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

September

sogeti
Part of Capgemini

Weak signals for Strategic CTI & Cyber Deception

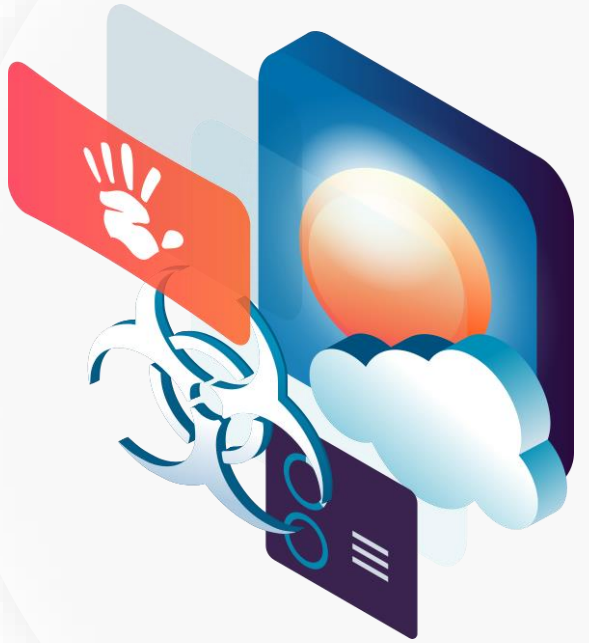
Hide and seek : the challenging game ransomwares and law enforcement play

Essential services (especially healthcare) have extensively been targeted in the recent past years by some of the top-tier ransomware gangs (**#Ryuk**, **#Conti**, **#PYSA**, etc…).
The May 2021 cyber attack against **Colonial Pipeline**, being the largest US gasoline/diesel supplier, marked a turning point in **ransomware attacks impacting critical infrastructures**.
The latter substantiates a previous anticipation that the **eCrime ecosystem will be** more and more leveraged to conduct **disruption/sabotage but also influence operations** (**#privateers** who would act on its behalf in return of funding, see the June and July edition of the Cyber-Weather).

Because **large-scale attacks** are intensively **covered by the global media while** involving **law enforcement**, it becomes essential for the impacted nation to react.
Rare enough to be noted is the recent reactions of **#hack-back** operations (**#DDOS** attacks) that two operators unveiled (**#LockBit** and **#Marketo**), which are half-heartedly accepted by the American authorities (being by far the most impacted country, see the 6th slide).
Other noticeable **change in TTPs** is the recent threatening of both **journalists** that **expose chat negotiations** and **victims calling for help** from investigators, the FBI or ransomware negotiators that would trigger the **publication of encrypted files** by the **ransomware operator**.
#Hack-back operations, **#chat-hijacking/#chat-exposure and #negociators** could **prevent data exposure** that **disrupt the business model of these groups**.

In response, **doxing sites** are **strengthening the security of their DLS infrastructures via anti-DDOS measures** and **verification stages.** The latter allow **only victims to negotiate** with the **ransomware operator** in the same vein as what **#blackmatter** (ex **#darkside**) recently did.
Because the **eCrime ecosystem** exhibits a high degree of mimicry and resiliency, **it is likely that newcomers will adopt an anti-DDOS & chat high jacking security policy by design** to undermine the efforts of law enforcement.
It is highly likely that **the United States will perpetuate hack-back operations when strategic U.S. entities are hit**, being part of a national context that justifies the creation of the "Ransomware task force" bringing together IT majors and members of the Five Eyes to fight ransomwares.

- **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**
- Apply known **vaccines/detection rules** 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**



Privateers, hack-back, Marketo, Lockbit, Conti, BlackMatter, negotiators, DDOS, doxing

Privateers/E-crime

Wizard Spider (linked to UNC1878/TEMP.MixMaster)

Russia
Ukraine

- Global (Big Game Hunting)

- Ryuk/Conti
- BazarLoader IaaS
- Massive use of Cobalt Strike

#Wizard Spider is a **Russian** speaking **eCrime group** that performs Big Game Hunting operations while developing one of the most impactful ransomwares.

In the wake of the disclosure of the **#CVE-2021-40444**, RiskiQ researchers spotted that **Wizard Spider' infrastructure is closely associated with the exploit of the Windows zero-day**. They observed that the threat actor behind the exploitation of this flaw deploying **#Cobalt Strike** beacons **overlaps the Wizard Spider's C2 infrastructure**.

This overlap doesn't mean that Wizard Spider is behind the campaign as it could be **one of its affiliates** (as a reminder, the threat group follows a **#Ransomware as a Service** scheme), **it could be another group** that "fraudulently" abused the group' infrastructure or **it could be a state-sponsored operation** disguised in classical "eCrime" activity to stay undercover.

Anyways, the **growing leveraging of zero-days by eCrime actors** tend to reinforce the hypothesis that **#privateer groups**, as we assume Wizard Spider is, **are adopting tactics** previously only available to **#APT** groups.

E-crime

Blackmatter ransomware

C.I.S

- Global (Big Game Hunting)

- No CIS countries kill-switch
- Pre-attack intelligence

#Blackmatter is a **#ransomware** strain discovered by the end of July 2021 following a **#RaaS** scheme and a double-extorsion tactic. Even though one of their operators claimed that his brand is separated from **#Sodinokibi** or **#Darkside** ones, more and more researchers point at **strong overlaps** between **the latter** and **#Blackmatter**.

Based on technical evidences such as the encryption routine study or, among others, code similarities, **it's likely that #Blackmatter signs the come-back of Darkside core teams**. This revival takes place in a moment where **#Darkside** disappeared following its infamous **#Colonial Pipeline** major attack. **#Blackmatter also seems to fear a law-enforcement operation** if we study the new "ethics rules" that follows the group stating that they will not attack critical infrastructures… and pipelines.

A **leaked private negotiation chat** between **#Blackmatter** and **#NewCoop** (a major US agriculture group) highlighted a **great pre-attack intelligence collection** of the threat group as **#NewCoop** tried to lure **#Blackmatter** claiming that they fall under critical infrastructures "ransomware immunity". Despite **#Blackmatter** goodwill, **it's highly likely that US authorities will hunt the operators as they've shown to be capable to compromise critical infrastructures**.

Wizard Spider, CVE-2021-40444, Cobalt Strike, Ransomware-as-a-Service, APT, Windows

Blackmatter, Sodinokibi, Darkside, Colonial Pipeline, New Coop

Cyber-Weather Spotlight

Vulnerability

CVE-2021-40444 : MSHTML zero-day RCE

September 7, 2021, Microsoft alerted on the active exploitation of the **Windows MSHTML remote code execution** vulnerability (**CVE-2021-40444**) by malicious actors.
This vulnerability permits an attacker to forge an **ActiveX control** in order to be executed by the vulnerable component **MSHTML**. The code is executed with the user' rights who opens the malicious document. This component, although being the engine of Internet Explorer, is also used by the software of the **Office Suite** software such as **Outlook** for the preview of the documents within a mailbox.
The **Microsoft Threat Intelligence Center** (#MSTIC) team studied samples retrieved in a series of attacks. The latter demonstrated that the vulnerability exploitation was only the first step in such to leverage **Cobalt Strike beacons** communicating with an infrastructure tracked as **DEV-0365** whose characteristics and history suggest that it would be linked to both the group tracked as **DEV-0193** and **UNC1878** that deployed **Ryuk operated by #Wizard Spider**.

Of important note is that **the attack only works if** the victim disables the **protected view**, enabled by default, or the **Application Guard** for Office as these prevent the automatic execution of the ActiveX.

Course of action

1. **Keep Application Guard and Protected View activated** and Communicate to users in order to double check legitimacy of documents before deactivate those protection.

2. disable new ActiveX installation in Internet Explorer
In Group Policy settings, navigate to
Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page

For each zone(Internet Zone, Intranet Zone, Local Machine Zone, or Trusted Sites Zone):
- Enable Download signed ActiveX controls policy and set it to "Disable".
- Enable Download unsigned ActiveX controls policy and set it to "Disable".

ActiveX controls installed prior the activation of those policies will still remain enabled.

3. Disable preview in Windows Explorer
Delete the value data of the following registry keys:
- HKEY_CLASSES_ROOT\.docx\ShellEx\{8895b1c6-b41f-4c1c-a562-0d564250836f}
- HKEY_CLASSES_ROOT\.doc\ShellEx\{8895b1c6-b41f-4c1c-a562-0d564250836f}
- HKEY_CLASSES_ROOT\.docm\ShellEx\{8895b1c6-b41f-4c1c-a562-0d564250836f}
- HKEY_CLASSES_ROOT\.rtf\ShellEx\{8895b1c6-b41f-4c1c-a562-0d564250836f}

Vulnerability, Windows, Microsoft, MSHTML, 0day, RCE, Cobalt Strike, MSTIC, MSOffice, UNC1878, ActiveX

Patch, RPC, Protected view, registry, group policy

Cyber-Weather

Evolution of top-tier ransom-dox-wares

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

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**

LOCKBIT 2.0

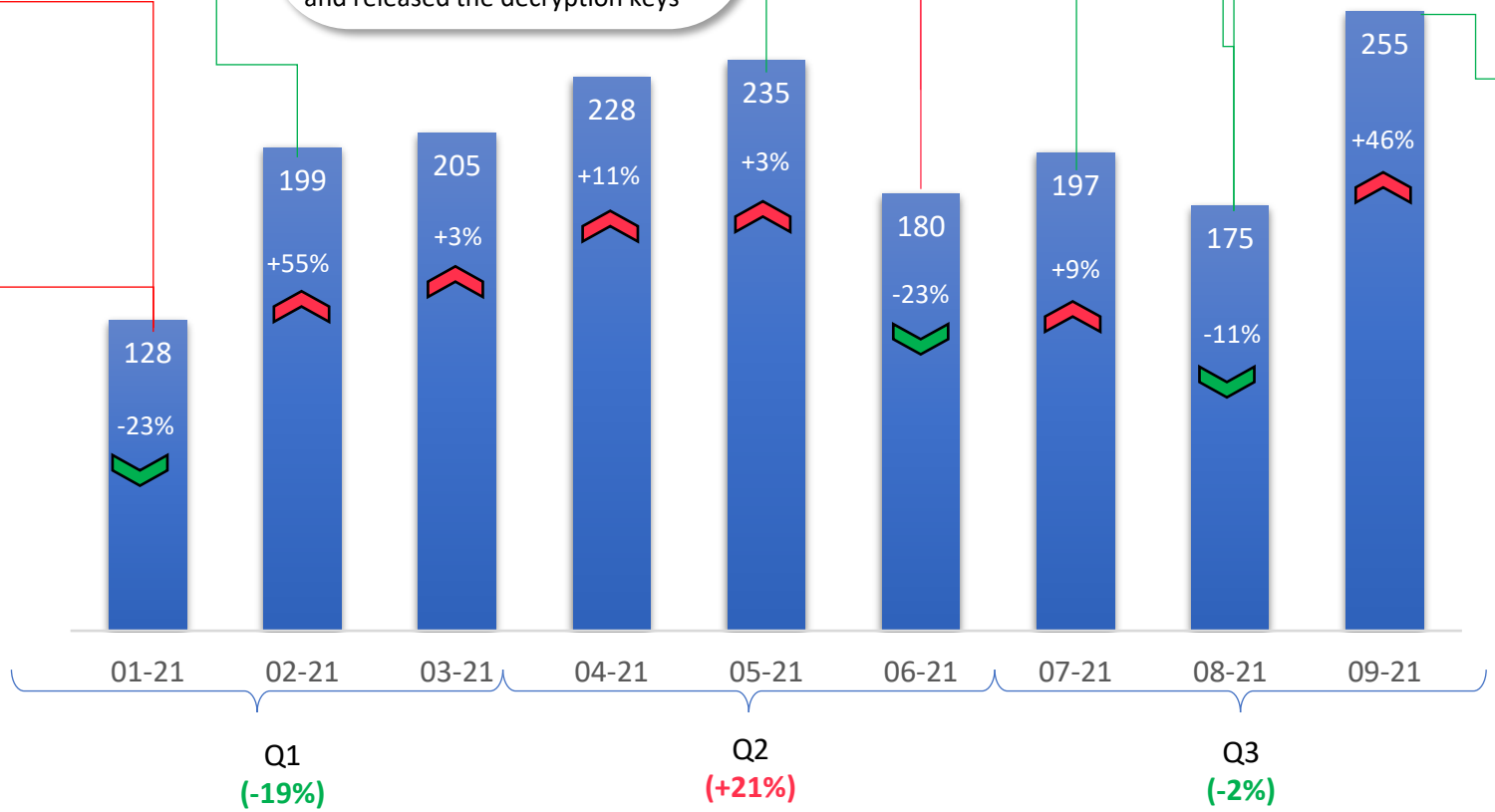
After one month of pause, #Lockbit returns with version 2.0

PYSA | ClOP | CUBA | PAYLOAD.BIN

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

COOMINGPROJECT | LOCKBIT | CONTI | BLACKMATTER

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



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

sogeti
Part of Capgemini

Cyber-Weather

Evolution of top-tier ransom-dox-wares

US allies are the most targeted

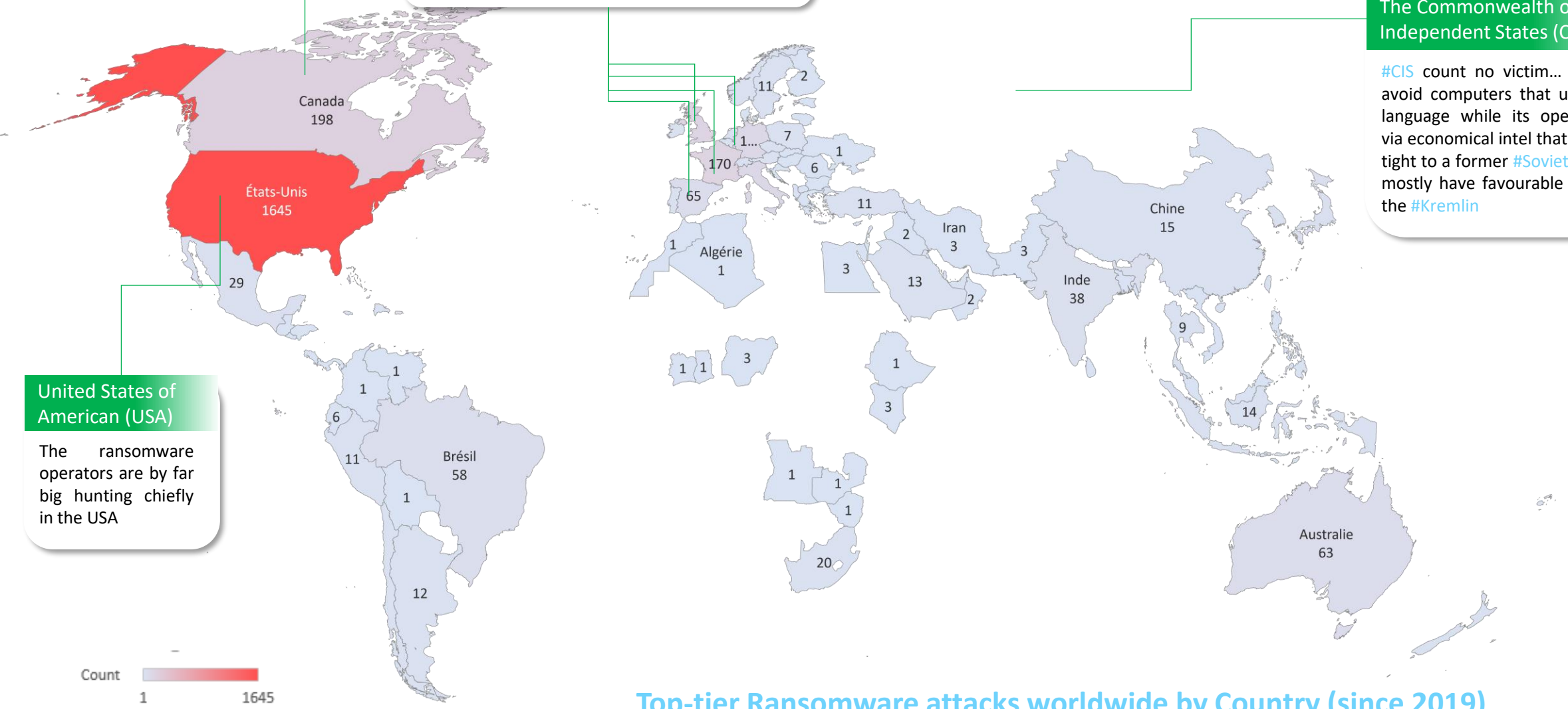
Strategic and critical infrastructures of US Allies are also targeted (#Western-Europe, #Canada, #Australia, #Brazil)

The Commonwealth of Independent States (CIS)

#CIS count no victim… 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