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

October

sogeti

Part of Capgemini

Weak signals for Strategic CTI & Cyber Deception

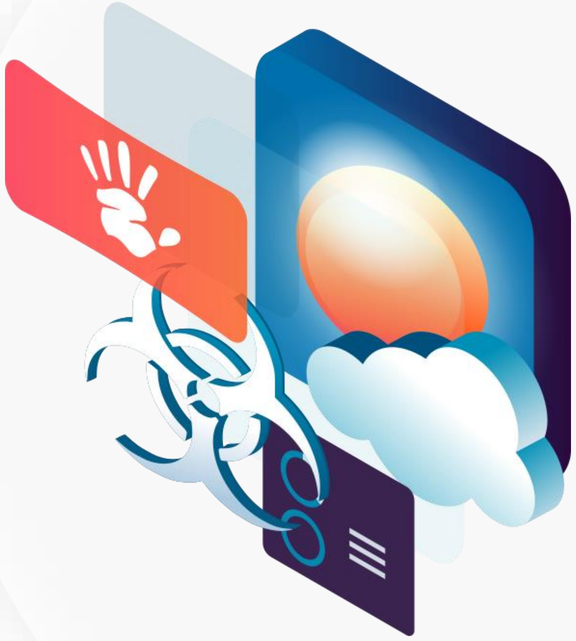
The game of cartels : when unity creates strength

#Maze has been the first recognized ransomware to create ae e-Crime #cartel with other operators to concentrate powers and hackers skills. This association likely embedded Maze, #Egregor, #Sekhmet, #Ragnar and #Lockbit. In 2020, another concerning group dubbed #Wizard Spider appeared and rapidly became a strong competitor of Maze Crew with its infamous Conti and Ryuk variants. **For now, the eCrime scene has heavily changed : the RaaS scheme is now trending and a plenty of small and bigger cartels exist**. Wizard Spider *aka* #FIN12, is still on top of them relying on a great implantation in the #Initial Access Broker (IaaS) landscape with Zloader, Qakbot, Bazar or Trickbot.
From the other side, #Pinchy Spider (Sodinikibi) has suffered from law-enforcement operations and is now redirecting its affiliates to the consortium led by #Groove and #RAMP. It's not clear if #Indrik Spider (Dridex gang, FIN7) is part of the Groove/RAMP/Pinchy cartel but Indrik has ever used Sodinokibi in its operations. **One can conjecture that Indrik brought the now defunct Darkside and** #BlackMatter and #MacawLocker **in their pockets to set a frontal competitive "service offer" against Wizard Spider gang**.

Ransomware cartels know now that they can be disrupted by large-scale law enforcement operations such as ones suffered by Sodinokibi, Darkside or LockerGoga. This growing international response constrain them to rapidly rebrand their ransomwares with new names, new graphics and sometimes new variants. **It's not impossible that in the coming future, we'd see "one shot" ransomwares designed for a big company with a doxing operation durant some days and after a disappreance to stay uncovered from law-enforcement eyes**.

The trending cartelization of the eCrime ecosystem is based on the parallel fast development of the IaaS one. It allows cartels to use loaders as part of their « malware supply-chain » and breach networks for their count. Loaders can be used by one or more groups with fees and depending of the reputation of the groups but also the size of the networks targeted. A more thorough analysis of the role of the loaders has been produced by Curated Intelligence and can be found here.
For actual threats, we highlight the growing popularity of the Cobalt Strike loader dubbed SquirrelWaffle. It can drop either #Cobalt Strike or Qbot : as a reminder, Cobalt Strike and Qbot are favorites tools of numerous ransomware gangs such as Wizard, Pinchy or Carbon Spider's. A #SquirrelWaffle should thus be treated as seriously as a potential ransomware infection.

- **Focus efforts** on #patching/monitoring **the most impactful flaws** reported in our Flash-News produced by CTI team about last TTPs of such ecosystem.
- **Train your teams** to detect phishing & social-engineering methods
- Regularly **test your backups & maintain them offline**
- **Block the C2 servers communicated by the CTI Team** that delivers Cobalt Strike beacons or related loaders such as SquirrelWaffle.
  - If it's not possible, **report every single connection to aforementioned C2s** for thorough analysis to avoid a ransomware infection



Maze, Cartel, Egregor, Sekhmet, Ragnar, Lockbit, Wizard Spider, FIN12, Initial Access Broker, Pinchy Spider, Groove, RAMP, Indrik Spider, BlackMatter, MacawLocker, Cobalt Strike, SquirrelWaffle, Patching-Monitoring #

Cyber-Weather Spotlight

## APT

### APT29 (aka Cozy Bear, Nobelium)

Russia

- Europe
- FiveEyes
- NATO alliance

- Sunspot
- StellarParticle
- FoggyWeb
- Supply-chain interested

#APT29 (aka Cozy Bear, Nobelium) is a **Russian APT group believed to operate on behalf of the Russian Federation** and likely linked with the **#SVR** (Russian foreign intelligence service) and **#FSB** (Internal Russian intelligence service).

APT29 usually targets occidental countries, NATO alliance ones and more globally states engaged in diplomatic conflict with Russia in order to perform **cyberespionage operations or destabilize political activites in targeted countries**.

Primarily known for its implication on the **#Pentagon** hack (2015) or the **#Democratic National Committee** one (2016), Cozy Bear is believed to be behind the infamous **#SolarWinds supply-chain compromise** that targeted organisations worldwide in 2020.

Recently, Microsoft released details of new custom backdoor dubbed **#FoggyWeb** to **target Windows domains and steal sensitive informations on Active Directory servers**. This event highlights the activism of the group after the SolarWinds hack, **activism** that can be also noted as Windows found that **Nobelium tried, with success sometimes, to replicate a global IT supply-chain compromise in past 4 months**.

# APT29, SVR, FSB, Pentagon, DNC, SolarWinds supply-chain compromise, FoggyWeb

E-crime

### CoomingProject

Unknown

- Opportunistic, French-speaking companies tropism noted

- ShinyHunters like operations

#CoomingProject is a threat group specialized in **#data leak** first appeared on August, 31st 2021. Even its data leak site (DLS) shows low-skilled user interface, in September **#CoomingProject** team **claimed 24 successful compromises**.

In its "press release", the threat group has announced **a focus on Canadian and French firms but the victims study highlights a broader geographic targeting** that lead us to qualify Cooming as an **#opportunistic** threat group. Nonetheless, based on a **SOCMINT** (**SOC**ial **M**edia **INT**elligence) analysis performed by CTI Team, we found that the avatar initially responsible for the CoomingProject is highly-likely a **#French** national.

For now, it's not clear if **#CoomingProject** gets its data through **#ransomware** operations or if it exploits unsecure database through internet exposed services of victims targeted. A hint could be the reference of **CoomingProject to the infamous data-leakers** dubbed the **#ShinyHunters** responsible, among others, of data-breaches in Microsoft, Pixlr or NitroPDF.

As the time of writing, the DLS of **#CoomingProject** is down and **on October, 27th of writing the group announced on its Telegram channel that it temporarily shut down its operations**. One can conjecture that enough money has been earnt or the group has been put in light too faster and then attracted law enforcement eyes.

CoomingProject, Data leak, Opportunistic, French, Ransomware, ShinyHunters #

Vulnerability

CVE-2021-41773: Apache zero-day Path Traversal attack

In October 5th 2021, Apache Software Foundation released a new version (2.4.50) for its HTTP web server to correct two critical vulnerabilities. The exploitation of the first one, **CVE-2021-41773**, allows **Traversal Path attack**.

This type of attack allows **information disclosure** by accessing file outside of the supposed web root of the server. As well as information disclosure, some **remote code execution** could also be effective using this vulnerability if some other conditions are fulfilled. If **CGI module** is available and if the attacker can upload a malicious file, its content can be executed.

This vulnerability has been discovered by security researcher **Ash Dalton** and the **cPanel Security Team** on September, 29th and is actively exploited in the wild. A Shodan request had highlighted that there is more than 100k servers vulnerable to the vulnerability.

In addition, the patch for version **2.4.50** has been revealed as insufficient and has been reported as **CVE-2021-42013** as this version is still vulnerable to traversal path attack for files not protected by the configuration "require all denied". So only the version 2.4.49 configured as default is vulnerable.

A second vulnerability has been patched in this version, **#CVE-2021-41524**, that can lead to a denial-of-service (**#DoS**) by a NULL pointer dereference exploitation.

Course of action

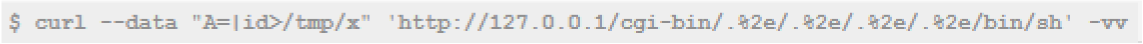
1. **It is strongly recommended to update to version 2.4.51** to cover the vulnerability.
2. **If it's impossible :**

➢ Check that the access control parameter "**require all denied**" is active.

➢ Check that module CGI cannot be used as well as uploading file capability to prevent the RCE exploitation.

In addition, if the web server version had been vulnerable:

➢ it is strongly recommended to perform **threat hunting** on **web server logs** to search for logs with http code 200 combined with "**.%2e/**" like below:



```
$ curl --data "A=|id>/tmp/x" 'http://127.0.0.1/cgi-bin/.%2e/.%2e/.%2e/.%2e/bin/sh' -vv
```

#
Vulnerability, Apache, Web server, Path Traversal, RCE, CVE-2021-41773, CVE-2021-42013, cPanel Security, DoS, CVE-2021-41524

Patch, configuration, require all denied, 2.4.51
#

Do not copy, cite, or distribute without permission

sogeti
Part of Capgemini

Cyber-Weather

Evolution of top-tier ransom-dox-wares

NETWALKER

#Netwalker had a peak of activity until its been seized the 27th of January by the U.S. Department of Justice

EGREGOR

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

CONTI | PYSA | REVIL | AVADDON | DARKSIDE

#Conti had a peak of activity until dividing its rate by 2 since **June** 2021

#Pysa had a peak of activity till **May** 2021

#Revil had a peak of activity till they claimed responsibility for a hack at the IT firm Kaseya **in July**

#DarkSide has **gone dark** after more than $2 million was seized by the U.S Department of Justice in **June**

#Avaddon has **shut down** operation and released the decryption keys

LOCKBIT 2.0

After one month of pause, #Lockbit returns with version 2.0

PYSA | ClOP | CUBA | PAYLOAD.BIN

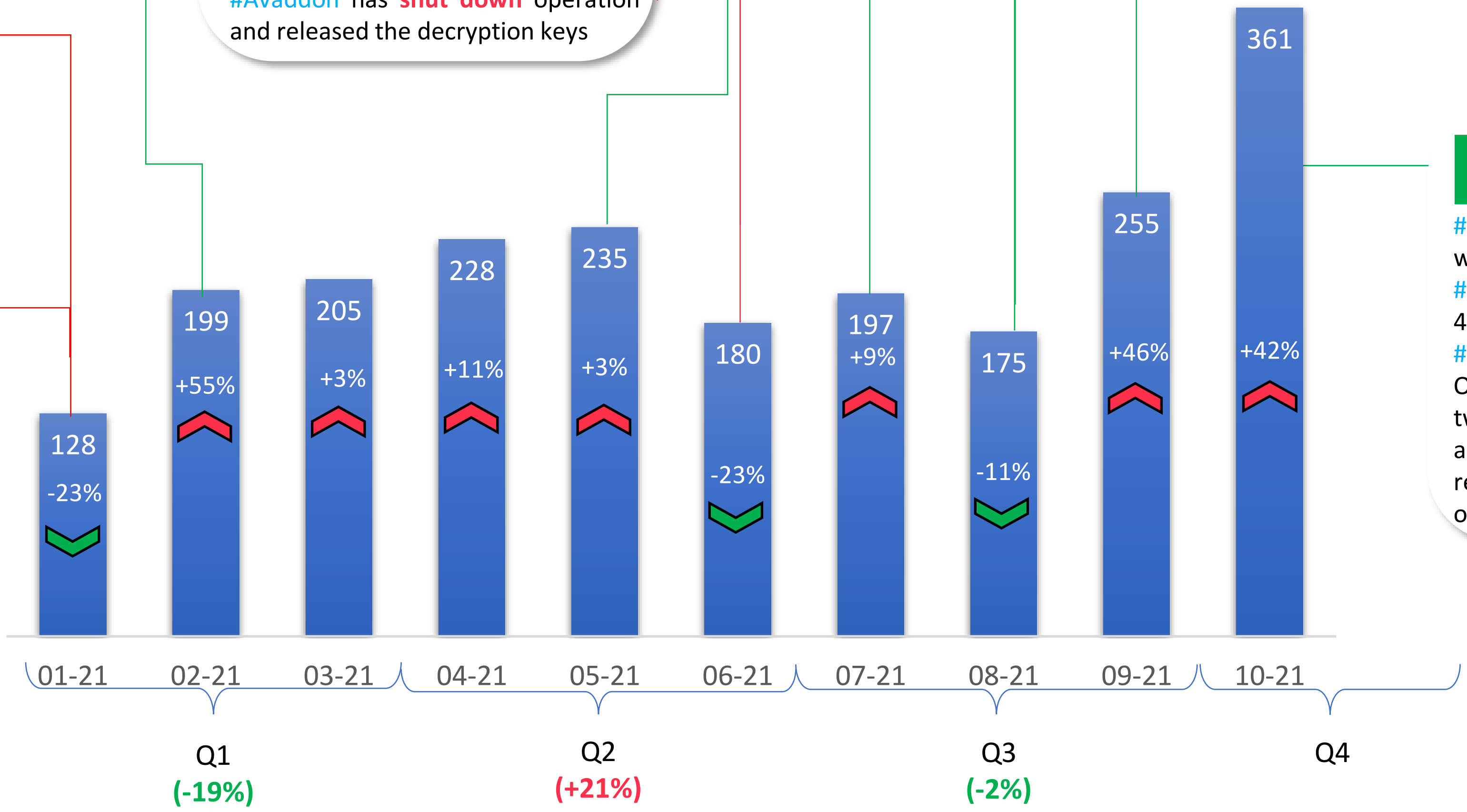
#Pysa, #ClOP, #Cuba and Payload.bin returns this month

COOMINGPROJECT | LOCKBIT | CONTI | BLACKMATTER

#LockBit makes a huge progress in September almost doubling its activity while #CoomingProject counts already more than 20 victims and #Conti, #Pysa & #Blackmatter (ex #Darkside) continue at a huge pace

LOCKBIT | PYSA | CONTI | SPOOK

#LockBit is the more active ransomware with almost 100 victims in October where #Conti and #Pysa are behind with about 40~50 victims. #Prometheus rebrand as #Spook at the end of Sept and start in October with about 50 victims. After only two months, #Coomingproject stops its activities and #Revil went dark after its revival in September and being the target of enforcement forces



Total Number of top-tier ransom-dox-ware victims (2021)

Legend

🟥 Shutdown/Ceased

🟩 Online & active

🟨 Online & inactive

🟦 New this month

Sources: DarkTracer, DarkFeed, InterCert, CTI | CERT Sogeti ESEC

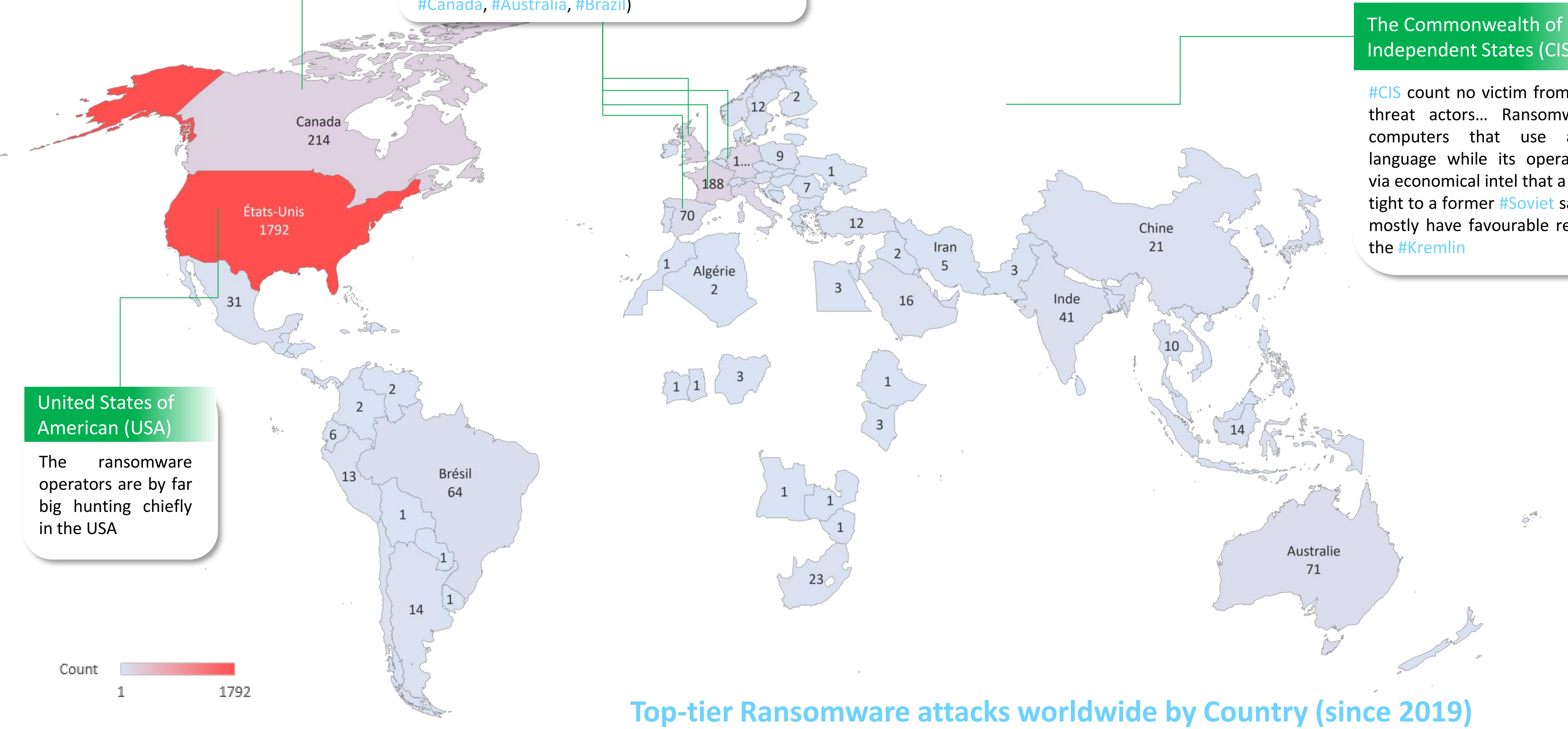
Do not copy, cite, or distribute without permission

sogeti

Part of Capgemini

Cyber-Weather

Evolution of top-tier ransom-dox-wares



US allies are the most targeted

Strategic and critical infrastructures of US Allies are also targeted (#Western-Europe, #Canada, #Australia, #Brazil)

The Commonwealth of Independent States (CIS)

#CIS count no victim from established threat actors… Ransomwares avoid computers that use a #Russian language while its operators ensure via economical intel that a victim is not tight to a former #Soviet satellites that mostly have favourable relations with the #Kremlin

United States of American (USA)

The ransomware operators are by far big hunting chiefly in the USA

Top-tier Ransomware attacks worldwide by Country (since 2019)

Sources: DarkTracer, DarkFeed, InterCert, CTI | CERT Sogeti ESEC

Avec Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, TomTom