CYBER INTELLIGENCE
Threat
INSIGHTS

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

WEAK SIGNALS FOR STRATEGIC CTI & CYBER DECEPTION

Lessons from NATO-Russia disputes in Ukraine

On January, 14th 2022, a massive cyber-operation has been launched against multiple strategic entities (Government bodies, infrastructures, IT companies…) amid both verbal and military tensions escalations between #Russia and between #Ukraine and its occidental countries supports.

As of writing a little is known : we get evidence that multiple wipers disguised in ransomwares infected Ukrainian systems following governement websites defacements with highly political messages displayed. The ruse is that the "ransomwares" overwrite the Master Boot Record which in reality wipe OS files and lead to a physical disruption.
We can thus stand that the primary motivations of the attackers are not economic and likely political.

Based on the timeline of the events, the propension of Ukraine to embody a target of interest for its neighbour, the strategy of Russia to engage in hybrid conflicts where the cyber medium is also important that the physical/military one, it's likely that Ukraine is actually targeted by Russian APT groups.

Foreign intelligence services (#SVR) or domestic intelligence ones (#FSB) linked threat groups are likely directed to low noisy cyber-espionnage operations while military intelligence directorate (#GRU) units are less affraid of light and can more perform disruption operations than their colleagues.

For the defacements that occurred, Ukrainian authorities blamed the Belarus-nexus threat actor #UNC1151. Concerning the destructive cyber-attacks, the incriminated threat group might be #APT29 which the toolset overlap TTPs employed. But, and it's a big "but", APT29 is believed to be part of the SVR foreign intelligence service who usually doesn't rely on sabotage operations.

Some points that those wipers also overlap with the so-called #Sandworm Team which has already targeted Ukrainian critical infrastructures between 2015 and 2017. Moreover, Sandworm Team is associated with the GRU, it could thus also have worked in conjunction with Ghostwriter operators.

Numerous #Occidental countries such as the #United Kingdom and #France have explicitly condemned the troops deployment near to the Donbass region's frontiers and have adopted a though rhetoric instead of the usual consensual diplomatic tone.

#Russia might use all its #privateers ecosystem and particularly its Top Tiers ransomwares as a retaliation against the alleged interferences of Paris and London.
On January, 17th, #Lockbit ransomware operators claimed to have breached networks of a dedicated citizen-friendly portal powered by the French Ministry of Justice. Lockbit is one of the #eCrime groups whose narrative is the most aligned with the Russian geostrategic interests.

Based on it, we believe with medium confidence that in a short-medium term, West-european countries (and particularly ones that try to acting as a go-between Ukraine and Russia) could be heavier targeted than before by eCrime privateers groups via their ransomware payloads such as #Conti, Lockbit and #Blackcat.

- 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 actionnable IoCs and detection tips.

Russia, Ukraine, SVR, FSB, GRU, UNC1151, APT29, Sandworm Team, Occidental countries, United Kingdom, France, Privateers, Lockbit, eCrime, Conti, Blackcat, patching/monitoring

Capgemini

CYBER-WEATHER
Spotlight

APT (Sandworm)

Russia

Occidental countries
Post-soviet countries

Petya
Crashoverride
Black Energy
ICS oriented targeting

#Sandworm (aka #Voodoo Bear, #Telebots) is a Russian APT group believed to operate on behalf of the Russia's Federation serving the Russian Military Intelligence Directorate (#GRU).

Sandworm usually targets former USSR countries but also Occidental ones with #disruption oriented toolset to destabilize and impact critical infrastructures. It's thus heavily monitored by Government bodies and energy enterprises because it concentrates its targeting to ICS/SCADA environments following the geopolitical agenda of Moscow. Active since 2007, Sandworm doesn't look for zero-day vulnerabilities or exploits but seem to leverage common exploitation behaviours such as spear phishing campaigns, custom and unique RATs but also highly sophisticated #wipers (such as Petya or Crashoverride).

In the wave of escalating tensions between Russian and Ukraine, #critical infrastructures in the latter were targeted by wipers malwares disguised as ransomwares ones. Even though no attribution could be made as of writing, it's important to recall that Sandworm is historically the preferred disruption's arm of Moscow.

E-CRIME (Hive)

C.I.S

Opportunistic
Big Game Hunting

Golang
ConnectWise
CobaltStrike

#Hive is a doxware that follows a Ransomware-as-a-Service scheme first spotted in June 2021.

Hive has rapidly attracted law enforcement eyes and particularly FBI ones when it seemed to have a healthcare targeting tropism. The ransomware has pretty classical TTPs : it employs either #ConnectWise of #CobaltStrike to breach corporate networks but a few phishing campaigns have been detected, delete shadow copies to prevent recovery and exfiltrate data to its dedicated data leak site (DLS) dubbed *HiveLeaks*.
It's noticeable that similarly to AvosLocker or Lockbit, Hive can target VMware ESXi hypervisor on Linux OS. This development is justified the need for ransomware operators to enlarger their targeting scope.

The Capgemini CERT-E intelligence unit has faced various incidents related to Hive infections on our partners's clients through January. It highlights the growing popularity of Hive within the eCrime ecosystem thanks to an absence of code of conduct (for example, several ransomware operators claim to not target charities, NGO's or healthcare institutions), an efficient DLS and a targeting of mediatic victims.

Capgemini

CYBER-WEATHER
Spotlight

VULNERABILITY

CVE-2021-4034:
PwnKit, Polkit pkexec Local Privilege Escalation Vulnerability

The November 18th 2021, Qualys Research Team reported a vulnerability about Polkit 's module, Pkexec. An attacker could elevate its privileges to root from any profile by exploiting this vulnerability.
PolKit, formerly called PolicyKit, can distribute and control privilege on Unix operating system. the module, pkexec manage processes to render unprivileged ones to communicates with privileges ones, by executing pkexec followed the unprivileged command with root rights. CVE-2021-4034, aka PwnKit, stays limited to attackers with a local access to the system.
The module do not anticipate that number of argument that could be passed to execve() function will be 0 and then allow introduction of an unsecured environment variable even if those kind of variable are deleted from pkexec environment.
This vulnerability is present on all versions of Polkit since its creation in May 2009 but is limited to operating system that do not restricted execve() number of argument, like Ubuntu, Debian, Fedora, and CentOS. This vulnerability cannot be exploited on OpenBSD as it refuses to passed execve() argc to zero.
This is not the first time PolKit is compromised in 2021 as another privilege escalation was available through CVE-2021-3560 but was limited to Polkit version 0.113 to 0.118.

Course of action

1. It is strongly recommended to update vulnerable systems as soon as a patch is available to cover the vulnerability.

➢ For example, Ubuntu following versions are patched: : 14.04, 16.04 ESM, 18.04, 20.04, et 21.04

2. If it’s impossible :

➢ Change Polkit pkexec binary right to remove SUID-bit:

 # chmod 0755 /usr/bin/pkexec

In addition, if the exploitation of this vulnerability can be found in system logs:

➢ search for the following sentences:

- ➢ *“the value for the SHELL variable was not found the /etc/shells file”*
- ➢ *“The value for environment variable [...] contains suspicious content”*

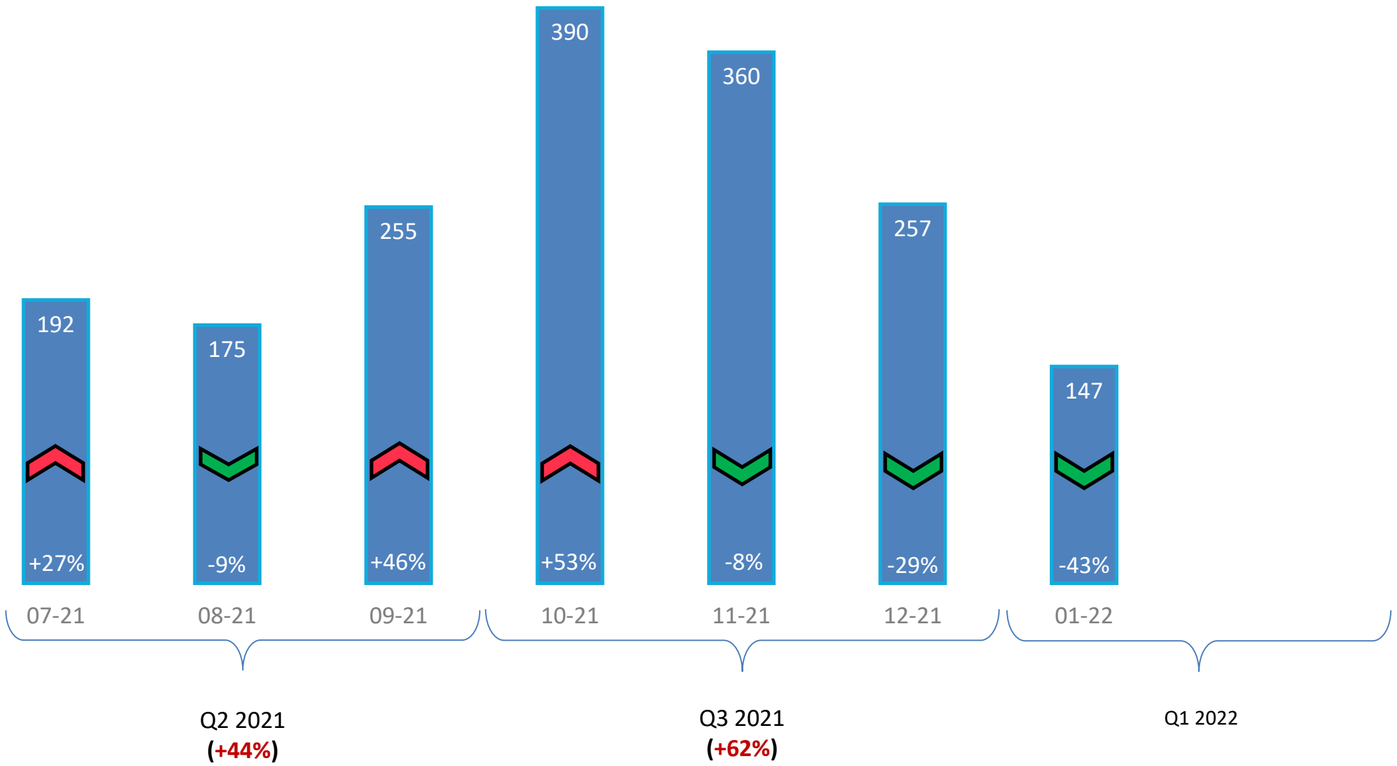
Vulnerability, Unix, Polkit, pkexec, PwnKit, Local Privilege escalation, CVE-2021-4034, CVE-2021-3560, Ubuntu, Fedora, Debian, CentOS

Patch, configuration, logs

Capgemini

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 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

11-21

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

12-21

LOCKBIT |CONTI | PYSA

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

KARAKURT

#Karakurt start its activity with 33 victims

Q1 2022

01-22

CONTI | LOCKBIT | KARAKURT

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