CYBER INTELLIGENCE
Threat
INSIGHTS

TLP:WHITE

Capgemini

CYBER-WEATHER

MONTHLY NEWS ROUNDUP

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

Sun Tzu (544 – 496 av.JC)

Capgemini

CYBER-WEATHER
Anticipation

TLP:WHITE

WEAK SIGNALS FOR STRATEGIC CTI & CYBER DECEPTION

Lessons from Russian/Ukrainian war

On February 24th, 2022, Vladimir Putin has launched a "special military operation in Ukraine". After the conflict's start, several threat groups have decided to support either Ukrainian or Russian forces.

Massive cyber operations have been observed in both sides against entities (Government bodies, infrastructures, Satellites, IT companies…), as well as on social media on which many fake news and propaganda contents have been spread to manipulate and influence public opinion.

In order to reduce impacts of such campaigns, governments have excluded or restricted several media and social networks (#RT, #Sputnik, #BBC, #Facebook). Moreover, they also reaffirm that in case of major cyberattack against critical entities, military response will be applied, including eventually nuclear attacks.

All these adversaries are very active, and their actions have a great impact on all actors implied directly and indirectly in the conflict.

#Privateers ecosystem and particularly top tier ransomware groups like #Wizard Spider or #CoomingProject group have officially announced their support for Russia. Recently with the #Conti leak revelations, researchers have proven link evidence between group members and Foreign intelligence services (#SVR) and domestic intelligence ones (#FSB). However, some other top ransomware groups like #Lockbit have announced they will not get involved in an international conflict and the motivation remains financial.

On the contrary, many hacktivists regrouped under Anonymous banner have declared war against #Russia. They have already targeted more than 2500 Russian allies' websites, leak sensitive data, perturbate railway traffic. They also lead anti-Russia propaganda campaigns by spreading a huge amount of conflict scenes on social networks or directly on Russian media they have hacked.

#APT groups like UNC1151 are continuing their focus on Ukraine. Cybersecurity researchers have discovered serveral wipers (#HermeticWiper and #IsaacWiper) and Trojan (#Foxblade) that have been developed and used against Ukraine.

Numerous Occidental countries such as the United States, European Union and United Kingdom have explicitly condemned the war in Ukraine and have adopted severe economic sanctions against Russia (SWIFT exclusion, Russian airplanes ban) and Russian oligarchs.

#Russia and their allies might continue to use all their #eCrime and #APT ecosystem on Ukraine and will increase their activities on Ukraine allies. Several major Occidental companies have been impacted by cyberattacks this month (McDonalds, Nvidia, Toyota, Aon, Samsung). For the moment there is no evidence that these events are linked to Russia activities

#Anonymous will probably continue its operations against Russia and try to break Russia media censure.
Based on it, we believe with medium confidence that in a short-medium term, West-European countries (and particularly ones that try to act as a go-between Ukraine and Russia) could be heavier targeted than before by eCrime privateer groups via their ransomware payloads such as #Conti, #Lapsus, #Snatch, #Stormous, #Hive

- Focus efforts on #patching/monitoring the most impactful flaws reported in our Flash-News produced by CTI team about last TTPs of such ecosystem. A Flash News has been sent about this topic with information regarding the monitoring of Russian threat groups by the CTI Team.
- Train your teams to detect phishing & social engineering methods
- Regularly test your backups & maintain them offline
- Follows all the communications written by CTI Team describing actionable IoCs and detection tips.

Russia, Ukraine, Anonymous, SVR, FSB, GRU, UNC1151, APT, Lockbit, HermeticWiper, IsaacWiper, Foxblade, Facebook, BBC, Privateers, Lockbit, eCrime, Conti, patching/monitoring, RT, Sputnik

Capgemini

CYBER-WEATHER
Spotlight

TLP:WHITE

APT (UNC1151)

Belarus

Occidental countries
Anti-NATO campaigns

Bleeding Bear
Ghostwriter campaign

#UNC1151 (aka #Ghostwriter) is a Belarus APT group believed to operate on behalf of the Ministry of Defense of the Republic of Belarus since 2017.

UNC1151 has been involved in cyber espionage, online disinformation and influence campaigns throughout Europe known as "Ghostwriter". These activities involve anti-NATO disinformation campaigns and politically damaging hack-and-leak operations. Moreover, UNC1151 does not hesitate to target Educational sector, Government entities or Defense and Military institutions using some specific backdoors (#HalfShell, #RadioStar or #VideoKiller) or malwares (#B374K and #HiddenValue).

In the wave of escalating tensions between Russian and Ukraine, the group conducted defacing campaigns during January 2022. Then, following Russia's entry into the war against Ukraine, a spear-phishing campaign targeting private email accounts belonging to Ukrainian armed forces personnel began in late February. Finally, the data recovered through this phishing campaign was reused very quickly in order to carry out, in early March, a second campaign against Ukrainian refugees trying to flee the war. It seems that UNC1151 is closely linked to some groups of supposedly Russian origin.

E-CRIME (Conti)

C.I.S

Opportunistic
Big Game Hunting

Double-extortion tactic
E-Crime pioneer

#Conti is a doxware operated by the group Wizard Spider since February 2020. The malware follows the RaaS (Ransomware-as-a-Service) model.

Conti, as other sophisticated ransomwares, encrypts files using 32 concurrent threads simultaneously and utilizing all computing power. Conti has the capability to encrypt local hard drives, network shares and other devices on the local network with an AES-256 encryption key. As each key is unique for each victim, Conti operators cannot provide a decryption tool. Frequently, the malware is used as a secondary payload of a #Trickbot or #BazarLoader infection. It also uses top open-source tools like #Meterpreter, #CobaltStrike or #PowerShellEmpire. Parts of data stolen are then leaked on the DLS website, to increase the pressure on the victim to force the payment.

More recently, the Conti malware has been in the news following claims of support for Russia by its operators. Then, just a few days later, a very large data leak impacted the group, including months of internal exchanges and the contents of the malware's source code publicly disclosed.

Capgemini

CYBER-WEATHER
Spotlight

TLP:WHITE

VULNERABILITY

CVE-2022-21882:
Window Object Type Confusion
Local Privilege Escalation Vulnerability

On February 4, CISA added CVE-2022-21882, also called "Window Object Type Confusion", to its list of known exploited vulnerabilities, "based on evidence that threat actors are actively exploiting". Discovered on January 13, this vulnerability impacts Windows systems and corresponds to a local privilege escalation where an attacker could easily gain system level privilege (CVSS Score of 7,2).

The vulnerability corresponds to a bypass of CVE-2021-1732, previously used by APT groups. Both vulnerabilities abuse Win32k, a windows component in relation with the graphical drivers.

The exploit uses GUI API functions to make kernel calls, and in particular a function (xxxClientAllocWindowClassExtraBytes) that will allocate space in the user mode desktop heap. After having hooked this function, the exploit code changes the flag ConsoleWindow of the tagWND object. The system does not check this flag change, resulting in type confusion : the type of the changes from user mode pointer to kernel heap offset, controlled by the attacker. The attacker can thus read and write out-of-bounds in kernel memory to acquire system level privileges.

Proofs-of-Concept are available on GitHub and the complexity of exploitation is low. Even if the vulnerability has been disclosed in January, a security researcher, Gil Dabah, claims that he published the vulnerability two years ago on Tweeter, but did not submit it to Microsoft due to the company's bad management of bug bounty awards.

Course of action

1. It is strongly recommended to update vulnerable systems with Windows January patch (KB5009543)

➢ Windows affected systems are :

- Windows 10 versions 1809, 1909, 20H2, 21H1, and 21H2,
- Windows 11,
- Windows Server 2019 & 2022.

2. In the meantime :

➢ If an Intrusion Detection System (IDS) is available, update its configuration with SNORT rules released by Cisco Talos researchers (SIDs 58859 and 58860).

Vulnerability, Local Privilege escalation, CVE-2022-21882, CVE-2021-1732, Window Object Type Confusion, Win32k, OOB read/write, kernel, CISA

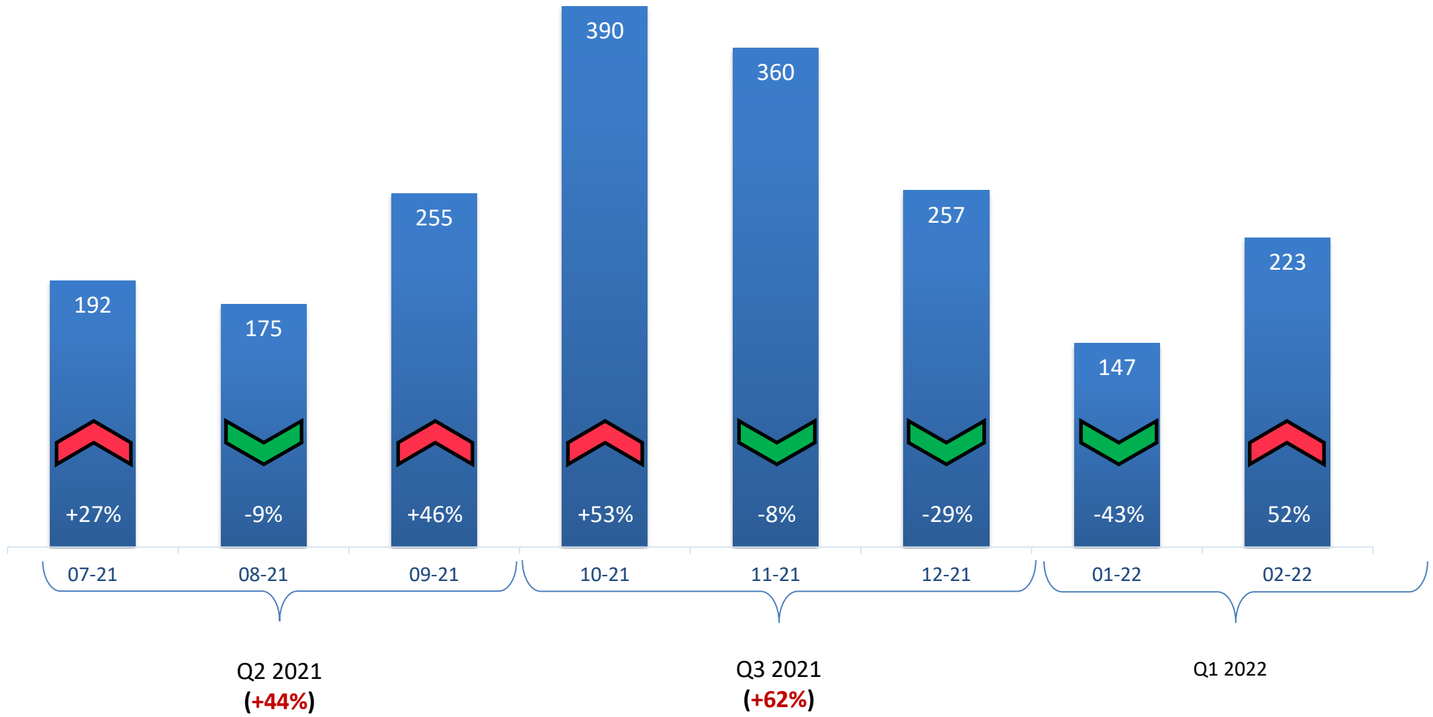
Patch, IDS, Snort, Win10, Win11, Windows Server

Capgemini

TLP:WHITE

CYBER-WEATHER

Evolution of top-tier ransom-dox-wares



Q2 2021 (+21%)

07-21

DARKSIDE | AVADDON | BABUK

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

08-21

LOCKBIT

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

BLACKMATTER

#BlackMatter could be based on the code source of #Darkside

PYSA | Cl0P | CUBA | PAYLOAD.BIN

#Pysa, #Cl0P, #Cuba and #Payload.bin returns this month

09-21

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

Q3 2021 (-2%)

10-21

LOCKBIT | PYSA | CONTI | SPOOK

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

11-21

LOCKBIT | PYSA | CONTI | SPOOK

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

12-21

LOCKBIT |CONTI | PYSA

General decrease of total number of victims. #Lockbit, #Conti and #Pysa still lead the board

KARAKURT

#Karakurt starts its activity with 33 victims

Q1 2022

01-22

CONTI | LOCKBIT | KARAKURT

Significant decrease of activity. #Lockbit leads the board with 5 victims

02-22

CONTI | LOCKBIT | KARAKURT | ALPHAV

#Conti activity continues despite leaks. #Lockbit leads the board by far. #AlphaV and #Karakurt are the most active behind the leaders