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

November

sogeti

Part of Capgemini

Weak signals for Strategic CTI & Cyber Deception

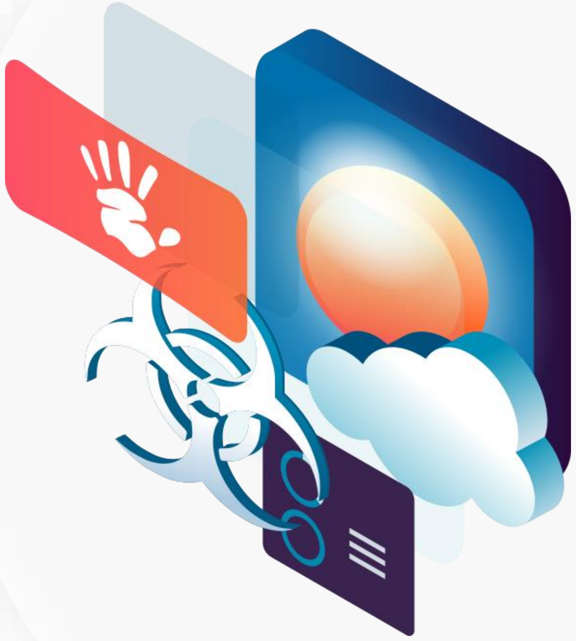
The revival of Emotet : Wizard and Mummy Spiders renew collaboration ?

In the October edition of this Cyber-Weather, we conjectured that two main RaaS service offers were in competition on the eCrime ecosystem : namely the #Indrik Spider one and the #Wizard Spider one. **On November 14th security researchers spotted that some #Trickbot botnets were seen trying download DDLs flagged as the infamous #Emotet loader**. As a reminder, #Trickbot is a botnet infrastructure developed by #Wizard Spider (Ryuk/Conti) that had strong connections with #Emotet which acted as a powerful Initial Access as a Service (IaaS) tool.
We must highlight that both #Trickbot and #Emotet infrastructures were shut down during law enforcement operations due to the impact of the two tools in ransomware infections.
Despite this, the #Emotet Epoch 4 & 5 botnets seem to be alive and leverage #Trickbot survivors servers to perform infections.
#Emotet isn't a "classic" loader : it's enough sophisticated to hijack emails servers and manipulate replies threads to appears legitimate, even for experienced users, and lead to open protected and weaponized archives or malicious Office docs with "trojanized" macros embedded.

If we look at the timeline : the #Emotet revival coincides with the trending threat named #SquirrelWaffle. Although #SquirrelWaffle has not been observed as a ransomware loader at this time, a #SquirrelWaffle > #Qbot > #Cobalt Strike infection chain has been detected. Qbot has previously been used by #Ryuk, #Egregor, #Conti or #Sodinokibi. **Thus, and based on the fact that Qbot could be dropped by Emotet, we believe with moderate confidence that SquirrelWaffle and Emotet could eventually be the preferred tools of Wizard Spider to compete with Lockbit and to fill the void left by Sodinokibi operators**.

It's been a few Cyber-Weather editions that we talk about collaboration in the eCrime sphere. **Identifying which groups have connections with others allow us to spot future moves of loaders and thus prevent infections for our clients**. In the actual case with the revival of #Emotet, **it's highly likely that this MaaS** (#Malware as a Service) **is going to have privileged relations with Wizard Spider** (with ransomwares infections) **but also with other ransomware operators as #Emotet has proven by the past its efficiency** (this is one of the reason it has been shut down, by the way). The task of the CTI Team is then to track #Emotet strains to quickly identify if they led to ransomware infections outside #Ryuk or #Conti variants.

- **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**
- **Pay an extra-attention to suspicious mails** as #Emotet has demonstrated strong capabilities to make their phishing lures as legitimate even for experienced users.
- If you got any suspicions of #Emotet detections or confirmed infections, **please forward these information to the CTI Team**.



Indrik Spider, Wizard Spider, Trickbot, Emotet, SquirrelWaffle, Qbot, Cobalt Strike, Ryuk, Egregor, Conti, Sodinokibi, Malware as a Service, Patching-monitoring

Cyber-Weather Spotlight

APT

### Gamaredon (aka Primitive Bear, Blue Alpha)

Russia

- Ukraine (massively)
- Occidental countries

- EvilGnome
- Pteranodon
- UltraVNC
- Crafted spywares distributed via political oriented phishing lures

#Gamaredon (aka Primitive Bear, Blue Alpha) is a **Russian APT group believed to operate on behalf of the Russian Federation** and likely linked with the Office of the #FSB of #Russia in the Republic of #Crimea and the city of Sebastopol (Internal Russian intelligence service in the annexed region of Crimea).

#Gamaredon usually targets **mainly Ukrainian targets and particularly ones involved in the Defense, Government or Intelligence fields**. It seems to be designed by Kremlin to take part of the cyber conflict between #Ukraine and #Russia and more globally to the **influence and informational conflict between Moscow and Kiev**.

Active since 2013, the undercover cyber-arm of #Russia in annexed Crimea doesn't rely on high level obfuscation. **It rather relies on effective spear-phishing campaigns with custom #RATs or spywares**. Even if it mainly targets #Ukraine, it leveraged Covid-19 lures themes to infect users in Europe in unusual intelligence operations.

On November 4th, the #SBU (Ukrainian Secret Service) released an **in-depth report about Gamaredon organization with individuals implicated in the group**. According to the #SBU, #Gamaredon performed more than 5000 cyberattacks since the occupation of the Crimean peninsula in 2014. Moreover, the #SBU succeeded, based on their words, to **intercept communications between #Gamaredon members** and identified former Ukrainian nationals that betrayed Kiev in exchange of funds. To conclude, the report of the #SBU brings us a better comprehension of Russian APT cyber-landscape that will allow us to better counter these threats knowing who is behind the computer.

Gamaredon, FSB, Russia, Crimea, Ukraine, RATs, SBU

E-crime

### Lockean

C.I.S

- Opportunistic
- French-speaking companies tropism noted

- Big Game Hunting
- Depending on Emotet and TA551 malspam campaigns
- Intensive use of Qbot

#Lockean is **a cybercriminal group specialized in breaching networks via loaders for giving access to ransomware payloads**. This group uses #Big Game Hunting techniques and is part of numerous Ransomware as a Service (RaaS) schemes.

Ones of the common TTPs of #Lockean (tactics, techniques and procedures) rely on #Qbot first stage loader ditributed via #Emotet (Mummy Spider) or #TA551 malspam campaigns, the use of Cobalt Strike beacons or the use of the Rclone exfiltration tool.

According to the French national cybersecurity agency (ANSSI), #Lockean has been/is affiliated to #DoppelPaymer, #Egregor, #Sodinokibi and #ProLock. **Thus, this group had peticular strong links with the TA2101 threat actor (Maze/Egregor) before switching to Pinchy Spider's RaaS**. After #Egregor and #Sodinokibi shut down its operations, one can conjecture that #Lockean could join the Doppel Spider cartel which is suspected to run the #Grief ransomware as a successor of #DoppelPaymer.

#Lockean is an eCrime group that heavily targeted French companies last year : the ANSSI links #Lockean to several incidents such as the compromises of Gefco, Pierre Fabre, Ouest France and Fareva. Two other entities were targeted but their names have not been revealed. **The French tropism of #Lockean is worrying for our French clients : that's the reason why we monitor Lockean's loaders** (such as #Qbot, #IcedID or #Emotet which returns from the dark).

Lockean, Big Game Hunting, Qbot, Emotet, TA551, DoppelPaymer, Egregor, Sodinokibi, ProLock, Grief, IcedID #

Vulnerability

CVE-2021-41379: InstallerFileTakeOver LPE

Microsoft appears to have patched during the November 2021 Patch Tuesday a vulnerability named **CVE-2021-41379** and relying on **Microsoft Windows Installer** which allow a **local privilege escalation** (**LPE**) to **SYSTEM** rights for an attacker on the local machine. **Abdelhamid Naceri**, the security researcher who discovered the vulnerability, confirmed by analyzing the patch that it did not fully cover the vulnerability, publishing a proof of concept for this privilege escalation on all versions of Microsoft Windows, including **Windows 10**, **Windows 11** or **Windows Server 2022** via an alternative method other than the original proof of concept. It allows to override the discretionary access control list (**DACL**) of Microsoft Edge Elevation Service by copying its code instead to be executed allowing a user without privileges to obtain SYSTEM rights.

Cisco Talos researchers have confirmed that they have found traces of the exploitation of this vulnerability in recent campaigns and have published two **SNORT rules** (SIDs 58635 and 58636) to detect the attempted exploitation of the vulnerability. Even if the exploitation cannot be done without access to the system, there is currently no patch to fully correct the vulnerability.

Nextron systems cyber security team have provided detection measures based on yara rules.

Course of action

1. **It is strongly recommended to patch** systems when a patch will be available.
2. **In the Meantime :**

- If an Intrusion Detection System (**IDS**) is available, update its configuration with **SNORT** rules released by Cisco Talos researchers (SIDs 58635 and 58636).
- A **sigma detection rule** is available **here** to detect file creation by exploitation of this vulnerability.

Nextron systems cyber security team created a private **yara** rule that performed detection on **Virustotal** samples (more than 30 different sample in 48 hours). A test on this platform could **correlate** SIGMA or SNORT detection.

Some Yara rules are available **here** by Security researcher **@Arkbird**.

Vulnerability, Microsoft, Windows 10, Windows 11, Windows 2022 Server, LPE, CVE-2021-41379

Yara, Sigma, Virustotal #

sogeti
Part of Capgemini

Do not copy, cite, or distribute without permission

Cyber-Weather

Evolution of top-tier ransom-dox-wares

EGREGOR | NETWALKER

#Egregor reduced its activity in **January.** #Netwalker have been been seized the 27th of January by the U.S. Department of Justice

CONTI | PYSA

#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 | AVADDON | DARKSIDE

#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

PYSA | ClOP | CUBA | PAYLOAD.BIN | LOCKBIT

#Pysa, #ClOP, #Cuba and Payload.bin in **August**. After one month Lockbit return with a version 2.0

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

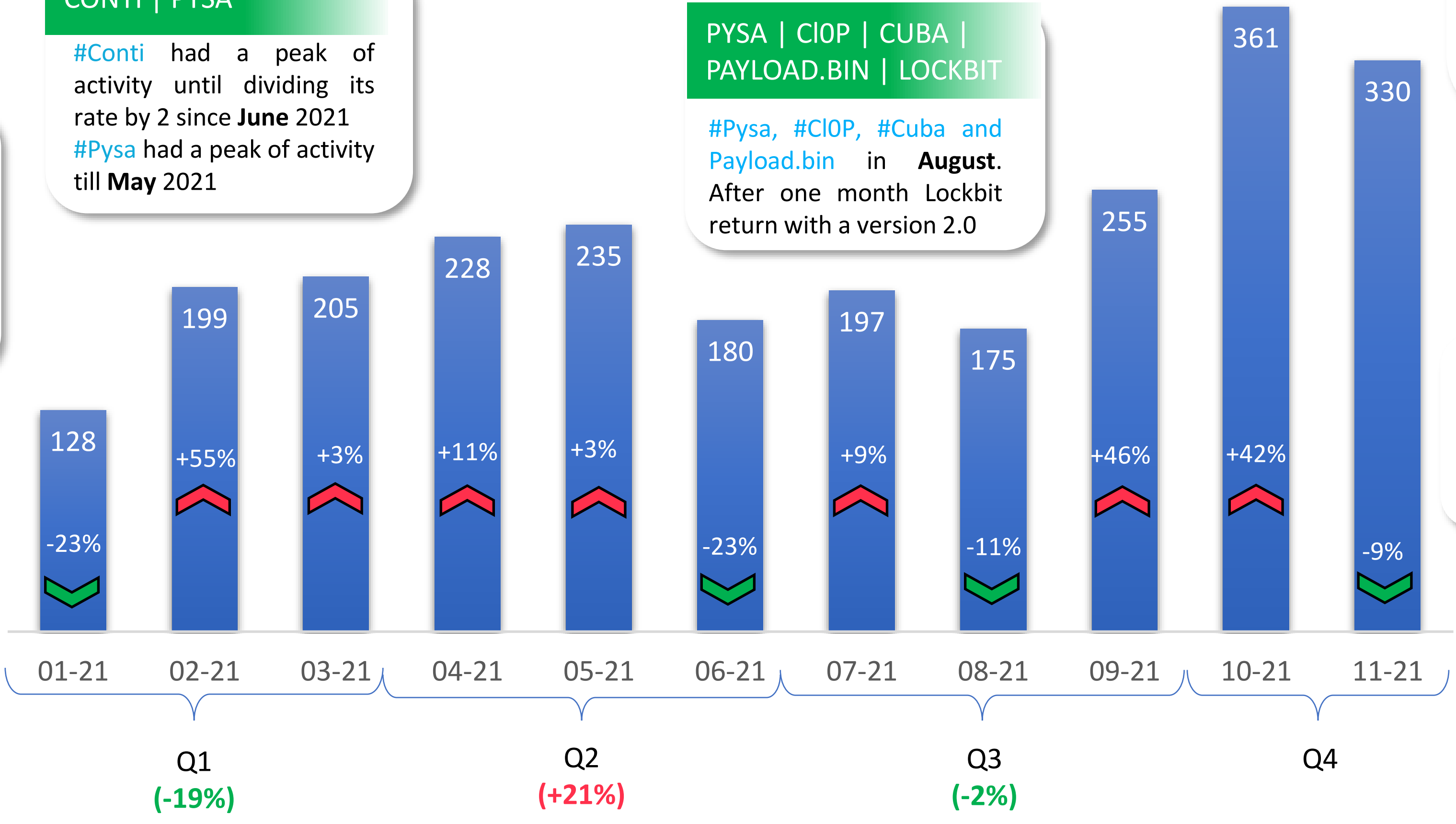
#LockBit is the more active ransomware with almost 100 victims in October where #Conti and #Pysa are behind with about 40~50 victims. #Prometheus rebrand as #Spook at the end of Sept and start in October with about 50 victims. After only two months, #Coomingproject stops its activities and #Revil went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

LOCKBIT | PYSA | CONTI | SPOOK

#LockBit and #Conti are leading the board in November with around 90 victims each. #Pysa stay behind with 59 victims.

BLACKMATTER | REVIL |SPOOK

No more activities in November from #Spook, #Payload.bin, #Groove, #AtomSilo, #BlackMatter or #REvil the last 2 being targeted by law enforcement forces



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

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

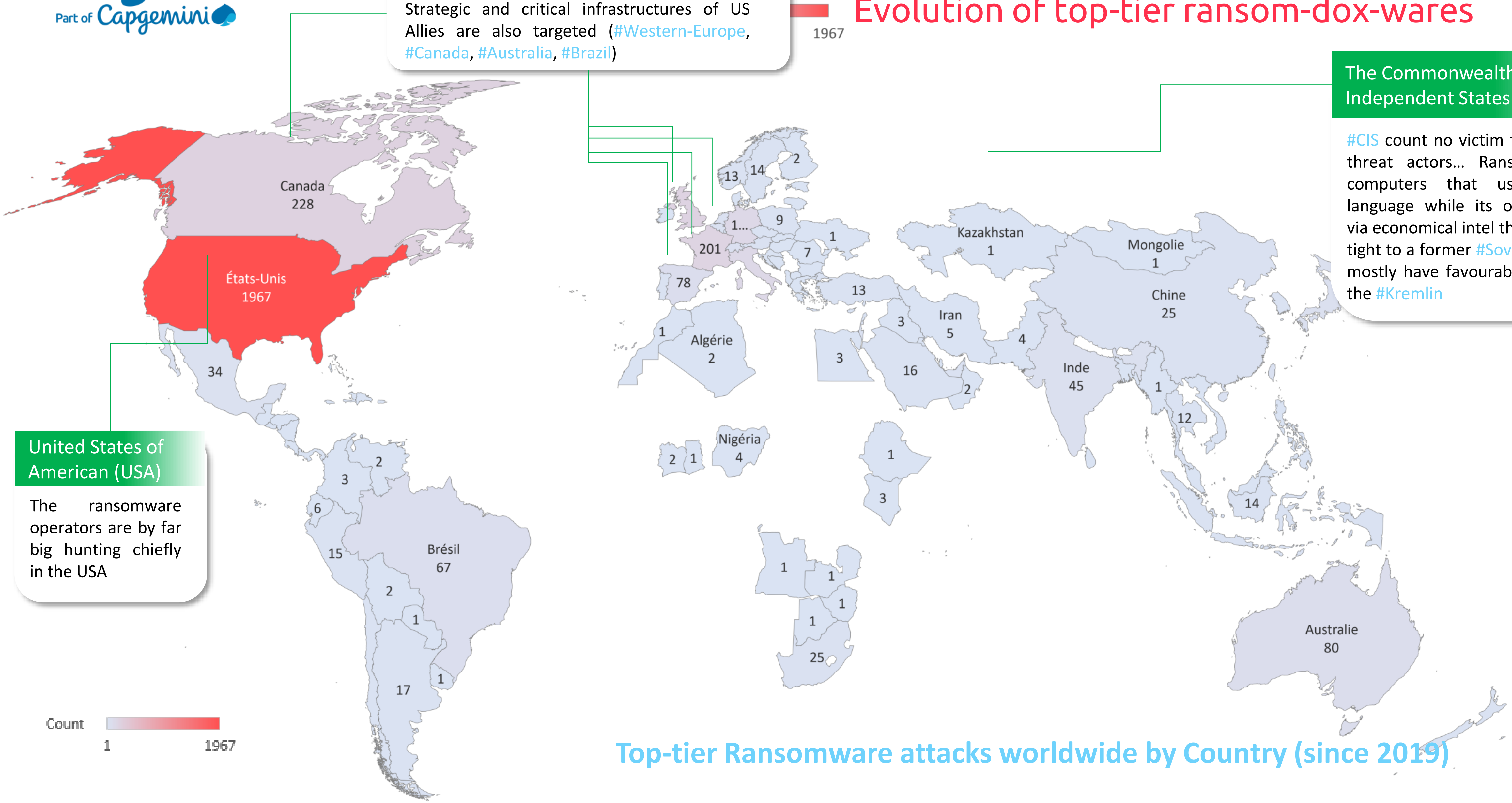
Legend

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

Do not copy, cite, or distribute without permission

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