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

Business as usual for adversaries during Ukraine-Russia war

March was a though month for cybersecurity teams. Beyond claims of compromise by hacktivist threat actors on both the Ukrainian and Russian sides, eCrime & APT adversaries continue to follow their doctrines of engagement.

On the eCrime side, our hypothesis is confirmed by the increasingly visible targeting of strategic entities: the French National Civil Aviation School (#ENAC) and the Romanian oil company #Rompetrol have been targeted by #Hive ransomware.

Another actor draw the cybersecurity community attention in March: threat group dubbed #Lapsus$ claimed to have breached big companies networks such as Microsoft, Okta, Samsung or Nvidia. Interestingly, this group doesn't seem to leverage ransomware payloads but rather focuses on data exfiltration operations. Even if Lapsus$ key members have been arrested by law enforcement in United Kingdom, it's unclear right now if they have the resilience to continue their operations.

On the APT side, china state-sponsored groups show growth in their cyberespionage operations : we can quote #APT31, #APT41 and #Red Delta intrusion sets that have been the subject of several threat advisories from cybersecurity editors in March.

The cybercriminal landscape continue its evolution through what the CERT-E already hypothesized earlier: if the double extorsion scheme (i.e encryption followed by data exfiltration on data leak sites) remains the most common tactic for top eCrime groups, weak signals suggest that a shift is pending for threat actors that explore the possibility to concentrate themselves on #data exfiltration followed by public claims to monetise compromised data without the use of ransomware payloads.

Security researchers from SentinelOne, confirming analysis from the Ukrainian CERT, found that the PRC-linked threat group dubbed #Scarab (aka UAC-0026) performed intelligence collection oriented operations against Ukrainian entities without naming them. This is the first time that #Chinese actors are publicly suspected to attempt to compromise Ukrainian targets since the beginning of the Ukraine-Russia war.

This fact sheds light to the reorientation of CERT-E focus on adversaries that could harm our clients perimeter: we decided a the beginning of March to add Chinese actors to Russian ones as a result of our anticipation of the growing implication of Beijing in the Ukraine-Russia cyber conflict.

Chinese cyber adversaries may take advantage of the worldwide attention towards Russian threat actors to perform cyber espionage campaigns: CERT-E estimates the probability of the Western economic fabric being affected by Chinese actors in the actual context at medium.

We must recall that the China-backed threat actors remain a tough threat to Western organizations over the time.

Western companies are very concerned about cyber consequences of the war as companies located in #NATO countries or in ones that impose strong sanctions to Russia could be targeted by Moscow-aligned threat actors in retaliation. They thus could be also targeted by Beijing-aligned ones knowing weak signals that suggest a collaboration of China and Moscow in terms of cyber-operations.

A such focus could let opportunities for other advanced adversaries, such as Chinese ones, to take advantage of these opportunities to accentuate their traditional #cyber espionage operations and gather both economic and industrial intelligence

- Focus efforts on #patching/monitoring the most impactful flaws reported in our Flash-News produced by CTI team about last TTPs of such ecosystems. A Flash News has been sent about this topic with information regarding the monitoring of Russian threat groups by the CTI Team. Moreover, an updated advisory regarding Chinese actors is pending
- 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

ENAC, Rompetrol, Hive, Lapsus$, APT31, APT41, Red Delta, Data exfiltration, Scarab, Chinese actors, NATO, Cyber espionage operations

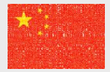
Capgemini

CYBER-WEATHER
Spotlight

TLP:WHITE

APT (Red Delta/TA416)

People's Republic of China



Occidental countries & NATO espionage

Phishing campaigns
PlugX malware

#Red Delta (aka #TA416) is an APT group believed to operate on behalf of People's Republic of China since 2020.

From reconnaissance steps begun in February to July 2020, Red Delta's operators have been observed targeting catholic minorities in China and catholic organizations based in Italy such as The Holy See. This targeting matches with the CCP (Chinese Communist Party) objectives to strengthen surveillance and control against Christians Chinese people viewed by Beijing authorities as a potential threat to the national security in China.

In the wave of escalating tensions between Russian and Ukraine, Proofpoint researchers identified that Red Delta conducted web reconnaissance campaigns in November and December 2021. Those phishing campaigns relied on base64 encoded email delivering PlugX malware to target in January 2022 European diplomatic entities. Then, following Russia's aggression against Ukraine and with the focus performed by the cyber community on Russian related groups, Red Delta is continuing their phishing activity using compromised email addresses of a diplomat from a European NATO country. The technical level of those campaigns has greatly evolved during the last two years, latest version containing command obfuscation.

E-CRIME (Lapsus$/DEV-O537)

Worldwide

High-tech Focus
Big Game Hunting

Double-extortion tactic
E-Crime rookie

#Lapsus$ (aka #DEV-O537) is an eCrime group that started its operation in 2021. This group is believed to be composed of worldwide members.

Despite most of actual eCrime actors, they are not using ransomware (at least for the operations claimed under the Lapsus$ flag) but they focus on data exfiltration rather than encryption. The first victims were in South America and in Portugal. Since they have targeted major IT and High-Tech companies like #Nvidia, #Samsung, #Ubisoft, #Microsoft, #Okta, #Globant, #LG and #Vodafone to leverage their access from one organization to access the partner or supplier organizations. #Lapsus$ actors focused their social engineering efforts to gather knowledge about their target's business operations and to recruit insider for access to credentials and MFA approval. They have been also observed using stolen source code and certificates in order to obfuscate backdoors or trojans. The group prefers a private Telegram channel instead of the more traditional data leak sites.

London's Police has arrested seven teenagers connected to the #Lapsus$ data extortion gang on March 24th. Even if many important members have been arrested, the group could not be down for good. After having announced that the group will take vacation until late of March, it came back to its operations March 30th by leaking data from #Globant IT.

VULNERABILITIES

CVE-2022-1040: Sophos Firewall

On the 28th of March, a critical bug scoring 9.8 out of 10 affecting Sophos Firewall devices has been reported to Sophos via their bug bounty program and has been added by CISA to its "Known Exploited Vulnerability Catalog".
The vulnerability corresponds to a RCE (Remote Code Execution) allowed by a bypass of the firewall's admin panel. No technical information has been provided by the editor.

Affected Versions

Sophos Firewall v18.5 MR3 (18.5.3) and older.

Course of action

A hotfix has been released by Sophos and it is recommended to apply it as soon as possible, in addition to enable the feature "Allow automatic installation of hotfixes". If patching is not possible, Sophos explains that their customers can mitigate the vunerability by ensuring that the webadmin and user portal are not exposed to the internet, and rather use VPN or Sophos Central (their cloud-based device management portal) for administration actions.

Sophos, SonicWall Firewall, RCE, Patch

CVE-2022-0847: Dirty Pipe

Disclosed in the beginning of the month with a CVSS score of 7.8, CVE-2022-0847, also dubbed Dirty Pipe, is a Linux kernel vulnerability allowing local privilege escalation. The vulnerability, affecting a wide range of systems, is easy to exploit with various PoC available.
The vulnerability allows to write in any file where the attacker have read permissions, thus giving the possibility to elevate its privileges by various techniques (by adding a new user in /etc/passwd file or by modifying a script or binary executed with elevated privileges for example). The weakness resides in the bad handling of page caches by the Linux kernel, and particularly by not correctly resetting the flags managing the page caches while using pipes (used for communication between processes). The attacker can then write in a previously used pipe, and the kernel will synchronize page cache data with the file on the disk (opened by the attacker in reading mode), thus rewriting it. The kernel function writing data in the pipe never checks the user's rights.

Affected Versions

Linux kernels from version 5.8.
NB : Datadog released a PoC showing that it is possible to break out from unprivileged containers.

Course of action

Apply patches (update to Linux kernel versions 5.16.11, 5.15.25, and 5.10.102 or later)

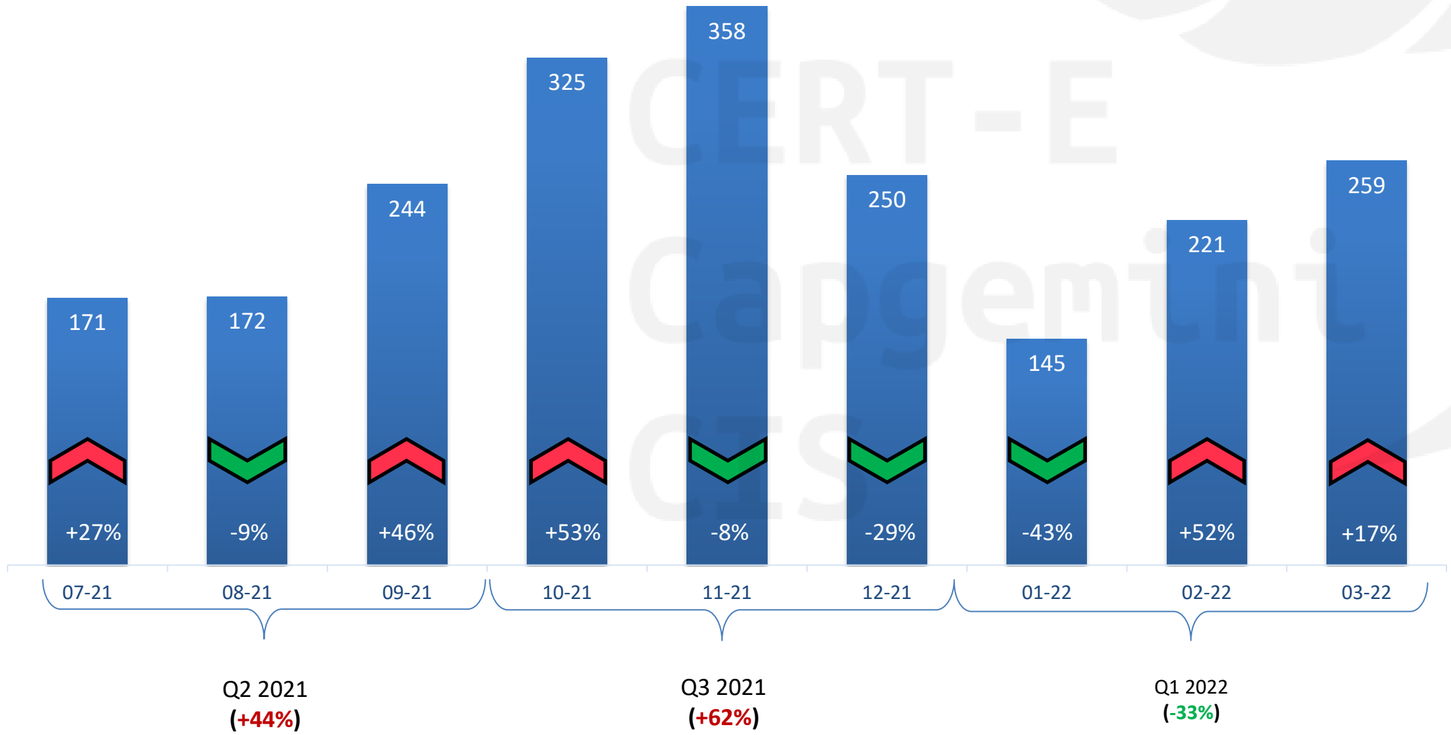
Dirty Pipe, LPE, Linux, Container, Patch

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 followed by #Conti and #Pysa. #Prometheus rebrands as #Spook at the end of September. #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.
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 (-33%)

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

03-22

CONTI | LOCKBIT

#Ukranian conflict does not change the landscape as #Conti and #Lockbit leads the board by far.