TLP : WHITE

Capgemini

ANNUAL THREAT REVIEW 2021

CERT-E CIS

Prepared by the Cyber Threat Intelligence Unit

Table of Contents

Public. © 2022 Capgemini. All rights reserved.

Disclaimer:

The information you have accessed or received is provided "as is" for informational purposes only.

The Capgemini CERT-E CIS does not provide any warranties of any kind regarding this information.

In no event shall the Capgemini Company or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages, arising out of, resulting from, or in any way connected with this information, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the information.

The display of the Capgemini seal or other Capgemini visual identities, including the Capgemini CERT-E CIS name or logo shall not be interpreted to provide any person or organization the authorization to use the official seal, insignia or other visual identities of the Capgemini CERT-E CIS.

The Capgemini seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by Capgemini or Capgemini CERT-E CIS. All content on this report is **TLP:WHITE**. Sources may use **TLP:WHITE** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restrictions.

For more information on the Traffic Light Protocol, see: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol

Capgemini CERT-E CIS does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by Capgemini CERT-E CIS.

In case of questions, comments, or suggestions, kindly write to this address:
sogetiesecctiteam.eur@capgemini.com

Methodology

This research paper aims to present to the reader the main facts of interest observed in cyberspace within the year 2021 (from 1 January 2021 to 31 December 2021). It is based on the data analyzed by the CTI unit in its monthly "Cyber-Weather" reports. All the threat groups and all the malwares are therefore voluntarily not covered: only those on which the CERT-E CIS worked during its "Cyber-Weather" are mentioned.

It is intended for both strategic (CxOs) and technical audiences who wish to better understand the threat landscape that cyber threat intelligence researchers face.

This paper is not intended to be exhaustive and, like any research work by an IT company, is necessarily oriented towards the cyber threats likely to affect CERT-E CIS clients.

To make the identification of adversaries easier, CERT-E CIS uses in this paper the taxonomies of the security companies Crowdstrike[1] for eCrime groups and Mandiant[2] /Crowdstrike for APTs groups. Where a group is better known by a name given by another vendor than these two, it will be used.

[1] https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/
[2] https://www.mandiant.com/resources/apt-groups

Public. © 2022 Capgemini. All rights reserved.

Glossary

eCrime: Adversaries typically involved in financially motivated operations, historically less skilled than APT actors, and which do not pursue geopolitical agendas

Doxxing: Tactic of an adversary aimed to publish victims' data on a webpage in order to pressurize them to pay a ransom or a money amount

Doxware: Contraction of "ransomware" and "doxxing" to designate a ransomware that practices the doxxing (also known as double extorsion tactic)

RaaS (Ransomware as a Service): Adversary scheme in which the ransomware developers sell the use of their payload to affiliates in exchange of fees

MaaS (Malware as a Service): Adversary scheme in which the malware developer sells the use of its payload to other threat groups in exchange of fees (see RaaS)

IaaS (Initial access as a Service): Also known as Initial Access Broker (ISB), adversary scheme in which the threat actor is tasked to breach and gain foothold on the victims' networks in order to facilitate a second stage infection, typically with ransomware payloads in exchange of fees

APT (Advanced Persistent Threat): Adversaries typically involved in cyberespionage or disruption operations, historically highly skilled, most of the time follow a geopolitical agenda and aimed at being uncovered and persistent for a long period in the victims' networks

BGH (Big Game Hunting): Adversaries scheme where cybercriminal groups focus their targeting on companies that are large enough and have sufficient turnover to expect a high ransom

Privateers: Sophisticated and impactful cybercriminal groups pursuing Big Game Hunting and being allegedly supported or at least indulged by the states that host their infrastructures

SVR (Sloujba vnechneï razvedki Rossiskoï Federatsi): Foreign intelligence service of the Russian Federation

FSB (Federalnaïa sloujba bezopasnosti Rossiyskoï Federatsii): Domestic intelligence service of the Russian Federation

GRU (Glavnoïé Razvédyvatel'noïé Oupravlénié): Military intelligence service of the Russian Federation

MSS (Ministry of State Security): Main intelligence service of the People's Republic of China

DHS (Department of Homeland Security): United States Homeland Security department

DoJ (Department of Justice): United States Justice department

NSA (National Security Agency): United States intelligence service focused on technical intelligence; mainly signals intelligence and cyber intelligence

DLS (Data Leak Site): Website hosted either on clear or darkweb on which threat actors publish exfiltrated data of victims' networks

Rebranding: Strategy for an adversary to use a different name or a different payload to evade law enforcement tracking

ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information): French national information security agency

Public. © 2022 Capgemini. All rights reserved.

Oligopolisation: Market structure where a small number of actors share the market dominance. In this paper, the word must be understood as the domination of a small number of threat actors on the cybercriminal ecosystem

Cartelization: Phenomenon where cybercriminal actors make agreements or cooperate to bolster their efficiency and their resiliency

Public. © 2022 Capgemini. All rights reserved.

In a nutshell

The year 2021 has been a particularly good one for ransomware operators and for members of nation-state groups. Boom of the doxxing phenomenon, restructuring of the cybercriminal threat landscape around cartels, massive exploitation of zero-days for cyber espionage purposes, targeting of critical infrastructures by unusual actors... Here is what to remember:

- **Explosion of double-extortion tactic within the cybercriminal ecosystem**

  The cybercriminal threat landscape is becoming increasingly adaptive and innovative. eCrime actors are copying what works in order to maximize their profits. In this case, the phenomenon of doxxing had its moment of glory in 2021, with nearly 2,408 compromises reported. The eCrime sphere is also structured into cartels or workgroups involving a division of labor between actors responsible for gaining a footprint in the network and those responsible for exfiltrating and/or encrypting them, all based on a flourishing economic model.

- **Targeting of strategic sectors and companies by privateers**

  The traditional "cybercriminal actors/APT" division on the main criterion of the adversary's affiliation with a government (and by extension support for its foreign policy) is increasingly being questioned. Weak signals have been accumulating that point to the involvement of several threat groups that were initially financially motivated but have turned out to be surrogates in cyber operations to destabilize Western countries. These privateers groups operate in a grey area: in exchange for not targeting the countries of the former USSR, they likely operate with less fear of law enforcement and thus likely target sensitive companies or administrations in countries in diplomatic trouble with the Russian Federation.

- **Restructuring of the cybercriminal landscape following numerous takedowns**

  In addition to being adaptive and innovative, eCrime actors are also resilient: by trying to attack strategic companies for states, they are more likely to be the target of takedown operations. These have increased significantly (both in volume and in media coverage) because of shared public-private initiatives and as a result of inter-state partnerships. Although some have been successful, adversaries have become more imaginative and agile in their relentless rebranding strategies to confuse, create other payloads or migrate to more sophisticated groups.

- **Rapid and methodical exploitation of zero-day vulnerabilities by the APT ecosystem (and eCrime...)**

  Technological convergence leads to an increased dependence of companies on the same technologies, which can have serious consequences when critical vulnerabilities affect them. It happened to Microsoft Exchange servers, where several CVEs were released in March and were quickly exploited by threat actors, most of them Chinese-speaking[3]. The ProxyLogon and ProxyShell flaws were exploited by both APT groups (APT31 and APT40 groups have been publicly accused by some Western countries) and, less commonly, by eCrime ones shortly after they were made public. It should also be noted that these groups are becoming more sophisticated and are now able to use zero-days to carry out compromises with global repercussions such as those that affected Kaseya or Accellion.

[3] At our best knowledge

 © 2022 Capgemini. All rights reserved.

Public. © 2022 Capgemini. All rights reserved.

1 Dancing with the Spiders: a boom year for the eCrime ecosystem

In 2020, we counted 578 companies or institutions whose data were exposed on data leak sites (DLS) operated by ransomware groups. In 2021, this number has more than quadrupled to 2408, an increase of almost 316%.

This exponential growth is not really surprising: the phenomenon of doxxing as adopted within the cybercriminal ecosystem (eCrime) was initiated by the Twisted Spider group (aka TA2101) via its Maze ransomware and by DoppelSpider via its DoppelPaymer ransomware in Autumn 2020. One of the main characteristics of this ecosystem is its high degree of adaptability and replication. In other words, "we copy what works". It is clear that Maze has quickly become the leader in double extortion tactic[4], followed by other strains to increase their turnover[5].

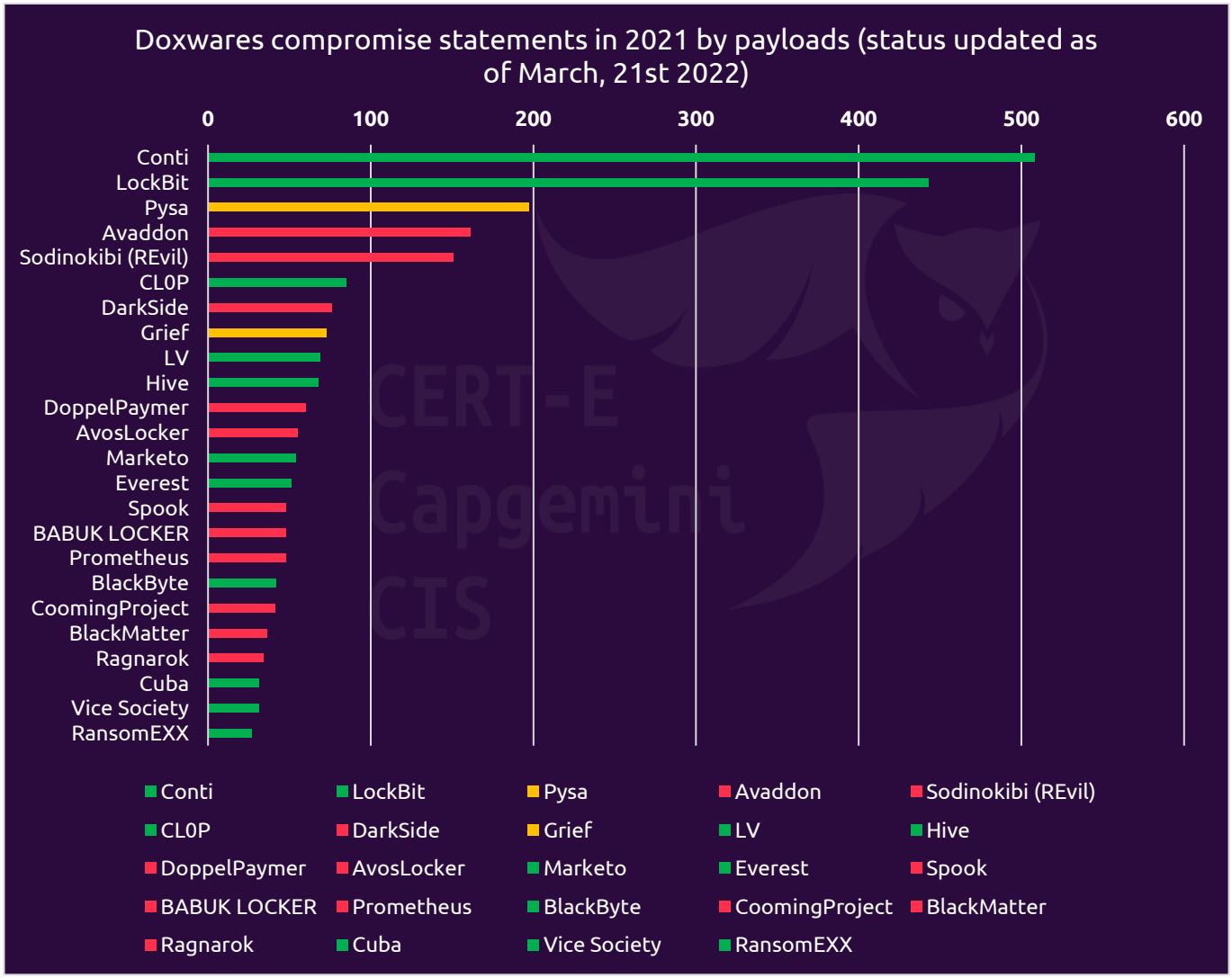
If at the beginning of 2020 there were two active doxwares[6] namely Maze and DoppelPaymer, at the end of 2021 we can monitor more than 60 doxxing sites. Such developments do not happen by chance.

[4] The double extorsion tactic means that the threat group not only encrypts data but also exfiltrate them on a blog hosted either on the clear or darkweb to pressurize victims and force them to pay to avoid brand image damage
[5] Targeting of large corporate networks with the aim of maximize turnover can be referred as Big Game Hunting (BGH) operations
[6] Contraction of « ransomware » and « doxxing »; means that ransomware operators use the double extorsion tactic

 © 2022 Capgemini. All rights reserved.

Legend:

- Shutdown or seized
- Online and inactive
- Online and active



One of the first reasons is the structuring of the ecosystem around the phenomenon of Ransomware as a Service (RaaS). This model consists of applying Taylor's division of labor to the distribution of ransomware: the group developing the ransomware will recruit individuals (called "affiliates") to act as cyber-extortion subcontractors. They will collect the ransom and keep a percentage of it agreed in advance with the developer, who will be responsible for centralizing and supervising operations. The field of possibilities is thus widening with multiple actors having been selectively recruited.

Another explanatory factor can be found in the concomitant development of the Initial Access as a Service (IaaS) landscape (aka access brokers or loaders). The malware that makes up this category falls into the MaaS category[7]: it most often has Tactics techniques and procedures (TTPs) that categorize it as a banking trojan, particularly because of its RAT, spyware, and mass (but also targeted) phishing infection capabilities. This malware is rented by ransomware operators for a share of the ransom for IaaS developers to penetrate the targeted systems and

[7] Initial access as a Service (IaaS) malwares and Ransomware as a Service (RaaS) payloads are part of the Malware as a Service (MaaS) ecosystem

Public. © 2022 Capgemini. All rights reserved.

open the way for the payload to be dropped. Beyond the purely commercial relationship, real organizational and financial links have been established between these two ecosystems. The most famous loader, Emotet, is developed by the Mummy Spider group. It turns out that this group has close links with the Wizard Spider group developing Conti and Ryuk ransomwares. Other examples can be found in the work done by our colleagues at Crowdstrike on this subject[8]. It is important to note that this growing collaboration accelerated extremely in 2021 with the appearance or reinforcement of loader capabilities that increased the rate of ransomware compromises (note the loaders Emotet, Trickbot, Qbot, IcedID, Bazar, Dridex, SquirrelWaffle, Zloader etc.). The compromises studied in 2021 highlight triple chain attacks or double chain attacks:

- In the first case, three different malwares have been observed: for example, Emotet, Trickbot and Ryuk
- In the second case, two different malwares have been involved: for example, Qbot and Conti

Note that most often, the last step in the chain (i.e., the ransomware) is dropped via the use of an open-source offensive tool such as Cobalt Strike beacons or Metasploit.

The final factor that can justify such a growth in the number of compromises in 2021 is the phenomenon of cartelization of the cybercriminal sphere.

"Unity creates strength". Cyberspace is not a fixed and hermetic space. Cybercriminal actors can therefore be led to talk to each other, to collaborate, as seen above, between ransomware operators and loaders, and even to build relationships of trust, as long as their objectives are common. Thus, following the example of the development of IaaS, ransomware operators have tended in 2021 to carry out joint compromises. These ones are often claimed on the doxxing website of each of the participants in the form "Provided by xxx Team" or "xxx Cartel". Let us recall that in 2021 the number of operators wishing to carry out doxxing has exploded, reducing de facto the market share of the "historical leaders"[9]. The latter, forced by the competition to renew themselves in order to avoid financial losses, had no other choice than to form alliances. Affiliates were thus able to become fully-fledged groups but still linked to the central group. This movement, which we (until very recently) called the cartelization of the cybercriminal ecosystem, already has a number of telling examples (remember that these assumptions of links have to be considered as is and that there can always be false flag and/or errors):

- **Witchcraft Cartel**: Wizard Spider (Ryuk/Conti) as flagship, privileged links with Mummy Spider (Emotet), Lunar Spider (IcedID) & Mallard Spider aka Lockean (Qbot)
- **Labyrinth Cartel**: Maze in flagship, rebrand or shift to Egregor + links in the past with Sekhmet, Lockbit & Viking Spider (Ragnar)
- **Boxing Cartel**: Pinchy Spider (Sodinokibi/rEvil), once shut redirect to RAMP led by Groove & Babuk
- **Carbon Spider**: Darkside/Darkmatter/Blackmatter/Blackcat (aka ALPHV)

While these different cartels have been able to collaborate with each other, notably to share techniques, infrastructures, and doctrines, it's less likely that they shared profits too. For example, members of the Witchcraft and Labyrinth cartels have been able to maintain links to the point of forming a single cartel[10]. However, Capgemini CERT-E CIS finds this assertion not very credible considering the tactical differences and the various accusations made by one group against the other in hacking forums posts.

During 2021 a certain purge took place within these cartels: Maze, Egregor, Sekhmet, Sodinokibi, Darkside, Darkmatter & Blackmatter were deactivated. Others such as Lockbit have ceased operations but have returned under a different name (although it cannot be said as of writing that the Bitwise Spider group behind Lockbit 2.0 is the same group behind the original Lockbit).

Nevertheless, with the exception of the Boxing cartel, which seems more committed to maintaining the RAMP exfiltrated data resale platform, and the Labyrinth cartel, these cartels have shown resilience as they maintain at least one strain (Conti & Blackcat) in the Top 5 most impactful ransomwares.

[8] https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
[9] Historical « leaders » of the ransomware game are also known as Top Tiers groups
[10] https://www.cbsnews.com/news/ransomware-cybercrime-cartel-wizard-spider-viking-spider-lockbit-twisted-spider/

 © 2022 Capgemini. All rights reserved.

2 Privateers threat actors: through the cyber-warfare fog

While 2021 was a particularly good year for the eCrime ecosystem, the response of law enforcement agencies and more generally of governments was structured in parallel, leading to numerous operations to dismantle ransomware infrastructures.

The boom of the doxxing phenomenon in 2021 has been accompanied by the birth of another modus operandi called Big Game Hunting (BGH). BGH consists of cybercriminal groups focusing their targeting on companies that are large enough and have sufficient turnover to expect a high ransom. Beyond the financial interest represented by these companies, the aspect of brand image should not be overlooked. As we have seen, there are more and more ransomware operators seeking to dominate the eCrime scene. One way to win the competition is therefore to target entities with high media impact in order to gain notoriety and attract more and more affiliates.

Wherever, BGH also carries risks for operators: by targeting governmental, institutional services or critical infrastructures, they inevitably attract the attention of law enforcement and intelligence services. As an example, we can cite two events that have supported a shift in doctrine in terms of the fight against ransomware.

On May 6, 2021, Colonial Pipeline was targeted by the Darkside ransomware (operated by the Carbon Spider group). 45% of the fuel consumed by the East Coast of the United States passes through Colonial Pipeline's infrastructure, so such targeting can have serious economic and social repercussions. The highly publicized compromise led to President Joe Biden declaring the emergency state on May 9 and major supply disruptions were experienced.

On May 30, 2021, the world's leading meat producer JBS was compromised by the Sodinokibi/Revil ransomware (operated by the Pinchy Spider group). This attack caused several shutdowns of meat production, especially in the US and Canada. Considering the critical size of the company and its importance in the global supply chain, the US Department of Agriculture was concerned about the economic repercussions in terms of prices and stock-outs.

Recognizing that ransomware could now impact significant parts of the economy and pose national security problems, the US adopted a new doctrine to combat ransomware. A ransomware Task Force was created on July 14, 2021, by the Biden administration, bringing together IT security companies, critical infrastructure providers, federal agencies and intelligence services. This Task Force aims to better coordinate the response to ransomware attacks, to streamline the sharing of indicators of compromise and to study the opportunity of offensive operations (so called hack-back) when necessary.

Thus, in our opinion, it's highly likely that the United States will perpetuate hack-back operations when strategic U.S. entities are hit.

On May 14, 2021, the operators of the Darkside ransomware announced that they had lost access to their public infrastructure and cryptocurrency funds. They therefore announced the cessation of their activities. On June 7, 2021, the US Deputy Attorney General Lisa Monaco announced that the Federal state had been able to recover $2.3 million in Bitcoins out of the $4.4 million paid by Colonial Pipeline, without giving any further details about the method used to access the attackers' wallet.

On July 13, 2021, shortly after another high-profile supply-chain attack on the Kaseya software company, Sodinokibi/Revil ceased operations (assumed for fear of suffering the same fate as Darkside). Despite attempts to recruit new affiliates and revive its operations, the group announced in October that it believed it had been hacked and permanently ceased operations. On January 14, 2022, the Russian internal intelligence service (FSB) conducted a large-scale operation based on information sharing with the United States (surprisingly), which led to the arrest of several members of Pinchy Spider and the dismantling of the group.

Ironically, the year 2021 was both one in which the number of compromises by doxxing was the highest and one in which several leading groups disappeared or were dismantled by law enforcement agencies: Egregor, Netwalker, Avaddon, Darkside (and its rebrandings) or Revil.

This ransomware hunt by Western states is creating a clear mess in the eCrime ecosystem and forcing ransomware groups to change their modus operandi or at least adapt. Amongst these changes, we can first note the security

Public. © 2022 Capgemini. All rights reserved.

hardening of DLS sites with anti-DDOS measures (ransomwares claiming to suffer such attacks, we can cite such protection for Lockbit 2.0 DLS or AvosLocker for example). The rebranding strategy is also growing; it consists of renaming the doxxing site or changing the strain with a different name in order to escape the law enforcement (it's for example emblematic of the Carbon Spider group which has rebranded Darkside into Darkmatter and then Blackmatter, but also of the Indrik Spider group which has rebranded WastedLocker into Hades, Phoenix and then Macaw Locker).

Finally, we can mention a better targeting of companies to avoid, as much as possible, hitting those that could be of strategic interest to states, although the equation seems complicated to solve for ransomware because these companies are often the ones with the biggest financial capacity.

We have seen that ransomware groups specialized in doxxing no longer hesitate to target strategic companies. This type of targeting, one that affects the fundamental interests of the affected nations, can be described as an act of cyber warfare. Depending on their doctrine of employment in cyberspace, states may have to retaliate and challenge those who are accused of facilitating their operations or at least allowing them to do so.

In the infosec community, APT groups are usually linked to nation-states tasking them of cyber espionage and disruption operations. These groups are usually characterized using custom toolsets and a sustained effort in terms of operational security (OPSEC).

In contrast, eCrime groups are generally financially motivated, act on their own behalf and often rely on open-source tools. Currently, a growing portion of the infosec community believes that many eCrime groups no longer meet these criteria. Our colleagues of Talos[11] have proposed a new taxonomy of the cyber threat landscape via the designation of privateers for sophisticated and impactful cybercriminal groups pursuing Big Game Hunting and being allegedly supported or at least indulged by the states that host their infrastructures.

The Capgemini CERT-E is in line with this naming evolution: groups such as Russian alleged linked Ryuk, Conti, Cl0p or Lockbit but also Iranian alleged linked ones such as Pay2Key or Netw0rm meet several of these criteria. Therefore, it's reasonable to assume that nation-states will continue to be lenient towards these groups as long as they do not target domestic companies. Moreover, while state cyber espionage groups are likely to remain, privateers are likely to grow significantly, as their operators take advantage of non-existent (or non-efficient) international cyberspace laws. Adversary states that rely on privateers can therefore deny having links with them while benefiting from the geopolitical consequences of their attacks (see Darkside involvement in Colonial Pipeline). In our opinion, the threat of privateers, which is more hybrid and involves more money, should be put on the same footing as that represented by state-run cyber espionage groups.

To conclude, as of writing, most of privateers are based in Russia or in former USSR union. Almost all privateers either, have kill switch embedded in their payload that terminate the encryption if they are run into systems located in this geographical area, or explicitly avoid targeting these countries because they're afraid to be shut down by law enforcement.

These actors really play with the fog: their primary motivation seem to be financial, but in fact they support geostrategic goals of countries that protect them. It's hard to estimate to what extend they're part of the state-sponsored cyber landscape adversaries. Even if most of them say they reject being politically instrumentalized, a few as Lockbit 2.0 have performed interviews on YouTube on the Russian OSINT channel[12] where the adopted rhetoric was clearly aligned with the foreign policy of Moscow in conflict with the US one. Moreover, in the light of the Russian aggression of Ukraine at the end of February 2022, some groups already accused of being privateers such as Wizard Spider (Conti) have published statements to support the Russian point of view saying that they won't hesitate to use their skills as a retaliation measure if western countries threatened Russian organizations.[13] This kind of statement validates our hypothesis of this growing ecosystem of privateers.

[11] https://blog.talosintelligence.com/2021/05/privateer-groups.html
[12] https://www.youtube.com/watch?v=ldgmx4ZCfFg&t=54s
[13] https://www.bleepingcomputer.com/news/security/ransomware-gangs-hackers-pick-sides-over-russia-invading-ukraine/

 © 2022 Capgemini. All rights reserved.

3 Let the zero-day hunting continue!

State-sponsored adversaries continue to hunt for zero-day vulnerabilities to compromise government networks and large strategic companies' ones. The speed of exploitation of these vulnerabilities shows once again that the speed of reaction of the detection teams is paramount to blocking compromise attempts as soon as possible.

The year 2021 was first marked by new information on the attack suffered by the company SolarWinds via its Orion solution. Although this compromise did not really originate from a particular CVE, SolarWinds remains the most significant supply-chain attack of the end of 2020 in that it revealed massive Russian-speaking state espionage attempts around the world. Although it's been more than a year since, the compromise of SolarWinds' Orion software continues to be the subject of new information as investigations into the scope of the attack make progress. Reputable sources reported to Associated Press (AP) news agency[14] that the threat group responsible for the breach had access to the mailboxes of several U.S. Department of Homeland Security (DHS) officials, including Chad Wolf, former DHS Secretary between 2019 and 2021. As a reminder, US officials attribute SolarWinds' compromise to the Russian APT group APT29 (aka Cozy Bear) supposedly affiliated to the Russian domestic and/or foreign intelligence services SVR and FSB. Moreover, key-stakeholders of the DHS' cybersecurity staff could have also been victims of compromised mailboxes, including ones in charge of hunting operations against foreign threat activities. The "Big Brother effect" allowed by supply-chain attacks shed light to the thorny issue of technological convergence with a restricted number of solutions sold and used by a large part of enterprises and public sector organizations. Software supply chain attacks leverage either the source code, update mechanism, or build processes of vendor software to compromise victims throughout three main vectors (3rd party updates, malware installed on connected devices or application installers) while being often overlooked by organizations. All these elements raise questions about the ability of nation-state-sponsored threat groups to gain access to information that would allow these ones to benefit from both strategic and operational intelligence. Thus, cyber espionage operations seem to be taking a new turn, which for the time being seems complex to counter.

Furthermore, zero-days, previously actively pursued only by state-sponsored adversaries, are also being hunted by cybercriminal groups. One example is the coordinated attack on the Accellion legacy File Transfer Appliance (FTA) product in January 2021. This supply-chain attack (like the one suffered by Solarwinds) was enabled by zero-day exploits unknown to the vendor and, surprisingly, proved to be in the possession of the Russian-speaking eCrime group Indrik Spider. It must be recalled that among Accellion FTA customers, we can find big companies such as Morgan Stanley or Shell but also civilian government entities such as Australian health and transport agencies.

According to the investigation of Accellion and FireEye Mandiant teams[15], Indrik Spider leveraged four vulnerabilities to target Accellion FTA both public and private customers worldwide namely the CVE-2021-27101/27102/27103/27104. In cases analyzed by Mandiant's teams, a webshell dubbed Dewmode was used to exfiltrate data that was then published on Cl0p ransomware DLS following blackmails extorsion attempts, although no ransomware compromises had been detected. It appears that Indrik Spider tried to diversify its modus operandi by focusing this time on data exfiltration rather than encryption. This event highlights the good comprehension by the eCrime ecosystem that the data and the brand image of companies or governments are a great way to pressurize victims and force them to pay.

If you're interested in cybersecurity stuff or if you're an IT security analyst, you've probably heard about massive exploitation of Microsoft Exchange servers in March 2021.

Microsoft released on March 2, 2021, out-of-band security updates after Chinese state-sponsored groups compromised Exchange servers. The unraveled 0-day vulnerabilities affect all versions of Microsoft Exchange server's internet facing on-prem solely and not Exchange online. Two of these vulnerabilities (CVE-2021-26855 and CVE-2021-27065) and the technique used has been given the name of "ProxyLogon".

[14] https://apnews.com/article/solarwinds-hack-email-top-dhs-officials-8bcd4a4eb3be1f8f98244766bae70395
[15] https://www.mandiant.com/resources/accellion-fta-exploited-for-data-theft-and-extortion

 © 2022 Capgemini. All rights reserved.

The state-sponsored threat actor that pioneered such attack is identified by the Microsoft Threat Intelligence Center (MSTIC) as Hafnium (most being tight to China). Microsoft stated that they detected multiple 0-day exploits leveraged to attack on-premises version of Microsoft Exchange Server only in a limited number of targeted attacks. However, after a couple of days and more perspective it turns out that the operation Exchange Marauder exploitation as a first stage was at least successful for a numerous of entities[16].

A timeline was published in a blog post from Domaintools[17] that took a look on the possibility of an exploitation of the CVE-2021-26855 as early as November 2020. When two proofs of concept, one developed in Golang programming language on GitHub and another one written in Python (with Chinese comments) was published on a TorPaste (a PasteBin-like hidden service), state-sponsored actors heavily entered the game exploiting vulnerables Exchanges servers. According to Microsoft[18] teams, the Chinese APT ecosystem led the exploitation mobilizing several threat actors (which is understandable given the cyber-espionage potential of theses exploits) with for example:

- Tick (aka Bronze Butler)
- Emissary Panda (aka APT27 & Luckymouse)
- Calypso
- Winnti (aka APT41 & Wicked Panda)
- Tonto team (aka CactusPete)
- Hafnium

Later, a second wave of mass exploitation of Microsoft Exchange servers leveraging this time multiple vulnerabilities tracked as ProxyShell was observed. ProxyShell is a set of three disclosed vulnerabilities revealed by Orange Tsai[19] at the BlackHat which is a pre-authentication Remote Code Execution. This set of vulnerabilities is more exploitable than ProxyLogon and Microsoft communication about it was confusing, which left numerous servers unpatched. Ransomware gangs like LockFile[20] have weaponized Proxyshell and PetiPotam[21], a vulnerability that allows a remote unauthenticated user to take over an Active Directory domain with a Certificate Service (ADCS) running, to breach in and encrypt data of tens of organizations. A list of more than 100000 vulnerable on-prem devices that was shared on an underground Russian forum (XSS) have been retrieved.

ESET researchers observed that more than 10 APT and eCrime groups were actively exploiting the flaws leading to the response of Microsoft by releasing a one-click mitigation tools followed by FBI removing China Chopper webshells on its own initiative from private companies on Premise Exchange servers, backed up by US Department of Justice (DoJ) decision[22]. On the same day, the DoJ publicly disclosed the indictment of four Chinese citizens[23] by a court in San Diego, California, charging them with unauthorized computer intrusions, theft of intellectual property, trade secrets and information related to infectious disease research. Three of the individuals are identified as working for the Chinese Ministry of State Security (MSS), and one is identified as working for a company suspected of acting on behalf of the MSS. These statements came in a sustained effort of the Biden administration to systematically publicly hounded the responsibility of adversary states in cyberattacks. As a reminder, this was also the case for the SolarWinds compromise for which Moscow was blamed for. This position contrasts with the one of former President Donald Trump, who was less inclined to be concerned with adversary cyber operations.

Interestingly, on July 21st, the French national cybersecurity agency ANSSI shared IoCs[24] and a statement claiming members of APT31 (aka Judgment Panda) were actively targeting French enterprises hijacking home

---

[16] https://www.huntress.com/resources/ebook/exchange-server-exploitation
[17] https://www.domaintools.com/resources/blog/examining-exchange-exploitation-and-its-lessons-for-defenders
[18] https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/
[19] https://blog.orange.tw/2021/08/proxyshell-a-new-attack-surface-on-ms-exchange-part-3.html
[20] https://therecord.media/new-lockfile-ransomware-gang-weaponizes-proxyshell-and-petitpotam-attacks/
[21] https://www.rapid7.com/blog/post/2021/08/03/petitpotam-novel-attack-chain-can-fully-compromise-windows-domains-running-ad-cs/
[22] https://www.bleepingcomputer.com/news/security/fbi-nuked-web-shells-from-hacked-exchange-servers-without-telling-owners/
[23] https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion#:~:text=A%20federal%20grand%20jury%20in,abroad%20between%202011%20and%202018
[24] https://www.cert.ssi.gouv.fr/ioc/CERTFR-2021-IOC-003/

 © 2022 Capgemini. All rights reserved.

routers to form a proxy mesh around its server infrastructure to relay and disguise the origins of their attacks. The White House statement precisely blamed this group and the APT40 one for belonging to the Chinese MSS even though we still don't know as of writing if these statements are linked.

As far as APT31, the group had access to infamous NSA alleged Equation Group exploit three years before the Shadow Brokers bought this case to light. Thus, APT31 performs cyberespionage operations leveraging 0-days. One can conjecture that Judgment Panda could have accessed and exploited the Exchange flaws.

The use by eCrime groups of those vulnerabilities is not left out. The infection of unpatched Microsoft Exchange servers via ProxyLogon vulnerabilities by the DearCry[25] (aka DoeJoeCrypt) ransomware is the logical continuation of the revelation of various CVEs offering a considerable attack exposure to threat actors worldwide. According to Philip Misner[26], security manager at Microsoft, the exploitation of the now patched CVE-2021-26855 would have allowed the DearCry infection.

Among DearCry's specificities, we can note that it launches an "msupdate" service that it ends once the encryption is completed. The security researcher Florian Roth posted on Twitter[27] an interesting comment saying that the service 'msupdate' has already been used by the Chinese APT group Deep Panda (aka APT19) in 2012. Moreover, in a Crowdstrike report published in 2013 about Deep Panda, "msupdate" has been used to masquerade as a legitimate Microsoft Windows service. DearCry doesn't seem to leverage worming capabilities (as WannaCry does), encrypts '.aspx' files and the data by adding the ".CRYPT" extension.

Knowing that the huge size of the attack surface allowed by vulnerable Exchange servers, it's not surprising to see a heterogeneity in the targeting.

[25] https://www.bleepingcomputer.com/news/security/dearcry-ransomware-attacks-microsoft-exchange-with-proxylogon-exploits/
[26] https://twitter.com/phillip_misner/status/1370197696280027136
[27] https://twitter.com/cyb3rops/status/1370747925215731715

 © 2022 Capgemini. All rights reserved.

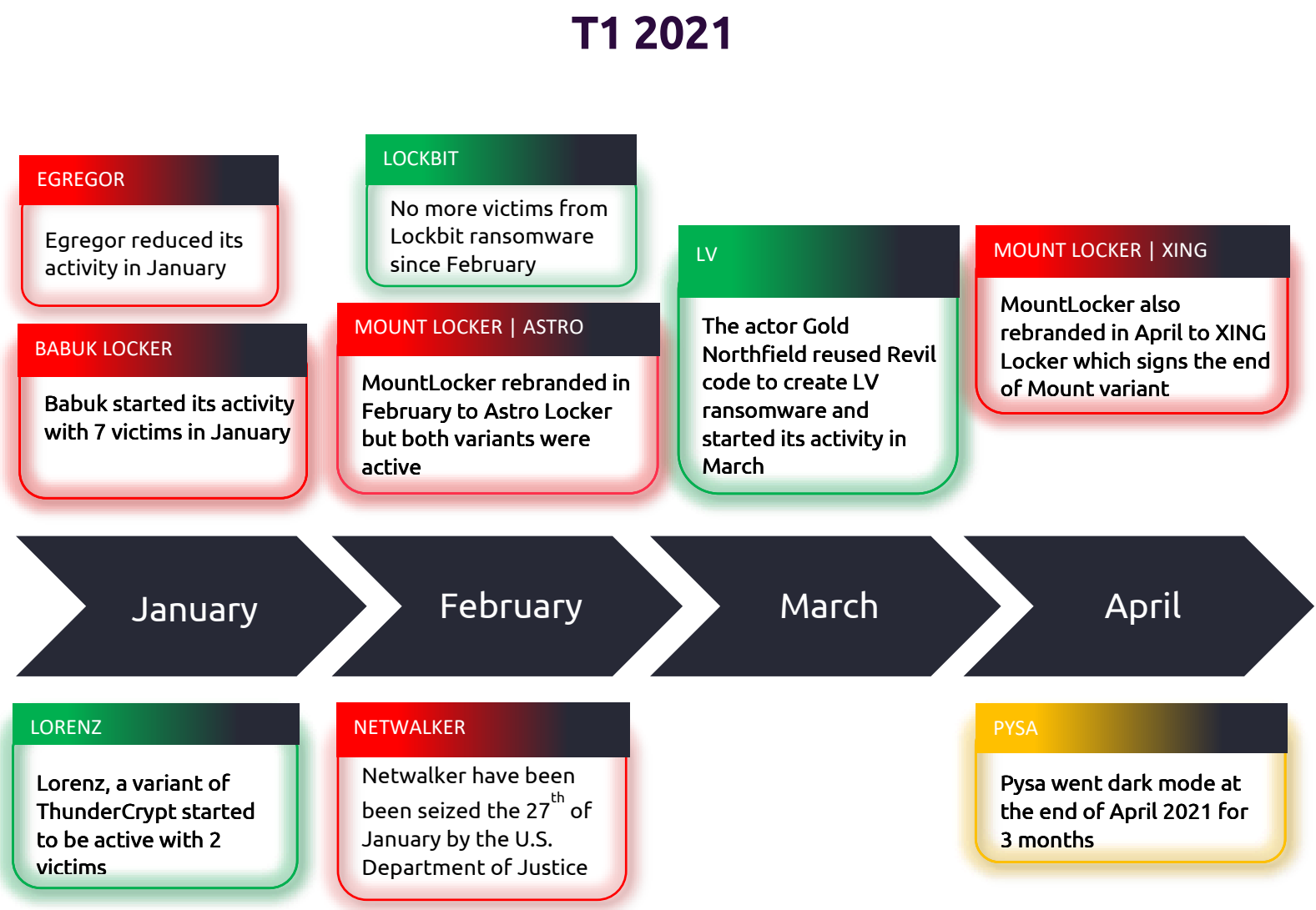
4 Doxwares events through 2021

4.1 Underground events of doxwares payloads

You may find below a timeline of noticeable events in the doxwares ecosystem through 2021 written by the CERT-E CIS. The legend is the same than in the section 1 of this paper.

Legend:

- Shutdown or seized
- Online and inactive
- Online and active



Credits: CERT-E Capgemini CIS

 © 2022 Capgemini. All rights reserved.

T2 2021

CONTI

Conti had a peak of activity until dividing its rate by 2 since June 2021

AVADDON

Avaddon has shut down operation and released decryption keys in June

LOCKBIT

Lockbit rebranded in Lockbit 2.0 and started to declare victims at a huge pace

CUBA | CL0P | PYSA | PAYLOAD.BIN

Pysa, Cl0P, Cuba and Payload.bin activities went up in August

May → June → July → August

DOPPEL PAYMER – ASTRO LOCKER

DoppelPaymer and AstroLocker signed their last victims in May before going down

DARKSIDE

DarkSide has gone dark after more than $2 million was seized by the U.S Department of Justice in June

REVIL

Revil had a peak of activity till they claimed responsibility for a hack at the IT firm Kaseya in July

RAGNAROK

Ragnarok released decryption keys in August before a shut-down of its activities

Credits: CERT-E Capgemini CIS

Public. © 2022 Capgemini. All rights reserved.

T3 2021

COOMING PROJECT

CoomingProject counted already more than 20 victims but after only two months, #Coomingproject stopped its activities

LOCKBIT

LockBit made a huge progress in September almost doubling its activity Conti, Pysa & Blackmatter (ex Darkside) continued at a huge pace

LOCKBIT | CONTI | PYSA

LockBit and Conti were leading the board in November with around 90 victims each. Pysa stayed behind with 59 victims.

September | October | November | December

REVIL

Revil went dark after its revival in September and being the target of enforcement forces

LOCKBIT | CONTI | PYSA

Lockbit was the more active ransomware with almost 100 victims in October where Conti and Pysa were behind with about 40~50 victims

PROMETHEUS | SPOOK

Prometheus rebranded as Spook at the end of September and start in October with about 50 victims

BLACKMATTER | REVIL | PAYLOAD.BIN

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

Credits: CERT-E Capgemini CIS

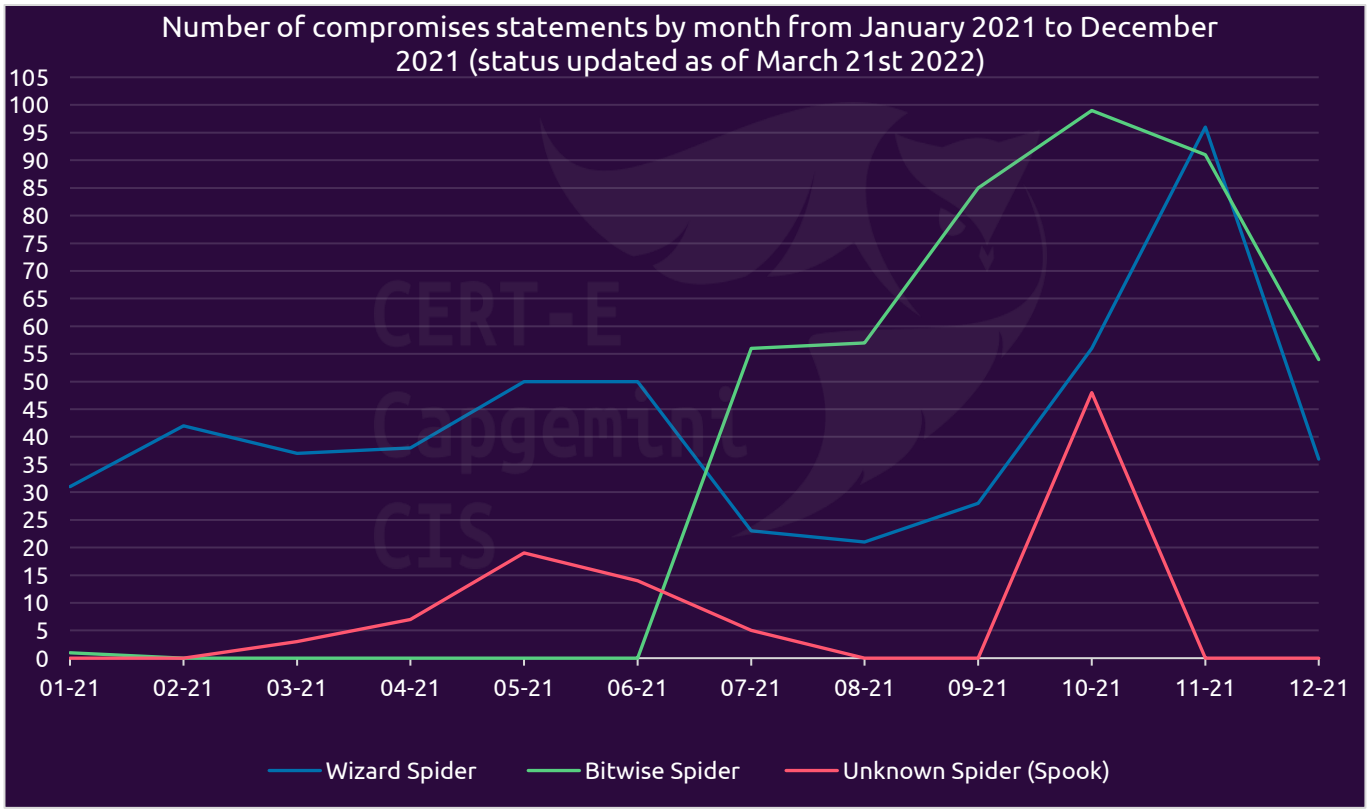
Public. © 2022 Capgemini. All rights reserved.

4.2 Evolution of activity of doxwares operators

To better match the increasing doxware ecosystem clustering scheme we observed in 2021, data below show the activity of threat groups (that can operate multiple doxwares). We only selected most impactful ones.

Legend:

- Shutdown or seized
- Online and inactive
- Online and active



WIZARD SPIDER

Wizard Spider had been very constant all year long with #Conti leading the global board and competing with #Bitwise until the end.

BITWISE SPIDER

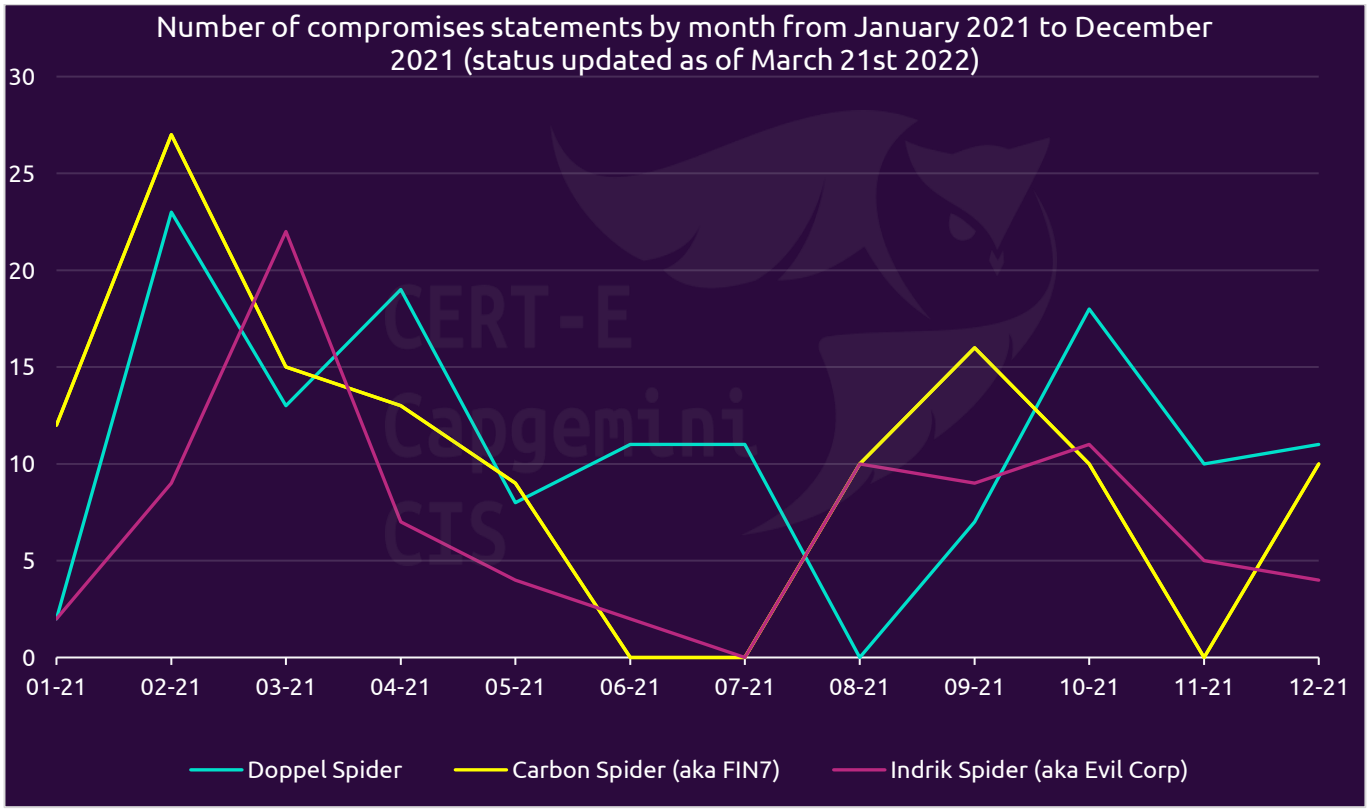
Bitwise Spider entered the main event only in May to become the most prolific actor of the second semester with #LockBit rebranded #Lockbit 2.0

UNKNOWN SPIDER (1)

This unnamed actor operated mostly Prometheus between March to August to switch to #Spook in October with 48 victims in one month

Credits: CERT-E Capgemini CIS

 © 2022 Capgemini. All rights reserved.



DOPPEL SPIDER

Doppel Spider started 2021 by operating DoppelPaymer before switching to Grief overlapping their activity in May when we found victims from both ransomwares.

INDRIK SPIDER (aka Evil Corp)

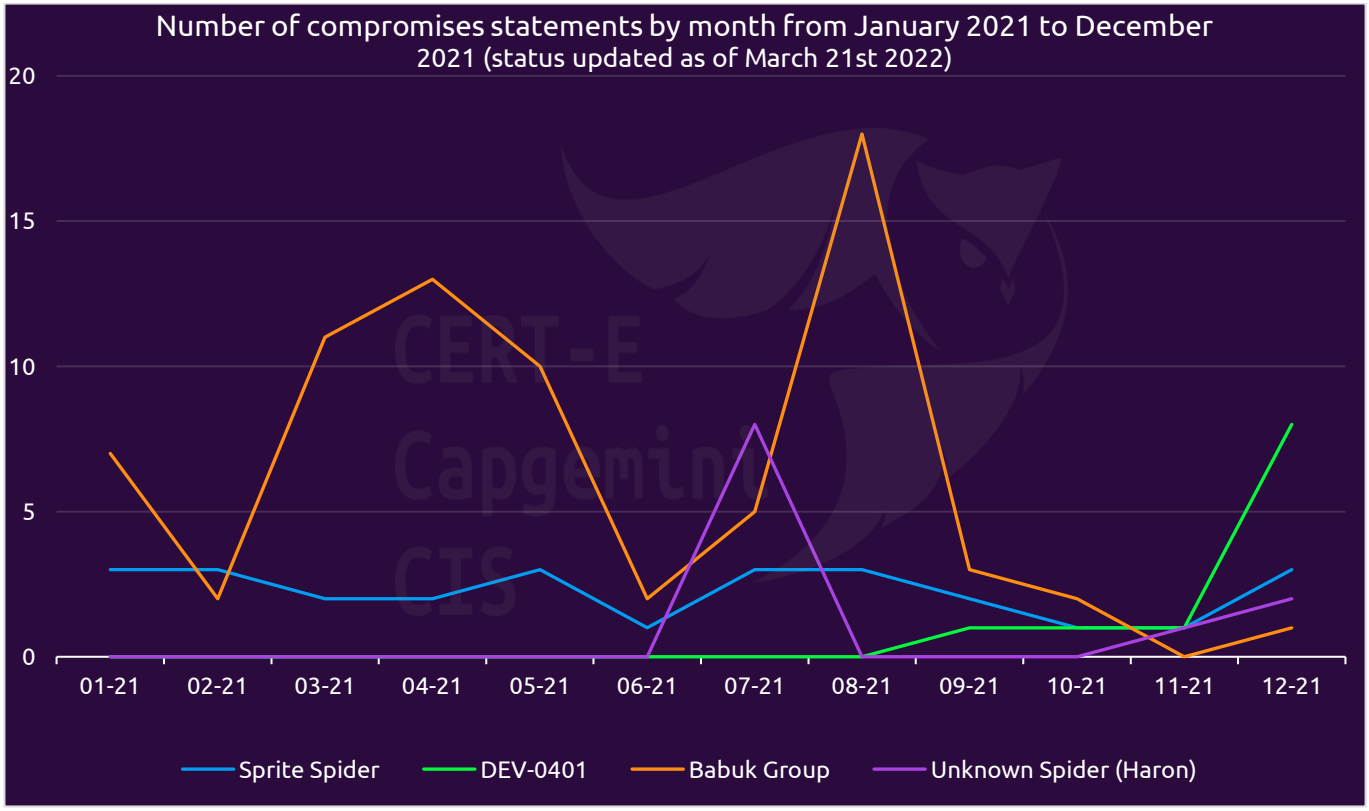
Cl0p ransomware had a constant flow of victims. This group being a public target of US authorities, they rebranded a lot of time during the year (WastedLocker, PhoenixLocker, MacawLocker…) as victims wishing to pay the ransom could be prosecuted by US government.

CARBON SPIDER

Carbon Spider had been a very mediatic actor with Darkside at the beginning until Colonial Pipeline attack aftermaths in May. They were tracked by authorities before being back with BlackMatter in August. Targeted a second time in the same year we went off before resurrecting as BlackCat/ALPHV in December.

Credits: CERT-E Capgemini CIS

 © 2022 Capgemini. All rights reserved.



UKNOWN

This unnamed group operated Haron until it rebrands after August in Midas.

DEV-0401

DEV-0401 appeared this year with AtomSilo to end 2021 by operating both AtomSilo and Rook. 2022 seems to start with another as they are also involved with Nightsky ransomware operations.

SPRITE SPIDER

After operating Defray777 they switched to RansomEXX in January claiming a small but constant number of victims all year long.

BABUK GROUP

Babuk Group started its activity in Q4 of 2020 by operating Babuk ransomware before switching to Payload.bin in May with their biggest activity in August.

Credits: CERT-E Capgemini CIS

Public. © 2022 Capgemini. All rights reserved.

5 Adversaries on the headlines

This section aims to provide information about activities of threat groups that drew CERT-E CIS attention during the year 2021. As the CERT-E CIS is integrated within the whole Toulouse SOC (France) organization, all insights about these adversaries have been pushed to different SOC stakeholders (Security Engineering team, SWAT team, Level 1,2 and 3 analysts) to take appropriate measures to counter these threats.

5.1 Russia-linked landscape

February 2021

- **Sandworm** (aka VoodooBear)
  - Targeting of Centreon' servers in several French entities and attributed to Sandworm according to the French national systems information security agency (ANSSI) thanks to the P.A.S webshell and the Exaramel backdoor.[28]

- **FIN11**
  - Targeting of Accellion FTA linked to FIN11 according to FireEye researchers and threatening to exfiltrate compromised data on Cl0p's data leak site via blackmail campaigns.[29]

March 2021

- **Indrik Spider**
  - Development of new ransomware payloads such as Hades, Phoenix Locker or Macaw Locker in a wider rebranding strategy to evade OFAC' sanctions that the adversary is facing.[30]

April 2021

- **APT29 (aka Cozy Bear)**
  - Official attribution by the US White House of the SolarWinds Orion supply-chain compromise to APT29 threat actors leading to an escalation of tensions between Moscow and Washington.[31]

- **Lunar Spider**
  - Signals point to a sale or rent of its IcedID loader malware to Ransomware as a Service operators such as Pinchy Spider, Sprite Spider and TA2101.

May 2021

- **Carbon Spider**
  - Apologies from Carbon Spider operators following the compromise of Colonial Pipeline that led to the declaration of state of emergency in the US and the dismantling of Darkside infrastructure.

July 2021

- **Pinchy Spider**
  - Claim by Revil's operators of the compromise of the software editor Kaseya thanks to a sophisticated supply-chain attack. Weak signals point to a classification of the group into the privateers eCrime ecosystem.

[28] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf
[29] https://threatpost.com/accellion-zero-day-attacks-clop-ransomware-fin11/164150/
[30] https://www.crowdstrike.com/blog/hades-ransomware-successor-to-indrik-spiders-wastedlocker/
[31] https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

 © 2022 Capgemini. All rights reserved.

August 2021

- **Bitwise Spider**
  - Use by the group of triple extorsion tactics (encryption, exfiltration and DDoS) against the IT giant Accenture which is consistent with the increase of the group's offensive capabilities.

September 2021

- **APT29 (aka Cozy Bear)**
  - New backdoor dubbed FoggyWeb directed to Active Directory servers uncovered by Microsoft researchers and linked to APT29. It highlights the activism of the threat group which has tried to replicate several others supply-chain compromises, sometimes successfully, despite the indictment stated above.[32]

- **Carbon Spider**
  - Targeting of the US farmer New Cooperative by Blackmatter ransomware which is a rebrand of Darkside. The group employed advanced reconnaissance steps that highlight its sophistication and its professionalism.[33]

- **Wizard Spider**
  - Conti and Ryuk ransomwares operators seem to be linked to the exploitation of the CVE-2021-40444 targeting MSHTML according to RiskIQ researchers. Cobalt Strike beacons deployed by the exploit overlap some Wizard Spider C2 infrastructure. But it also could be the work of an affiliate, an APT group or a false-flag trick.[34]

November 2021

- **Graceful Spider**
  - Global operation led by Interpol to arrest several members of the Cl0p ransomware worldwide. The codenamed "Cyclone" operation follows the first strike of six alleged members of the group in June 2021 led by Ukraine.[35]

- **Primitive Bear (aka Gamaredon)**
  - Comprehensive and detailed report written by the Ukrainian intelligence service (SBU) about Gamaredon organization, resources, tactics, techniques and procedures. The report highlights that the adversary performed more than 5000 attacks against Ukraine entities since 2014.[36]

- **Lockean**
  - Grouping by the French ANSSI of a unique cluster of activity dubbed "Lockean" which is an eCrime threat group that heavily rents loaders to ransomware operators. Lockean leverages among others, Qbot, the red team tool Cobalt Strike and the data exfiltration one rClone. In 2021, its victimology showed a particular targeting of French big enterprises such as Gefco, Fareva, Pierre Fabre and Ouest France.[37]

[32] https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor/
[33] https://twitter.com/ido_cohen2/status/1439863554606305286
[34] https://www.riskiq.com/blog/external-threat-management/wizard-spider-windows-0day-exploit/
[35] https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrime-ring
[36] https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armagedon.pdf
[37] https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-009/

 © 2022 Capgemini. All rights reserved.

December 2021

- **Carbon Spider**
  - Identification of a new ransomware payload written in Rust (which is quite unusual for a ransomware) particularly sophisticated. Some indications pointed towards Carbon Spider who could have been rebranded Blackmatter to evade law enforcement eyes. In early 2022, some BlackCat operators confirmed they were former Carbon Spider operators.[38]

[38] https://therecord.media/an-alphv-blackcat-representative-discusses-the-groups-plans-for-a-ransomware-meta-universe/

Public. © 2022 Capgemini. All rights reserved.

5.2 China-linked landscape

March 2021

- **Hafnium**
  - Exploitation of the so-called ProxyLogon vulnerabilities against Microsoft Exchange servers to perform cyberespionage operations according to Microsoft.[39] Other researchers don't cluster the ProxyLogon exploitation towards a unique name, as Microsoft does, but attribute these exploitations to multiple historical China-backed APT groups.[40]

April 2021

- **Karma Panda and Tonto Team**
  - Cybereason researchers uncovered a cyberespionage campaign against the Rubin Design Bureau, a Russian defense contractor in charge of the design of Russian nuclear submarines. A previously undocumented backdoor dubbed PortDoor was used and the APT group TA428 could have worked, with medium likelihood in conjunction with Tonto Team and Karma Panda.[41]

June 2021

- **Nomad Panda (aka RedFoxtrot)**
  - In-depth analysis by Recorded Future of the affiliation of Nomad Panda with the Unit 69010 from Strategic Support Forces (SSF), part of the People's Liberation Army (PLA) based in the autonomous region of Xinjiang. Among tools used by Nomad Panda, we found the common – and usual – Chinese toolset such as Icefog, Poison Ivy, Quickheal and PlugX.[42]

July 2021

- **APT31 (aka Judgment Panda)**
  - Official attribution by the US, Five Eyes countries, NATO and EU members of the Microsoft Exchange servers zero-day vulnerabilities exploitation of March 2021 to Judgment Panda and Kryptonite Panda (APT40). The Allies also linked these two groups to the Ministry of State Security (MSS) which is the main intelligence service of the People's Republic of China.[43][44]

[39] https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
[40] https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
[41] https://www.cybereason.com/blog/portdoor-new-chinese-apt-backdoor-attack-targets-russian-defense-sector
[42] https://go.recordedfuture.com/redfoxtrot-insikt-report
[43] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/
[44] https://www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking

Public. © 2022 Capgemini. All rights reserved.

5.3 Iran-linked landscape

January 2021

- **Lebanese Cedar**
  - Iran-backed terrorist[45] organization Hezbollah is believed to have links with Lebanese Cedar via its Cyber Unit according to Clearsky researchers. Lebanese Cedar updated its toolset, particularly its Caterpillar webshell and its Explosive RAT to target telecommunication and IT enterprises located both in western countries (mostly the US) but also in regional rivals of Tehran such as Egypt or Saudi Arabia.[46]

August 2021

- **Siamese Kitten (aka Hexane)**
  - New tactics, techniques and procedures of this adversary described by Clearsky teams. Among them, we can note an upgrade of their backdoor dubbed Shark and a pretty efficient social engineering operations through LinkedIn to target large companies in Israël, France, UK or in regional rivals of Iran in the Middle-East. Some overlaps with Refined Kitten (APT33) noted.[47]

[45] Capgemini doesn't endorse any political position in its research papers. We underline that even if in many occidental countries the Hezbollah is classified as a terrorist organization, other ones only consider its military arm like that while other countries (mainly arabic-speaking) don't take such statement.
[46] https://www.clearskysec.com/cedar/
[47] https://www.clearskysec.com/wp-content/uploads/2021/08/Siamesekitten.pdf

 © 2022 Capgemini. All rights reserved.

5.4 DPRK-linked landscape

January 2021

- **Stardust Chollima (aka APT38)**
  - North-Korean APT group Stardust Chollima employed advanced social engineering tactics to target infosecurity researchers. They relied on social media approaches (LinkedIn, Twitter, Telegram, Discord…), zero-day exploits or invites to participate in a trojanized research project to harvest intelligence of interest from them.[48]

[48] https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/

Public. © 2022 Capgemini. All rights reserved.

6 Perspectives

We have seen that 2021 has been the year of evolution in adversarial modus operandi: cybercriminal groups are becoming more ingenious, more agile, more resilient, and richer than ever. Occasionally, some can serve the political interests of governments, no longer hesitate to attack targets with very high added value and even manage to exploit zero-day vulnerabilities to maximize their profits.

On the other side, APT groups continue their operations, though at a low level and with their arsenals continuously renewed and even reinforced. They are still masters at exploiting vulnerabilities quickly and are increasingly reactive to geopolitical events around the world.

In view of these elements and the knowledge accumulated by the CERT-E CIS CTI unit, we issue the following outlook for the year 2022:

- **"One-shot" ransomwares & oligopolisation of the cybercriminal threat landscape**

  As the international response to ransomware groups increases, they must find ways to continue their compromises. While one circumvention strategy currently visible appears to be an intensive rebranding strategy to prevent traceability of ransomware strains, it is not viable as it is resource intensive to change the code so that it is not too similar the previous strain.
  Another tactic could be the creation of single-use ransomware strains: they would be developed to target a small number of high-value companies along with a data-leak site. Once the ransom has been obtained, the ransomware would cease operations to avoid being taken down. However, this tactic requires the mobilization of many affiliates as the volume of compromises would be much lower than the current average rate.

- **Slight drop of the cartelization phenomenon**

  Given that ransomware groups tended to join forces from time to time to pool their resources and by doing so to be more efficient, this phenomenon was relatively true at the beginning of the Big Game Hunting (i.e. around the year 2020). Since the beginning of 2021, as mentioned above, the number of compromises has exploded and with it the number of players motivated by the lure of gain. Like any market, the more players compete, the smaller the market share for each. Add to this competition the consequent weight of egos and the communication battle for the best image in terms of sophistication and seriousness, and collaboration within eCrime groups is less and less observed. Players continue to collaborate, but the prerequisite is a clear division of labor (notably between access brokers and ransomware) and an affiliate model already established and recognized by its peers. In this game, we will see not so much a continuation of cartelization as the formation of an oligopolistic structure where a small number of players will share the biggest gains. The most committed groups (Wizard Spider, Bitwise Spider and Carbon Spider) will have a vested interest in continuing their operations towards targets of interest and media attention to maintain their brand image. Especially as these groups are seen as privateers and therefore accused of politically motivated maintenance.

- **Strong growth of specialized data leakage groups**

  As a result of the success of doxxing, a large number of players are trying to take advantage of the benefits of this tactic, pushing operators to constantly upgrade their payloads in order to make a profit and stand out from their competitors. This race for efficiency is costly for newcomers (unless they join a RaaS operator for which they have to pay a fee). Thus, we are seeing more and more groups (CoomingProject for example) or stolen data marketplace platforms (Marketo) gaining in popularity without using ransomware. This less costly and more technically accessible modus operandi would allow those who adopt it to benefit from the reputation damage of data-leak sites against their targets while being able to monetize this data with ransomware groups keen on network access and sensitive information.

Public. © 2022 Capgemini. All rights reserved.

- **Deterioration of Russia/United States relations which will hinder the nascent cooperation between the two states to dismantle privateers[49]**

  Several Western (especially US) government officials have pointed the finger at Russia's inaction in the wake of the Colonial Pipeline compromise of May 2021. Moscow was accused of doing nothing (or even accommodating it) to dismantle the group behind the compromise, which according to US intelligence was present on Russian soil. In January 2022, the Russian domestic intelligence service FSB announced that it had dismantled the Pinchy Spider group (operator of the Revil ransomware) in collaboration with the US. This sign, which could be interpreted as a constrained but emerging collaboration, should not make us lose sight of the fact that this dismantling could have been orchestrated solely to show Russia's goodwill but also to "exfiltrate" Pinchy Spider members in order to protect them. At present, in light of Russia's aggression against Ukraine, the United States and its Western allies have imposed unprecedented economic sanctions against Moscow. With diplomatic relations between the two powers on the brink of collapse, future collaboration to dismantle the privateers is unlikely.

[49] This point has been written before the invasion of Ukraine by Russian forces on February 24th, it has been modified to take count of new power relations

 © 2022 Capgemini. All rights reserved.

Public. © 2022 Capgemini. All rights reserved.

TLP : WHITE

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 340,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2021 global revenues of €18 billion.

Get the Future You Want | www.capgemini.com

This document contains information that may be privileged or confidential and is the property of the Capgemini Group.

Public. Copyright © 2022 Capgemini. All rights reserved.