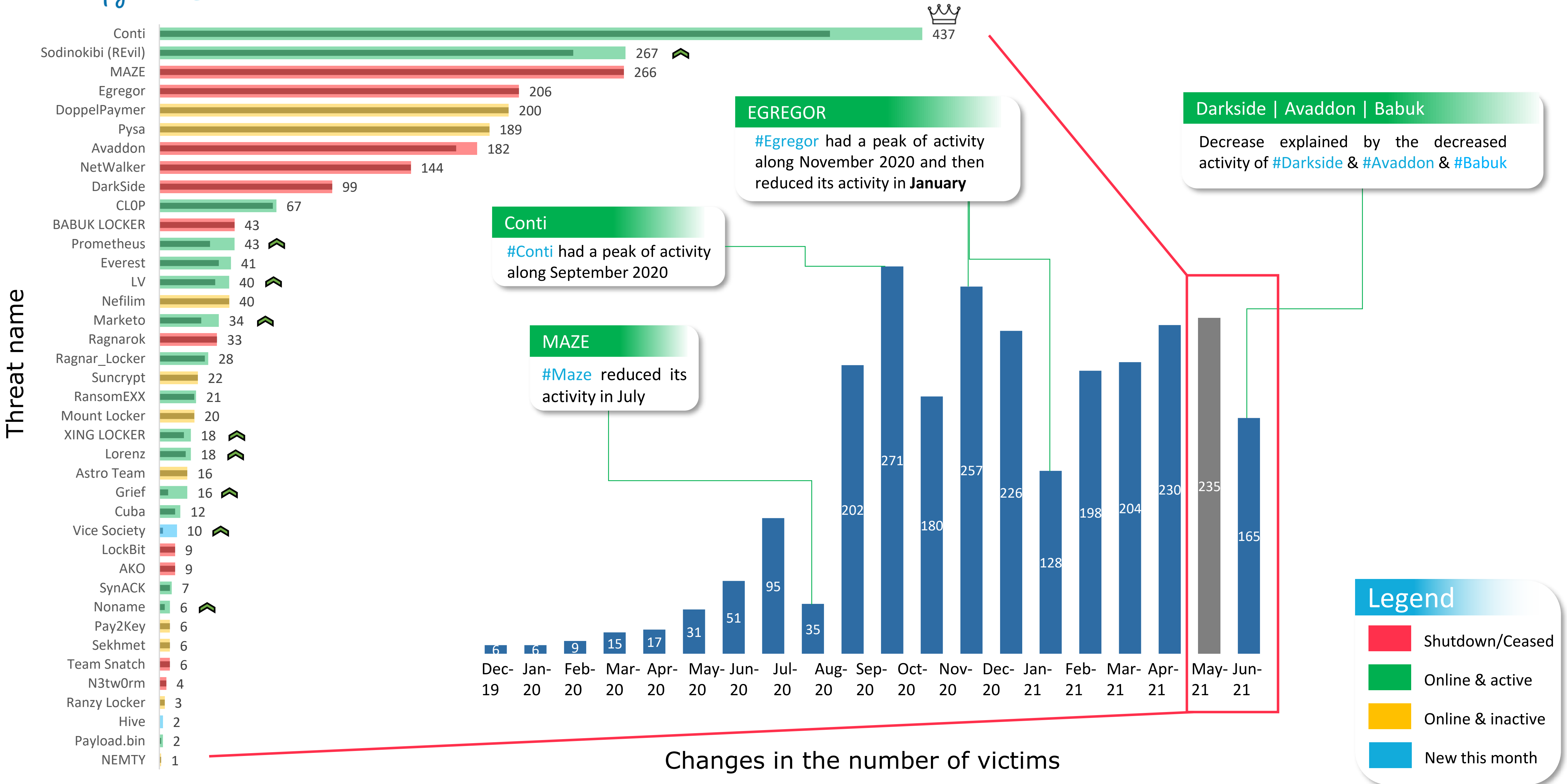
#
Python, Github, Supplychain, Cryptominer, Ubqminer, T-Rex

Audit, Verification
#

Cyber-Weather

Evolution of Doxwares

Total number of victims (May VS June)



EGREGOR

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

Darkside | Avaddon | Babuk

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

Conti

#Conti had a peak of activity along September 2020

MAZE

#Maze reduced its activity in July

Changes in the number of victims

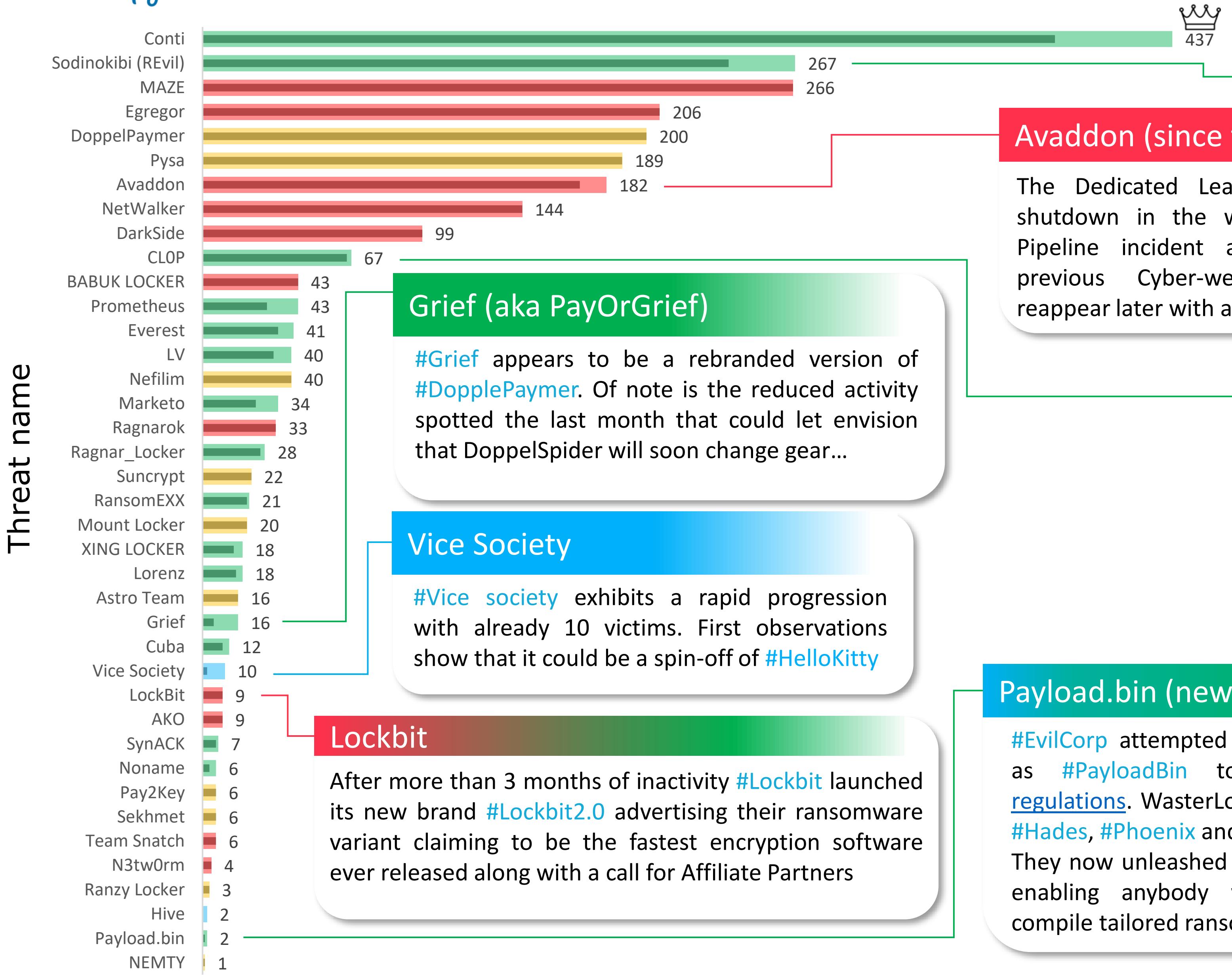
Legend

🟥	Shutdown/Ceased
🟩	Online & active
🟨	Online & inactive
🟦	New this month

Cyber-Weather

Evolution of Doxwares

Total number of victims



Grief (aka PayOrGrief)

#Grief appears to be a rebranded version of #DopplePaymer. Of note is the reduced activity spotted the last month that could let envision that DoppelSpider will soon change gear…

Vice Society

#Vice society exhibits a rapid progression with already 10 victims. First observations show that it could be a spin-off of #HelloKitty

Lockbit

After more than 3 months of inactivity #Lockbit launched its new brand #Lockbit2.0 advertising their ransomware variant claiming to be the fastest encryption software ever released along with a call for Affiliate Partners

Avaddon (since the 11th)

The Dedicated Leak Site of #Avaddon shutdown in the wake of the Colonial Pipeline incident as described in the previous Cyber-weather, They might reappear later with another brand

Payload.bin (new Babuk’ brand)

#EvilCorp attempted to rebrand #WastedLocker as #PayloadBin to avoid violating OFAC regulations. WasterLocker was earlier recalled as #Hades, #Phoenix and now #PayloadBin. They now unleashed a versatile software builder enabling anybody with malicious intent to compile tailored ransomware payloads.

Revil | 12th of June

#REvil Hits US Nuclear Weapons Contractor, "Sol Oriens“ and auctioned data

Cl0P (since the 16th)

The Dedicated Leak Site of #Cl0P is still up and exposed a new victim even after the joint operation from law enforcement agencies from Ukraine, South Korea, and the US that seized their money laundering infrastructure

Legend

🟥 Shutdown/Ceased

🟩 Online & active

🟨 Online & inactive

🟦 New this month