IDENTIFICATION OF A NEW CYBER CRIMINAL GROUP: LOCKEAN

Version 1.0

October 26, 2021

Table of contents

1 Context: links between several incidents within the French remit

Over the 2020-2021 period, the following compromises of French companies' information system (IS) by the **QakBot** malware have been reported to the ANSSI:

- Compromise of a French company in the manufacturing sector in June 2020, which will subsequently be called "Company A";
- Compromise of the transport company Gefco in September 2020 [1];
- Compromise of the Ouest-France newspaper in November 2020 [2];
- Compromise of the pharmaceutical group Fareva in mid-December 2020 [3];
- Compromise of a French services company in February 2021, which will subsequently be called "Company B";
- Compromise of the pharmaceutical company Pierre Fabre at the end of March 2021 [4].

In addition to the constant presence of **QakBot** as the first payload, some incidents had other similarities:

- in four incidents (Company A, Gefco, Fareva, Pierre Fabre) [1], the **QakBot** payload naming convention was the same;
- in five incidents (Gefco, Fareva, Pierre Fabre, Ouest-France, Company B), the use of **Cobalt Strike** was observed;
- in four incidents among these (Gefco, Fareva, Pierre Fabre, Company B) [2], the domain names of the command and control servers (C2) associated with **Cobalt Strike** had the same naming convention: they spoofed Akamai domains [3] and Azure domains [4]. This infrastructure is referred to as the Akamai/Azure Cluster in the remainder of the document;
- in three incidents (Gefco, Ouest-France, Pierre Fabre) [5], the exfiltration tool **Rclone** [6] was used with the same naming convention for the executable and its configuration file, based on the spoofing of the "svchost" Windows service.

In addition, two open source reports describe infection chains with the same characteristics: one from the IT security firm Intrinsec concerning the **ProLock** and **Egregor** [5] ransomware and the other from The DFIR Report regarding the **Sodinokibi** [6] ransomware.

[1] The naming convention used during the Ouest-France and Company B incidents is not known to the ANSSI or to the victims.
[2] The **Cobalt Strike** implant infrastructure discovered at Ouest-France is neither known to the ANSSI nor to the victims.
[3] Akamai Technologies is an American company specialising in the provision of cache servers for businesses.
[4] Microsoft Azure is Microsoft's cloud services platform.
[5] The exfiltration tool that may have been used during incidents A, B and Fareva is not known to the ANSSI or the victims.
[6] **Rclone** is an open-source command line tool used to manage or migrate content on cloud services.

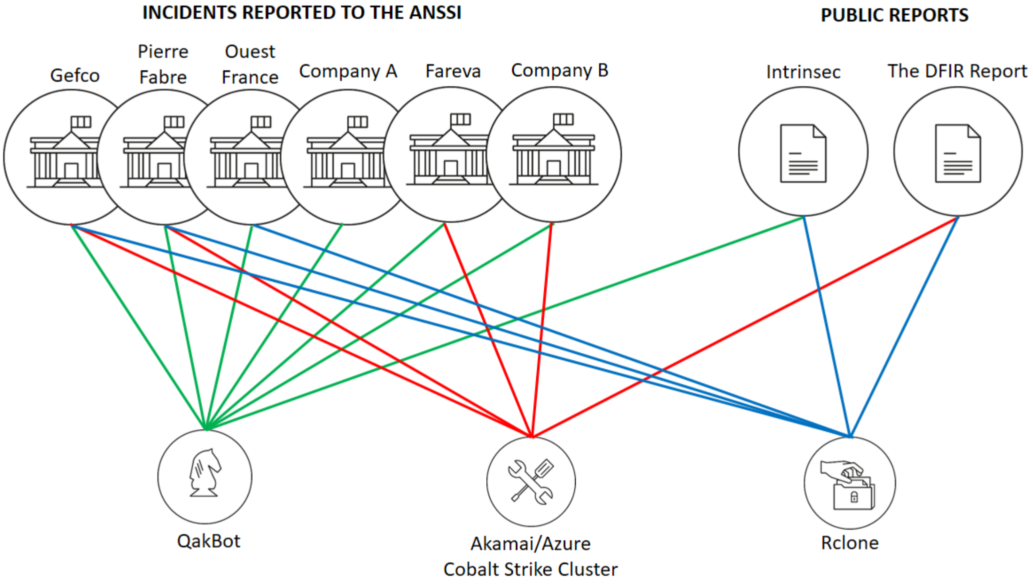


Fig. 1.1 – Links between several incidents and IT security firm reports

In view of these commonalities, the same group of attackers could be behind the six incidents reported to the ANSSI and be the subject of the reports by Intrinsec and The DFIR Report.

In addition, given that:

- the incidents at Gefco and Ouest-France resulted in the spread of the **Egregor ransomware**[7],
- the incident at Pierre Fabre and the incident described by The DFIR Report resulted in the spread of the **Sodinokibi ransomware**[8],
- the incidents at Company A and Fareva resulted in the spread of the **DoppelPaymer ransomware**[9],
- the incident described by Intrinsec resulted in the spread of the **ProLock ransomware**[10],
- all of these ransomware programs operate according to the *Ransomware-as-a-Service* (RaaS) business model,

this group is thought to have been affiliated since it was first observed in June 2020 with several RaaS, including Egregor, Sodinokibi, DoppelPaymer and ProLock.

[7] Egregor is RaaS that appeared at the start of the second half of 2020 and is supposedly operated by the cyber criminal group behind its predecessor: Maze. Egregor was taken down in February 2021 by a police operation.

[8] Emerging in 2019, Sodinokibi (aka REvil) is RaaS operated by the cyber criminal group Pinchy Spider. A victim data disclosure site is associated with this ransomware.

[9] DoppelPaymer is ransomware from the BitPaymer family and is operated by the cyber criminal group Doppel Spider. It is thought to have become RaaS from 2020. A victim data disclosure site has been associated with this ransomware since February 2020.

[10] ProLock is ransomware that appeared in early 2020 and disappeared in the third quarter of the same year.

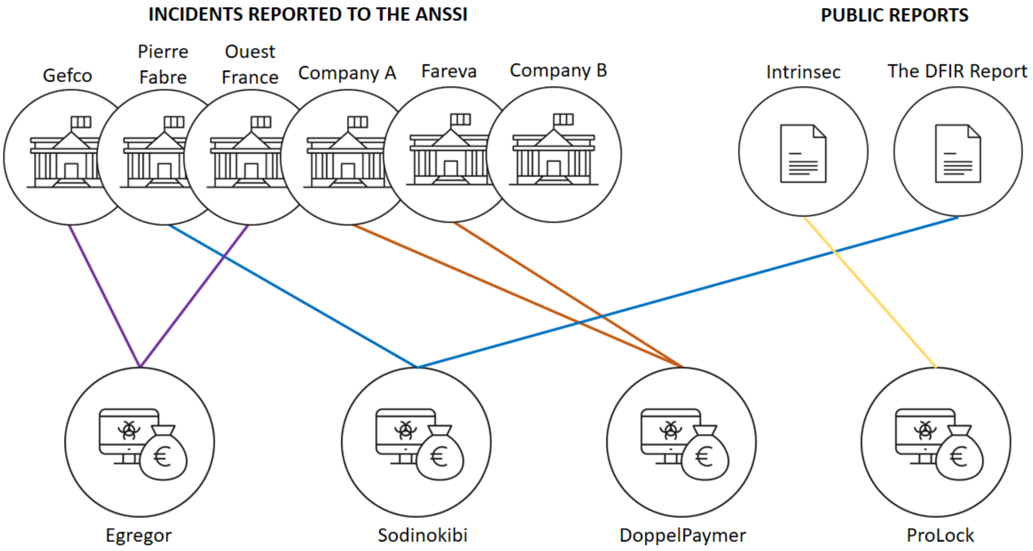


Fig. 1.2 – RaaS used during these various incidents

2 Investigations into and discovery of the Lockean cyber criminal group

Based on these incidents and their commonalities, investigations were carried out by the ANSSI to confirm the existence of this cyber criminal group, understand its modus operandi and distinguish its main Techniques, Tactics and Procedures (TTPs).

Comment: The ANSSI is not aware of any previous work technically linking all of these malicious activities and associating them with the same group of attackers.

2.1 Investigation into the Cobalt Strike C2 infrastructure involved

The table below lists the infrastructure observed in several of the incidents in which **Cobalt Strike** has been used. Several domain names of the C2 servers spoof Akamai and Azure domains. In addition, the term « `technology` » (and its derivatives) is regularly found in the domains and the same domain name is sometimes reused by deriving its *Top Level Domain* (TLD).

Incident	Domain Name	IP Address	Value of Server header	Value of Keep-Alive header	First Seen	Last Seen
Gefco	amajai-technologies.network	23.254.229.82			2020-09-19	2020-11-19
Gefco	amajai-technologies.industries	192.236.209.151			2020-09-17	2020-11-11
Fareva	cloudflace-network.digital	38.132.124.137	nginx	Timeout=10 max=100	2020-12-13	2021-01-08
Fareva	stackpatc-technologies.digital	185.245.84.133	apache	Timeout=10 max=100	2020-09-19	2021-01-08
Fareva	rackspare-technology.digital	38.132.99.229	nginx	Timeout=10 max=100	2020-12-26	2021-01-06
Company B	asurecloud.tech	94.158.244.89	SAF	Timeout=11 max=120	2021-02-09	2021-03-08
Company B	asurecloud.tech	80.209.233.56	apache	Timeout=10 max=100	2021-03-01	2021-03-03
Company B	akamacloud.tech	80.209.233.56	apache	Timeout=10 max=100	2021-03-01	2021-03-03
Company B	akamacloud.tech	138.201.149.51			2021-02-12	2021-03-03
Pierre Fabre	asureupdate.tech	194.15.112.119	de Update	Timeout=11 max=120	2021-03-27	2021-05-24
Pierre Fabre	asureupdate.pro	194.15.112.118	BizTalk	Timeout=10 max=100	2021-03-27	2021-04-03
Pierre Fabre	akamaclouds.app	66.181.34.13			2021-03-26	2021-04-20
The DFIR Report	cloudmetric.online	45.86.163.78	Nginx i386	Timeout=11 max=60	2021-02-28	2021-03-28
The DFIR Report	smalleststores.com	195.189.99.74	cloudflare	Timeout=10 max=100	2021-03-07	2021-03-15

Common configuration characteristics, called C2 server search heuristics, and here based on the values of the HTTP headers « `Server` » and « `Keep-Alive` », enabled 33 new **Cobalt Strike** C2 servers to be identified:

Common Value	Domain Name	IP Address	First Seen	Last Seen
apache / timeout 10	akastat.app	62.128.111.176	2021-04-24	2021-05-17
BizTalk	azurestat.app	94.158.244.78	2021-04-24	2021-05-18
BizTalk	cdnengine.biz	91.134.187.27	2021-03-04	2021-04-19
BizTalk	akamaclouds.tech	66.181.34.16	2021-03-25	2021-05-19
BizTalk	akabox.space	139.99.178.86	2021-05-12	2021-05-18
cloudflare	setupfastonline.com	212.114.52.87	2021-03-27	2021-05-19
cloudflare	akamalupdate.site	51.255.96.55	2021-02-12	2021-03-04
cloudflare	securitypanels.org	37.120.239.145	2021-03-23	2021-04-14
cloudflare	c2.hax.vg	54.206.202.171	2021-04-24	2021-05-02
de Update	azuresecure.tech	80.209.228.62	2021-04-08	2021-05-04
de Update	securesurvey.cloud	46.17.63.244	2021-03-05	2021-04-27
de Update	akabox.tech	194.135.90.221	2021-05-17	2021-06-06
Nginx i386	electronicwhosaleonline.com	74.118.138.236	2021-04-12	2021-05-04

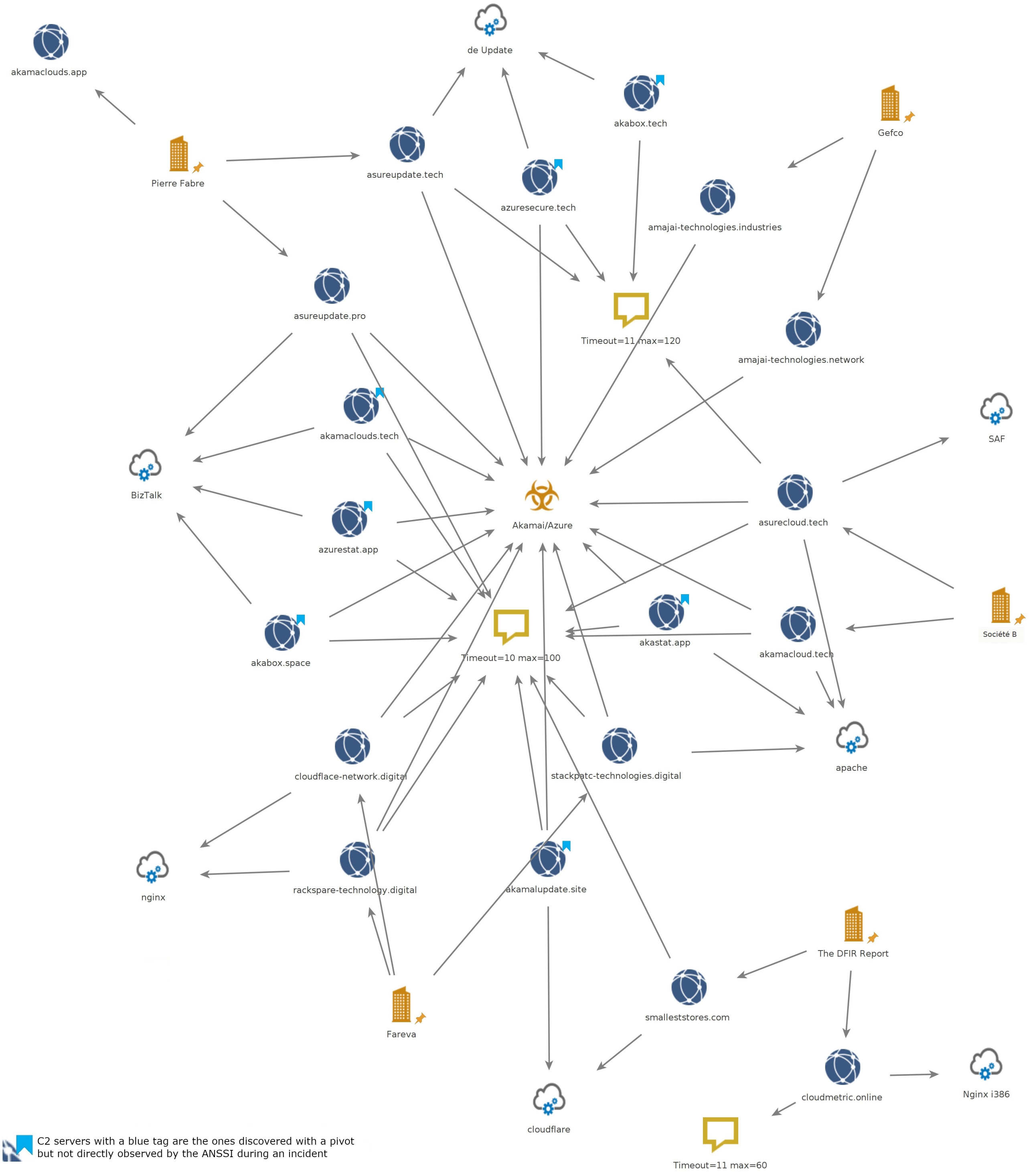
Nginx i386	madesecuritybusiness.com	204.16.247.35	2021-05-04	2021-07-28
Nginx i386	ropesecuritybusiness.com	74.118.138.174	2021-05-01	2021-07-27
Nginx i386	knotsecuritybusiness.com	23.108.57.245	2021-04-28	2021-06-24
Nginx i386	ticksecuritybusiness.com	23.108.57.31	2021-05-03	2021-06-23
Nginx i386	entirelysecuritybusiness.com	204.16.247.224	2021-05-17	2021-07-26
Nginx i386	hesitatesecuritybusiness.com	23.108.57.148	2021-05-03	2021-06-25
Nginx i386	stexwhosaleonline.com	23.82.185.111	2021-04-09	2021-05-22
Nginx i386	dealsforyoutoday.org	198.244.135.225	2021-04-08	2021-04-26
Nginx i386	onlineceoshelp.com	108.177.235.180	2021-04-18	2021-06-18
Nginx i386	risetomoon.com	213.227.154.244	2021-04-29	2021-06-23
Nginx i386	notescloud.org	185.228.83.170	2021-04-05	2021-04-10
Nginx i386	amasonstore.com	46.30.188.31	2021-03-18	2021-04-04
Nginx i386	classworldint.com	45.138.172.91	2021-05-03	2021-06-24
Nginx i386	orientalclient.com	74.118.138.235	2021-04-10	2021-05-04
Nginx i386	perfectappt.com	104.194.222.88	2021-03-20	2021-04-01
Nginx i386	displaychecks.com	108.177.235.52	2021-04-29	2021-06-22
Nginx i386	itstrueloves.com	23.82.185.110	2021-05-12	2021-05-14
Nginx i386	adjustclouds.com	108.177.235.44	2021-04-22	2021-06-18
Nginx i386	killsecuritybusiness.com	23.108.57.209	2021-04-29	2021-05-17
Nginx i386	securitybusinessmean.com	213.227.155.210	2021-05-02	2021-05-09
Nginx i386	justicedev.com	46.17.63.191	2021-04-14	2021-06-06

Several of these C2 servers use the naming convention spoofing Akamai and Azure observed in the incidents studied:

- « `akastat.space` »
- « `azurestat.app` »
- « `akamaclouds.tech` »
- « `akabox.space` »
- « `akabox.tech` »
- « `akamalupdate.site` »
- « `azuresecure.tech` »

Note that the domain name « `akamalupdate.site` », which shares common headers with the C2 server « `smalleststores.com` » observed by The DFIR Report, corresponds to the Akamai/Azure naming convention. This constitutes a technical infrastructure link between the incident described by The DFIR Report and those observed by the ANSSI.

The domain names that do not use the Akamai/Azure naming convention are not strongly linked to this cluster, as the header similarities alone do not seem to be a sufficient element to technically group them together.



C2 servers with a blue tag are the ones discovered with a pivot but not directly observed by the ANSSI during an incident

Fig. 2.1 – Summary of the **Cobalt Strike** infrastructure.

Additional pivots on the domain name format have enabled 49 other **Cobalt Strike** C2 servers of the Akamai/Azure cluster to be identified.

Domain Name	Registration Date	IP Address
amamai-tecnologies.cloud	2020-07-14	172.241.29.157
amamai-tecnologies.digital	2020-07-14	172.241.29.156
amamai-tecnologies.space	2020-07-14	172.241.29.155
amatai-technologies.digital	2020-07-28	172.241.27.72
amatai-technologies.site	2020-07-28	172.241.27.44
amatai-technologies.space	2020-07-28	172.241.27.66
amatai-technologies.website	2020-07-28	172.241.27.225
atakai-technologies.host	2020-08-03	172.241.27.17
atakai-technologies.online	2020-08-03	192.236.193.203
atakai-technologies.space	2020-08-03	192.236.194.99
atakai-technologies.website	2020-08-03	192.236.232.228
atakai-technologies.work	2020-08-03	192.236.193.184
akamai-technologies.digital	2020-08-06	Parking Namecheap
akamai-technologies.host	2020-08-06	Parking Namecheap
akamai-technologies.online	2020-08-06	Parking Namecheap
akamai-technologies.site	2020-08-06	23.254.230.196
akamai-technologies.space	2020-08-06	23.254.224.62
akamai-technologies.website	2020-08-06	23.254.202.217
amajai-technologies.digital	2020-09-12	192.236.209.144
amajai-technologies.host	2020-09-12	192.236.209.150
amajai-technologies.space	2020-09-12	23.254.229.91
amajai-technologies.tech	2020-09-12	23.254.229.103
amajai-technologies.website	2020-09-12	Parking Namecheap
amajai-technologies.online	2020-11-05	45.147.230.0
amajai-technologies.site	2020-11-05	45.147.231.51
amajai-technologies.support	2020-11-05	45.153.243.215
amajai-technologies.trade	2020-11-05	108.62.118.37
amajai-technologies.work	2020-11-05	23.106.160.137
amajai-technologies.world	2020-11-05	23.106.160.138
amazai-technologies.online	2020-11-18	192.236.248.176
amazai-technologies.site	2020-11-18	192.236.248.169
amazai-technologies.space	2020-11-18	Parking Namecheap
amazai-technologies.support	2020-11-18	Parking Namecheap
amazai-technologies.website	2020-11-18	Parking Namecheap
amazai-technologies.world	2020-11-18	Parking Namecheap
amapai-technologies.digital	2020-11-19	192.236.248.176
amapai-technologies.email	2020-11-19	192.236.248.169
amapai-technologies.site	2020-11-19	23.83.133.240
amapai-technologies.space	2020-11-19	23.81.246.89
amapai-technologies.support	2020-11-19	192.236.248.215
amapai-technologies.website	2020-11-19	142.11.227.114
amapai-technologies.work	2020-11-19	Parking Namecheap
amapai-technologies.world	2020-11-19	Parking Namecheap
rackspare-technology.download	2020-12-09	38.132.99.215
rackspare-technology.network	2020-12-09	95.174.65.241
rackspare-technology.online	2020-12-09	185.245.84.132
rackspare-technology.space	2020-12-09	45.11.19.217
akamacloud.pro	2021-02-08	80.209.233.56
asurecloud.pro	2021-02-08	94.158.244.88

All of the domain names observed in the incidents, as well as those resulting from the pivots, were purchased from the Namecheap registrar. They also all use exotic, often inexpensive TLDs.

Two types of TLS certificates have been observed on the C2 servers: the **Cobalt Strike** certificate, which by default is SHA-1 « `6ece5ece4192683d2d84e25b0ba7e04f9cb7eb7c` », and certificates issued by Let's Encrypt.

The C2 servers are mostly hosted by HostWinds and LeaseWeb in the United States.

2.2 Investigation into the QakBot implants used

The **QakBot** [11] implants involved in the incidents reported to the ANSSI, as well as in those described in the report by the IT security firm Intrinsec [5], use the following naming convention: « `md.*` ».

Following the observation of this convention, pivots on code analysis platforms made it possible to identify **QakBot** implants named « `md.exe` » and « `md.dll` », as well as others sharing the same botnet configuration parameter. The configurations of the implants were then extracted:

Hash	Type	Nom	botnet	campagne	Version
4568b57ad46502fe4740a6ec3282a874	QakBot	md.exe	domain01	1591171636	324.142
3a3842e2be15bb3c8f5c36283c8e31a2	QakBot	ljawof.exe	domain01	1596444853	
1f5458f4ccbad2399f84b6d20e485d40	QakBot	md.exe	domain01	1597161528	
5aa990d7864b3bd6c80718c7e86e00ba	QakBot	md.exe	domain01	1597161528	325.43
5ed9fb5fc74c6fdb3537629e9b23437a	QakBot	md.exe	domain01	1597161528	325.43
83b15f14e171cce96ab3fdea915c388a	QakBot	md.exe	domain01	1597161528	325.43
8edc802c274f3fd64be9aa5557b7ca79	QakBot	mdo.exe	domain01	1597161528	325.43
d92312b6a956d0d1da70c007068965f8	QakBot	md.exe	domain01	1597161528	325.43
e166035566a91e406ce66656be68012c	QakBot	md.exe	domain01	1597161528	325.43
005cdb34748048c41a3c57ba7358986d	QakBot	md.exe	domain01	1602007616	325.43
5d60ef2d7cb084878cdcccd63b4df50b	QakBot	md.exe	domain01	1602007616	325.43
ae95189f757df558e743ff2e0701f3dc	QakBot	md.exe	domain01	1602007616	325.43
04416cf8bf1c7d31a606edff765529df	QakBot	md.dll	domain02	1606721866	
1bb03c456a3e113d7085ea70d37e7a72	QakBot	ma.dll	domain02	1611939347	
16f84c82e6f0d47389f70d59d395778d	QakBot	md.dll	domain02	1613028094	401.138
a9d59daeb3b08134eb4f40be73085ea7	QakBot	md.dll	domain02	1613028094	
ee0a11ed10588b6c7c35b6a36f0998da	QakBot	md.dll	domain02	1613028094	401.138
f8bedd553a00abdc81ae847d21e958a1	QakBot	md.dll	domain02	1613028094	401.138
0a72e62e334437456386d3d6a84d44fc	QakBot	md.dll			
3f0879776f937dbb75e02826b39e09c0	QakBot	md.exe			
69ed71c758f31293e2e37e43d10a7fea	QakBot	md.exe	domain01		
8d2214d32e76ec51f9961aba3a92f8d4	QakBot	AdminPrivSetting.exe	domain01		
e7f7b215d2929225856641cb208c42ca	QakBot	mdo.exe	domain01		

The implants found in the incidents handled by the ANSSI from which the configuration was able to be extracted are all linked to the same **QakBot** affiliate, located via the root of the "botnet" field of the configuration: « `domain` ». All additional implants named « `md.exe` » and « `md.dll` », found via pivots, are also linked to the **QakBot** « `domain` » affiliate, which confirms the effectiveness of the search method based on the observed naming convention.

Incident	Hash	File Name	Botnet	Campaign
Gefco	5ed9fb5fc74c6fdb3537629e9b23437a	md.exe	domain01	1597161528
Fareva	04416cf8bf1c7d31a606edff765529df	md.dll	domain02	1606721866

However, on several occasions, **Cobalt Strike** implants communicating with the Akamai/Azure cluster were registered, not by the **QakBot** « `domain` » affiliate but by the **QakBot** « `Obama` » affiliate:

- « `obama35` » botnet: C2 « `azuresecure.tech` » [8, 9]
- « `obama41` » botnet: C2 « `akabox.tech` » [10]
- « `obama?` » botnet: C2 « `akastat.app` » [11]

[11] Emerging in 2009, **QakBot** (aka **Qbot**, **Pinkslipbot**) is a modular Trojan horse used to distribute other payloads, especially ransomware. In 2020, **QakBot** distributed the **ProLock**, **Egregor** and **DoppelPaymer** ransomware. In 2021, given the incident at Pierre Fabre, it appears that **QakBot** can also distribute **Sodinokibi**. **QakBot** operates under an affiliate model [7].

Three hypotheses can explain this observation:

- the « `Obama` » ID is linked to the « `domain` » ID;
- the **Cobalt Strike** Akamai/Azure infrastructure cluster is used by several groups of attackers and is therefore potentially provided by a third-party cyber criminal;
- the **Cobalt Strike** Akamai/Azure infrastructure is provided directly to some of its affiliates by Mallard Spider (aka Gold Lagoon), the cyber criminal group that developed and makes available **QakBot**.

*Comment: The ANSSI cannot draw any conclusions for the moment. However, **QakBot** distributed **Cobalt Strike** implants using C2 servers that are not part of the Akamai/Azure cluster, on multiple occasions [12, 13]. As such, this third hypothesis can reasonably be set aside.*

2.3 Investigation into the use of the Rclone exfiltration tool

In five incidents, the **Rclone** executable, as well as its configuration file, had the same name, spoofing the Windows service « `svchost` ».

Incident	Rclone	File Name
Company A		
Intrinsec – ProLock	■	(svchost.exe)
Gefco	■	svchost.exe svchost.conf
Ouest-France	■	svchost.exe svchost.conf
Fareva		
Company B		
Pierre Fabre	■	svchost.exe
The DFIR Report – Sodinokibi	■	svchost.exe svchost.conf

The **ProLock** incident described by the IT security firm Intrinsec is somewhat unique, as there is no direct reference to « `svchost.exe` », or to the servers used for exfiltration. However, Group-IB indicates that in the **ProLock** incidents, the **Rclone** executable was always renamed to look like legitimate system binaries [14]. It is therefore conceivable that this is also named « `svchost.exe` ».

The use of **Rclone** and the names of its files are not the only commonalities between the different incidents, given that there are also similarities regarding the exfiltration infrastructures used:

- The FTP exfiltration servers observed in the Gefco and Ouest-France incidents had similar self-signed TLS certificates (value « `Kanzas City` » used in the subject), in addition to having an identical version of **vsFTPd**.
- The WebDAV exfiltration servers observed in the incident addressed by The DFIR Report [6], as well as in the Gefco and Ouest-France incidents, had the same HTTP banners, notably the basic authentication named « `realm_name` ». This does not appear to be a known default configuration. Additionally, in the case of The DFIR Report and Gefco, the HTTP servers both exposed a self-signed certificate generated with **OpenSSL**.

Pivots made from these configuration elements made it possible to identify other exfiltration servers potentially used by the same group of attackers:

Source	Exfiltration Server (FTP/WebDAV)	First Seen	Last Seen
Gefco	93.190.140.75	2020-09-23	2020-12-20
Ouest-France	190.2.138.42	2020-11-19	2021-01-04
Pierre Fabre	193.239.84.133	2021-04-03	2021-04-10
Heuristique WebDAV « realm_name »	212.83.61.216	2021-05-05	2021-06-01
Heuristique Web DAV « widg1@ca.ca »	91.90.121.26	2021-04-24	2021-06-07
Heuristique WebDAV « realm_name »	45.147.160.196	2021-02-06	2021-07-03
The DFIR Report – Sodinokibi	45.147.160.5	2021-03-11	2021-07-31
Heuristique WebDAV « realm_name » et FTP « Kanzas City »	85.25.246.169	2021-02-21	2021-08-16

The following diagram summarises these technical links:

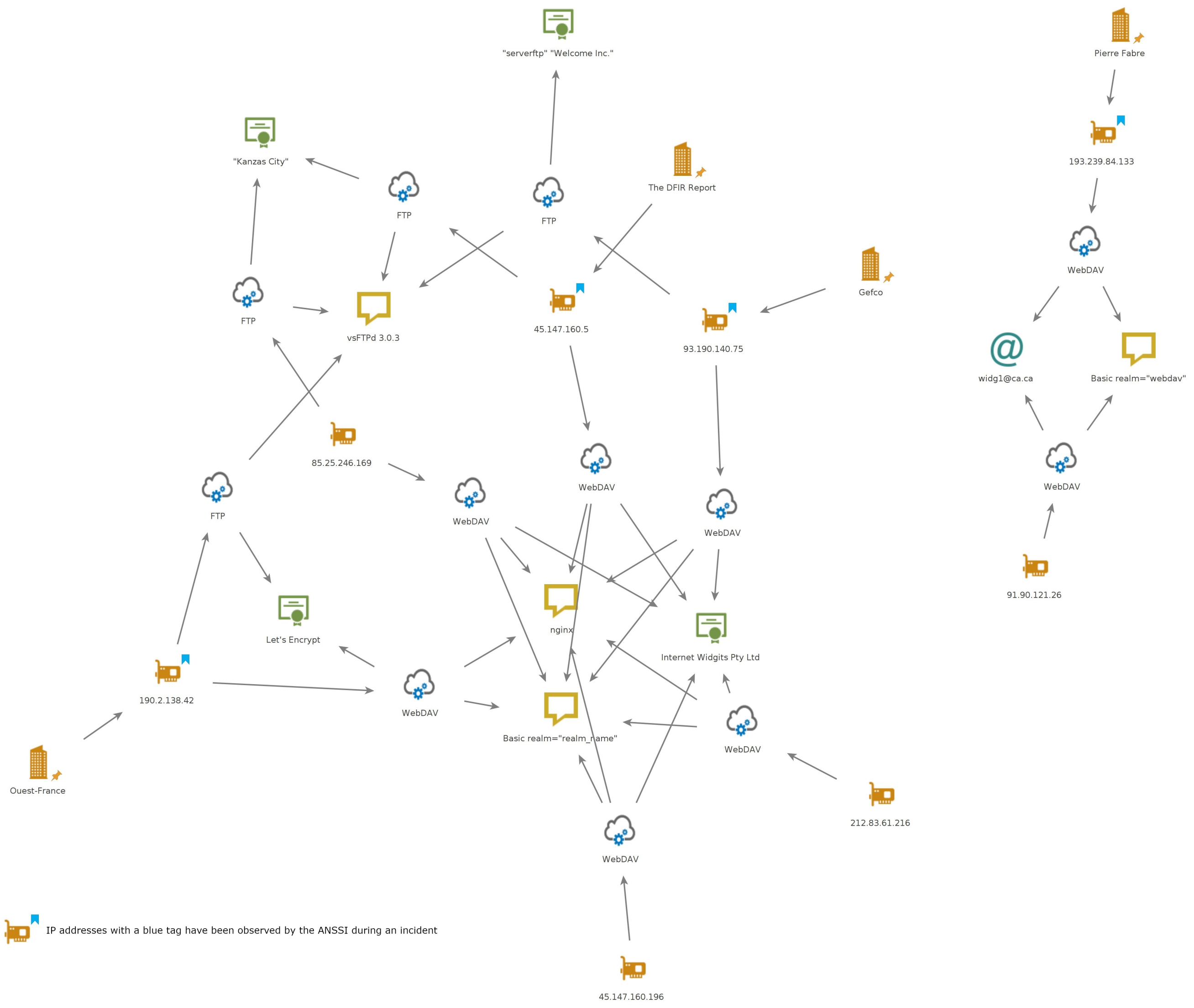


Fig. 2.2 – Summary of the links between the exfiltration servers.

2.4 Conclusion following the investigations

According to the ANSSI's investigations, there is indeed a cyber criminal group responsible for the attacks on Gefco, Company A, Company B, Pierre Fabre, Ouest France, Fareva and those reported by the IT security firms Intrinsec and The DFIR Report.

This group is characterised by the following main TTPs:

- the use of **Cobalt Strike**;
- the use of a **Cobalt Strike** C2 server naming convention spoofing Akamai and Azure domain names;
- the frequent use of the term « `technology` » and its derivatives in its domain names;
- the purchase of domain names from NameCheap;
- the use of exotic TLDs;
- the use of the default TLS certificate of **Cobalt Strike** and Let's Encrypt certificates;
- the hosting of its C2 servers with HostWinds and LeaseWeb;
- the use of **QakBot** as the first payload;
- the application of the "md" naming convention to the **QakBot** implants;
- its connection to the « `domain` » affiliate of **QakBot**, active since June 2020;
- the use of the **Rclone** exfiltration tool;
- the application of the "svchost" naming convention to the **Rclone** executable;
- exfiltration via FTP and WebDAV.

It will now be called "Lockean", based on the WebDAV username used for data exfiltration in the **Egregor** incident at Ouest France.

3 Infection chain associated with Lockean

3.1 Infection vector

3.1.1 Phishing emails distributed by a distribution service

In view of the incidents in which it is involved, Lockean allegedly used the **Emotet** distribution service in 2020 [2, 5], as well as that of TA551 in 2020 and 2021 [15, 16, 7, 17, 18], to distribute **QakBot** via phishing emails:

- During the **Egregor** ransomware attack at Ouest-France [2], the first payload would indeed have been the malicious code **Emotet**[12]. **Emotet** having been generally distributed in phishing emails, via Epoch botnets operated by its developers TA542 [20], it is likely that this infection vector initiated the compromise of Ouest-France. The involvement of the**Emotet** distribution service is confirmed by the report by the IT security firm Intrinsec [5], which describes an infection chain relating to Lockean and also involving it upstream, although its outcome was not to distribute the **Egregor** ransomware, as with Ouest-France, but to distribute the **ProLock** ransomware.
- While TA542 seems to have ceased its activities following the dismantling of **Emotet** at the start of 2021, another distribution service, then less well-known, appears to have been favoured by the cyber criminal group Lockean [6]. This distribution service is that of TA551 (aka Shathak, UNC2420, Gold Cabin)[13].

However, Lockean would not be the only **QakBot** affiliate to use these distribution services [7, 26]. As such, currently, any infection with TA551 aimed at distributing **QakBot** is not sufficient to presume a compromise by Lockean.

3.1.2 Intermediary loaders

In the incidents that the ANSSI links to the Lockean cyber criminal group, the initial access to the IS was achieved using the **QakBot** loader, with the exception of the incident described by The DFIR report, in which the **IcedID** loader was distributed as the first payload[14].

The fact that there was only one hour between the distribution of **IcedID** and **Cobalt Strike** during the incident analysed by The DFIR Report [6] indicates that it is likely there was a single attacker, a user common to the loader and the ransomware (in this case, **Sodinokibi**), rather than two attackers.

Lockean is nevertheless not thought to be the only common affiliate of **QakBot** and **IcedID** [7].

3.2 Lateral movement

During the lateral movement phase of the various incidents, four tools were observed: **Cobalt Strike**, **Adfind**, **BloodHound** and **BITSadmin**. Frequent use of **Cobalt Strike**, **Adfind** and **BITSadmin** was observed, while **BloodHound** seems less used.

[12] This code, operated by the cyber criminal group TA542, was, from 2017 until it was dismantled in January 2021 [19], a malware loader for clients.

[13] Active since 2018, it involves distributing malware on behalf of clients through massive phishing email campaigns [21, 17, 22, 15, 23, 24]. These emails are characterised by the fact that they often respond to legitimate discussion threads (*email thread hijacking*), that they usually contain an attachment in Zip format, sometimes protected by a password provided in the email, that this Zip file contains a booby-trapped Word or Excel file and that this Word or Excel file uses a DocuSign template generated by the tool **EtterSilent** [25, 16].

[14] In the incident covered by The DFIR Report [6], **IcedID** seems to have been distributed by **EtterSilent** [27], which could confirm that Lockean also used the services of TA551 to distribute **IcedID** (although TA551 is not the only cyber criminal group to use the **EtterSilent** tool).

Incident	Cobalt Strike	AdFind	BloodHound	BITSadmin
Company A				
Intrinsec – ProLock		■		■
Gefco	■	■	■	■
Ouest-France	■	■		■
Fareva	■			
Company B	■			
Pierre Fabre	■			
The DFIR Report – Sodinokibi	■	■	■	■

Note that the lack of observation of a tool does not mean that it was not used.

3.3 Exfiltration

Before encryption, Lockean exfiltrates its victims' data using the **Rclone** tool, which it renames by spoofing the name of the Windows service "svchost".

3.4 Encryption

The ANSSI's investigations have identified several ransomware (RaaS) programs with which Lockean has been affiliated.

3.4.1 Maze, Egregor and ProLock

During the two **Egregor** incidents at Gefco [1] and Ouest-France [2] attributed to Lockean by the ANSSI, the IP address « `185.238.0.233` » was used by the attackers to distribute scripts, as well as ransomware strains.

Incident	URL	MD5	Comment
Ouest-France	http://185.238.0.233/archbi.zip	-	Rclone
Gefco	http://185.238.0.233/b.dll	a654b3a37c27810db180822b72ad6d3e	Egregor

According to the IT security firms Intrinsec [5] and Cybereason [28], this IP address was also observed in a **ProLock** incident, in which it distributed the files « `connect.bat` » and « `office.txt` » [5].

Incident	URL	SHA1
Intrinsec – ProLock	http://185.238.0.233/office.txt	4769a775fd4a2c29b433736a59dc4277354a54f2
Intrinsec – ProLock	http://185.238.0.233/connect.bat	f5b14cc494303c91456bb50e7816358b6766a5b8

Strains of the **Maze** [15] ransomware have also been distributed from this IP address:

[15] Maze is RaaS that emerged in May 2019 and disappeared in August 2020. It is known in particular for having introduced the principle of double extortion in September 2019, in other words exfiltration of victims' data and the threat of disclosure on a site in.onion if the ransom is not paid. **Egregor** is seen as the RaaS successor of **Maze** [29].

URL	MD5
http://185.238.0.233/hnt.dll	c96df334b5ed70473ec6a58a545208b6
http://185.238.0.233/hnt.dll	81bc3a2409991325c6e71a06f6b7b881
http://185.238.0.233/kk.dll	e406d6097c42b81d5bcebe1827e66a19
http://185.238.0.233/p.dll	e95053d1eac4d0e48cdf1b633b12999f

As such, Lockean has been affiliated with the three RaaS Maze, Egregor and ProLock.

3.4.2 DoppelPaymer

Lockean may also have been a **DoppelPaymer** affiliate for the following reasons:

- strains of the **DoppelPaymer** ransomware were also distributed from the aforementioned IP address, according to a code analysis platform:

URL	MD5
http://185.238.0.233/88/k057.exe	44a7085f729b68073b5c67bbc66829cc
http://185.238.0.233/k068.exe	27fa39e6fb066736b4565b961c76f0b5
http://185.238.0.233/k071sm.exe	3a059ab3cbc168987613c137e7a916a9

  Note that in the **DoppelPaymer** incident at Fareva, the ransomware strain was named « `k166sm.exe` ». This name matches the naming convention used for the **DoppelPaymer** strains hosted on the IP address « `185.238.0.233` ». As such, it is possible that it was involved in the incident at Fareva, although this cannot be confirmed due to a lack of sufficient information about this incident, in which the ANSSI was not involved;
- Akamai typosquatting **Cobalt Strike** C2s (« `atakai-technologies.host` », « `akamai-technologies.site` » and « `akamai-technologies.space` ») were found in incidents leading to encryption by **DoppelPaymer** [30, 31], thereby supplementing the ANSSI's observations about the **DoppelPaymer** incidents at Company A and Fareva;
- **DoppelPaymer** was already distributed by **QakBot** (irrespective of whether it was distributed upstream by **Emotet**) [32];
- the renaming of **QakBot** as « `md.exe` », specific to the « `domain` » affiliate and therefore to Lockean, was found during the **DoppelPaymer** incident at Company A in June 2020.

3.4.3 Sodinokibi

On 31 March 2021, the ANSSI was alerted to the encryption of the company Pierre Fabre. During this attack, the « `domain02` » affiliate of **QakBot** distributed **Cobalt Strike** (one of the Akamai typosquatting C2s), **Rclone** (file renamed « `svchost.exe` ») and the **Sodinokibi** ransomware. Based on common infrastructure links and TTPs, the ANSSI deduced that Lockean was behind the compromise of Pierre Fabre's IS, as well as the infection chain described by The DFIR Report [6].

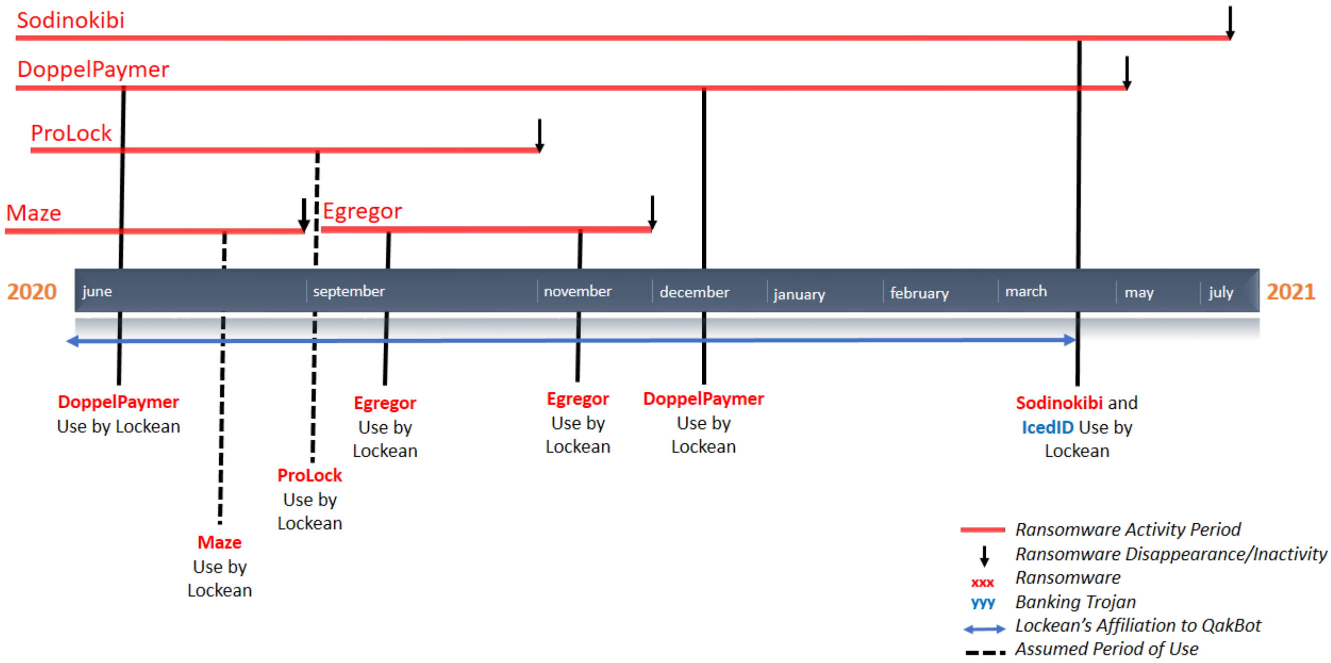


Fig. 3.1 – Known Lockean activity compared to the ransomware activity period

Lockean would have used:

- **DoppelPaymer**: since at least June 2020;
- **Egregor**: since its appearance in September 2020 [1]. By inference, the fact that Lockean may have used Maze and that Egregor took over from Maze in September 2020 after its discontinuation suggests that Lockean transferred its affiliation from Maze to Egregor, as intended by the developers of Maze [29]. However, it is not known to the ANSSI when Lockean began using **Maze**;
- **Sodinokibi**: since at least March 2021 [4, 6];
- **ProLock**: the period of use of this ransomware by Lockean is not identified, although it may have been concurrent with that of **Egregor** [5].

*Comment: The final shutdown of **Maze** around November 2020 and the dismantling of **Egregor** in February 2021 may have prompted Lockean to turn to the direct competitor of **Maze**, namely **Sodinokibi**. The inactivity of **Sodinokibi** from 13 July 2021 until early September could have prompted Lockean to temporarily replace it with another RaaS. In addition, as the RaaS **Grief**[16] supposedly took over from **DoppelPaymer** [33], it is possible that Lockean will use **Grief** in the future.*

3.5 Double extortion principle

The constant exfiltration of the victim's data before encryption and the existence of disclosure sites associated with the RaaS with which Lockean is affiliated (with the exception of **ProLock**) confirm that this cyber criminal group is a follower of the double extortion principle, in other words that it exfiltrates its victims' data and threatens to disclose it, to get them to pay the ransom, after encryption.

If the ransom is paid, Lockean only keeps an average of 70%, the remainder going to the developers of the RaaS

[16] Emerging at the end of May 2021, **Grief** (aka Pay, Deuil ransomware) is deemed to be the successor to DoppelPaymer and therefore to be operated by the same attackers. There are in fact no more publications of victims on the disclosure site associated with **DoppelPaymer** since early May 2021 and the first sample of **Grief** discovered pointed to the latter [33].

[34].

3.6 Summary of the infection chain

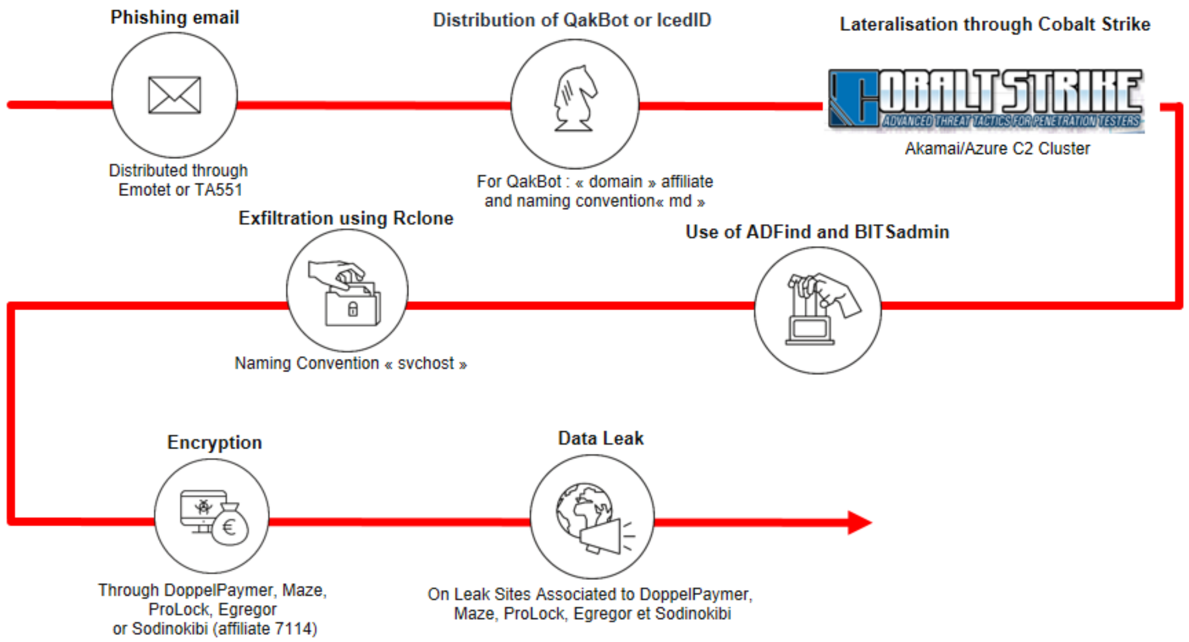

Phishing email
Distributed through Emotet or TA551
Distribution of QakBot or IcedID
For QakBot : « domain » affiliate and naming convention« md »
Lateralisation through Cobalt Strike
COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS
Akamai/Azure C2 Cluster
Exfiltration using Rclone
Naming Convention « svchost »
Use of ADFind and BITSadmin
Encryption
Through DoppelPaymer, Maze, ProLock, Egregor or Sodinokibi (affiliate 7114)
Data Leak
On Leak Sites Associated to DoppelPaymer, Maze, ProLock, Egregor et Sodinokibi

Fig. 3.2 – Summary infection chain associated with the Lockean cyber criminal group

4 Conclusion

Lockean's targeting is opportunistic and dependent on the distribution services it employs (**Emotet**, TA551).

Nevertheless, Lockean has a propensity to target French entities under a Big Game Hunting[17] [1, 4, 2] rationale and therefore represents a threat to watch out for.

Comment: Interestingly, despite being affiliated with ransomware that precludes targeting of entities located in Commonwealth of Independent States (CIS) countries, Lockean attacked the French transport company Gefco in 2020, even though Gefco is 75% owned by Russian Railways. Therefore, it is possible that Lockean was not aware of violating the "rules of engagement" - widely respected- for ransomware it uses.

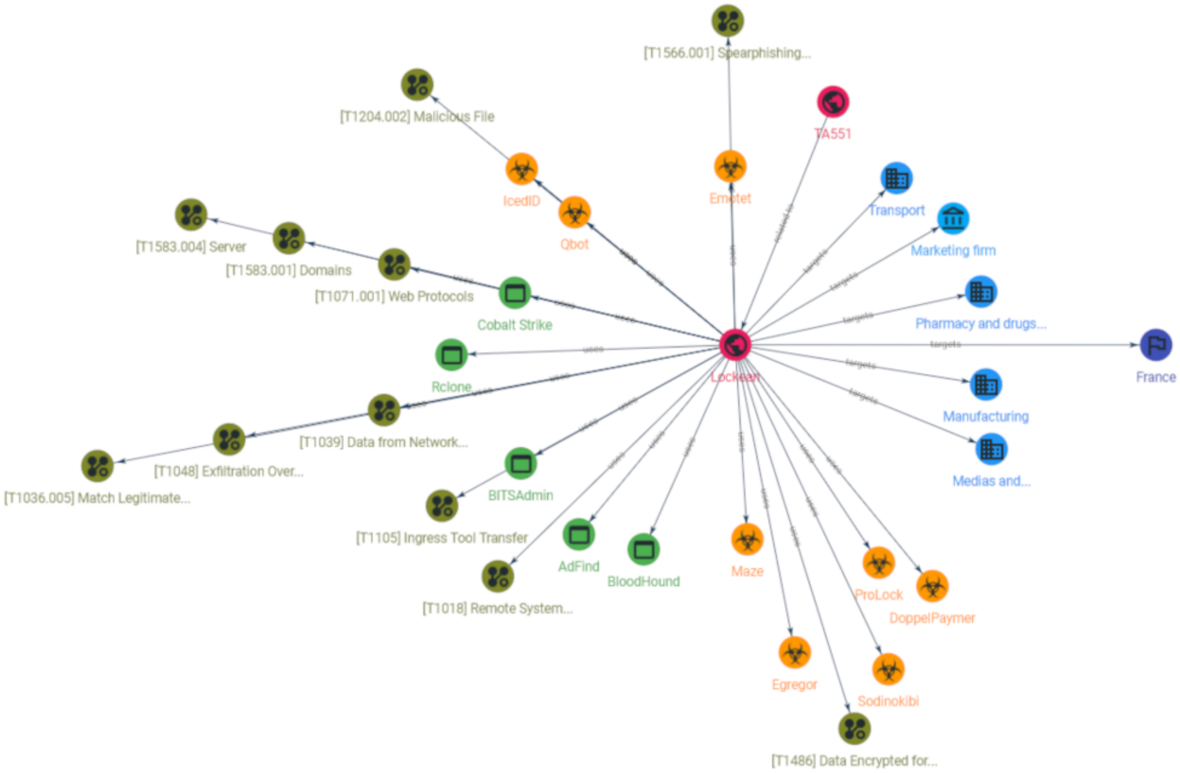


Fig. 4.1 – OpenCTI illustration of the Lockean attacker group

[17] Big Game Hunting involves – for cyber criminal groups with significant financial resources and technical skills – focusing on targeting particular companies and institutions in their ransomware attacks. This targeting is characterised in particular by advance preparation for extortion operations, sometimes several months ahead of time.

5 Appendix

5.1 Summary of the links between incidents related to the Lockean group

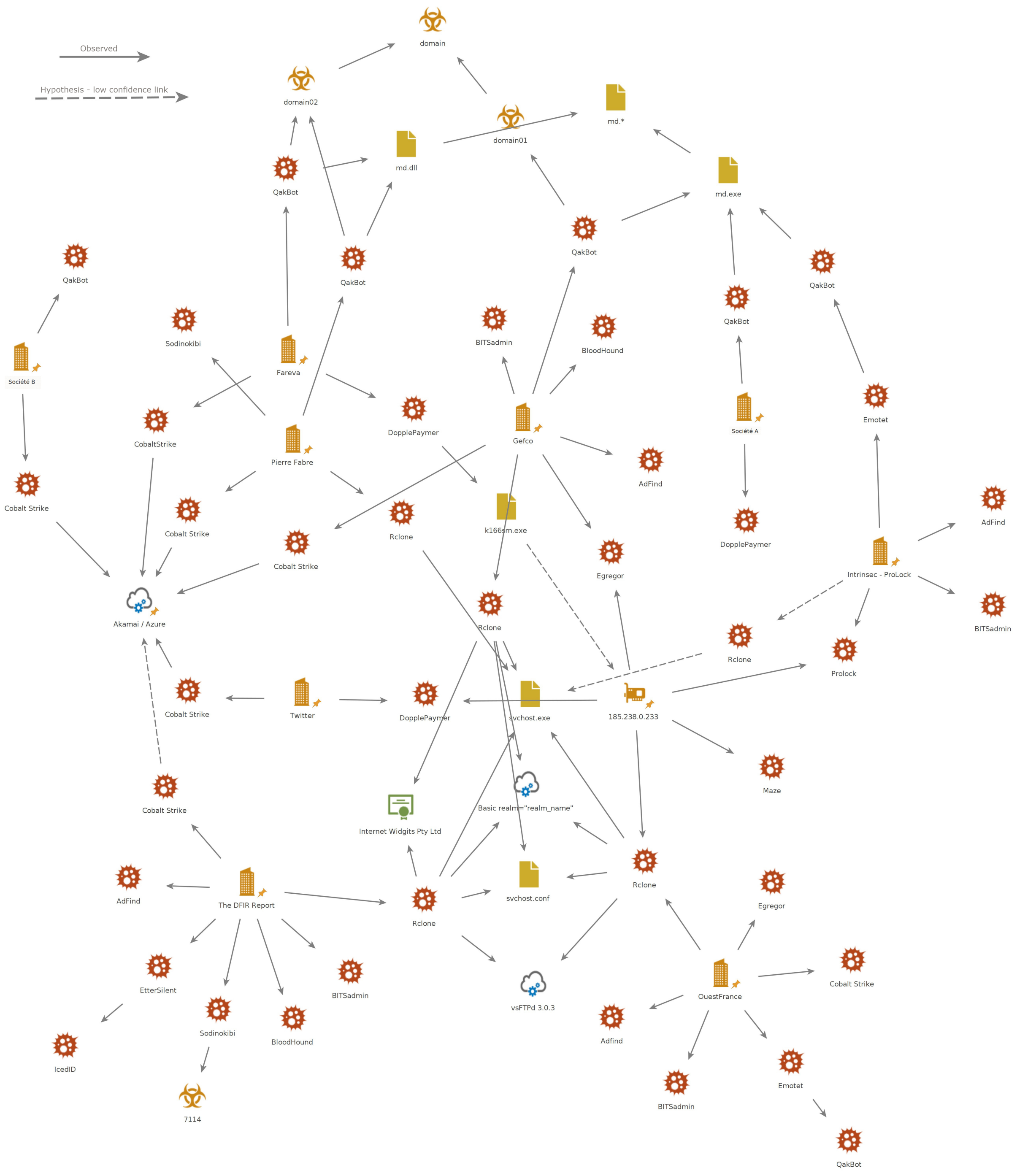


Fig. 5.1 – Summary of the links between incidents related to the Lockean group

5.2 Table of TTPs according to the MITRE ATT&CK framework

Identifier	Name	Comments
T1583.001	Acquire Infrastructure: Domains	Use of Namecheap registrar and naming convention Akamai / Azure
T1583.004	Acquire Infrastructure: Server	CobaltStrike C2 servers are mainly hosted by HostWinds and LeaseWeb
T1566.001	Phishing: Spearphishing Attachment	Spearphinshing emails distributed by Emotet or TA551
T1204.002	User Execution: Malicious File	Emotet QakBot or IcedID
T1036.005	Masquerading - Match Legitimate Name or Location	Rclone renamed svchost
T1018	Remote System Discovery	Use of Adfind of BloodHound
T1039	Data from Network Shared Drive	Data Collection Prior to Exfiltration
T1071.001	Application Layer Protocol: Web Protocols	HTTPS communications with CobaltStrike C2 servers
T1105	Ingress Tool Transfer	Use of BITSadmin
T1048	Exfiltration Over Alternative Protocol	Data Exfiltration through FTP or WebDAV using Rclone
T1486	Data Encrypted for Impact	Use of DopplePaymer Maze Prolock Egregor or Sodinokibi Ransomware

5.3 Indicators of compromise

Indicator	Comment
amajai-technologies.network	Cobalt Strike C2 Server
amajai-technologies.industries	Cobalt Strike C2 Server
cloudflace-network.digital	Cobalt Strike C2 Server
stackpatc-technologies.digital	Cobalt Strike C2 Server
rackspare-technology.digital	Cobalt Strike C2 Server
asurecloud.tech	Cobalt Strike C2 Server
akamacloud.tech	Cobalt Strike C2 Server
asureupdate.tech	Cobalt Strike C2 Server
asureupdate.pro	Cobalt Strike C2 Server
akamaclouds.app	Cobalt Strike C2 Server
cloudmetric.online	Cobalt Strike C2 Server
smalleststores.com	Cobalt Strike C2 Server
akastat.app	Cobalt Strike C2 Server
azurestat.app	Cobalt Strike C2 Server
cdnengine.biz	Cobalt Strike C2 Server
akamaclouds.tech	Cobalt Strike C2 Server
akabox.space	Cobalt Strike C2 Server
setupfastonline.com	Cobalt Strike C2 Server
akamalupdate.site	Cobalt Strike C2 Server
securitypanels.org	Cobalt Strike C2 Server
c2.hax.vg	Cobalt Strike C2 Server
azuresecure.tech	Cobalt Strike C2 Server
securesurvey.cloud	Cobalt Strike C2 Server
akabox.tech	Cobalt Strike C2 Server
electronicwhosaleonline.com	Cobalt Strike C2 Server
madesecuritybusiness.com	Cobalt Strike C2 Server
ropesecuritybusiness.com	Cobalt Strike C2 Server
knotsecuritybusiness.com	Cobalt Strike C2 Server
ticksecuritybusiness.com	Cobalt Strike C2 Server
entirelysecuritybusiness.com	Cobalt Strike C2 Server
hesitatesecuritybusiness.com	Cobalt Strike C2 Server
stexwhosaleonline.com	Cobalt Strike C2 Server
dealsforyoutoday.org	Cobalt Strike C2 Server
onlineceoshelp.com	Cobalt Strike C2 Server
risetomoon.com	Cobalt Strike C2 Server
notescloud.org	Cobalt Strike C2 Server

amasonstore.com	Cobalt Strike C2 Server
classworldint.com	Cobalt Strike C2 Server
orientalclient.com	Cobalt Strike C2 Server
perfectappt.com	Cobalt Strike C2 Server
displaychecks.com	Cobalt Strike C2 Server
itstrueloves.com	Cobalt Strike C2 Server
adjustclouds.com	Cobalt Strike C2 Server
killsecuritybusiness.com	Cobalt Strike C2 Server
securitybusinessmean.com	Cobalt Strike C2 Server
justicedev.com	Cobalt Strike C2 Server
amamai-tecnologies.cloud	Cobalt Strike C2 Server
amamai-tecnologies.digital	Cobalt Strike C2 Server
amamai-tecnologies.space	Cobalt Strike C2 Server
amatai-technologies.digital	Cobalt Strike C2 Server
amatai-technologies.site	Cobalt Strike C2 Server
amatai-technologies.space	Cobalt Strike C2 Server
amatai-technologies.website	Cobalt Strike C2 Server
atakai-technologies.host	Cobalt Strike C2 Server
atakai-technologies.online	Cobalt Strike C2 Server
atakai-technologies.space	Cobalt Strike C2 Server
atakai-technologies.website	Cobalt Strike C2 Server
atakai-technologies.work	Cobalt Strike C2 Server
akamai-technologies.digital	Cobalt Strike C2 Server
akamai-technologies.host	Cobalt Strike C2 Server
akamai-technologies.online	Cobalt Strike C2 Server
akamai-technologies.site	Cobalt Strike C2 Server
akamai-technologies.space	Cobalt Strike C2 Server
akamai-technologies.website	Cobalt Strike C2 Server
amajai-technologies.digital	Cobalt Strike C2 Server
amajai-technologies.host	Cobalt Strike C2 Server
amajai-technologies.space	Cobalt Strike C2 Server
amajai-technologies.tech	Cobalt Strike C2 Server
amajai-technologies.website	Cobalt Strike C2 Server
amajai-technologies.online	Cobalt Strike C2 Server
amajai-technologies.site	Cobalt Strike C2 Server
amajai-technologies.support	Cobalt Strike C2 Server
amajai-technologies.trade	Cobalt Strike C2 Server
amajai-technologies.work	Cobalt Strike C2 Server
amajai-technologies.world	Cobalt Strike C2 Server
amazai-technologies.online	Cobalt Strike C2 Server
amazai-technologies.site	Cobalt Strike C2 Server
amazai-technologies.space	Cobalt Strike C2 Server
amazai-technologies.support	Cobalt Strike C2 Server
amazai-technologies.website	Cobalt Strike C2 Server
amazai-technologies.world	Cobalt Strike C2 Server
amapai-technologies.digital	Cobalt Strike C2 Server
amapai-technologies.email	Cobalt Strike C2 Server
amapai-technologies.site	Cobalt Strike C2 Server
amapai-technologies.space	Cobalt Strike C2 Server
amapai-technologies.support	Cobalt Strike C2 Server
amapai-technologies.website	Cobalt Strike C2 Server
amapai-technologies.work	Cobalt Strike C2 Server
amapai-technologies.world	Cobalt Strike C2 Server
rackspare-technology.download	Cobalt Strike C2 Server
rackspare-technology.network	Cobalt Strike C2 Server
rackspare-technology.online	Cobalt Strike C2 Server
rackspare-technology.space	Cobalt Strike C2 Server
akamacloud.pro	Cobalt Strike C2 Server

asurecloud.pro	Cobalt Strike C2 Server
93.190.140.75	Exfiltration Server [2020-09-23:2020-12-20]
190.2.138.42	Exfiltration Server [2020-11-19:2021-01-04]
193.239.84.133	Exfiltration Server [2021-04-03:2021-04-10]
212.83.61.216	Exfiltration Server [2021-05-05:2021-06-01]
91.90.121.26	Exfiltration Server [2021-04-24:2021-06-07]
45.147.160.196	Exfiltration Server [2021-02-06:2021-07-03]
45.147.160.5	Exfiltration Server [2021-03-11:2021-07-31]
85.25.246.169	Exfiltration Server [2021-02-21:2021-08-16]
185.238.0.233	Script and ransowmare distribution server [2020-07-20:2021-01-09]

6 Bibliography

[1] GEFCO. *Message de Luc Nadal : Point à date sur la reprise de GEFCO après une cyber-attaque*. September 28, 2020.
URL: https://www.gefco.net/fr/newsroom/detail/news/message-de-luc-nadal-point-a-date-sur-la-reprise-de-gefco-apres-une-cyber-attaque/.

[2] Ouest France. *RÉCIT. Dans les coulisses de la cyberattaque vécue à Ouest-France*. February 2, 2021.
URL: https://www.ouest-france.fr/societe/cyberattaque/dans-les-coulisses-de-la-cyberattaque-vecue-a-ouest-france-7139874.

[3] ZDNet. *Santé : Le Fabricant Pharmaceutique Fareva Bloqué Par Une Cyberattaque*. January 5, 2021.
URL: https://www.zdnet.fr/actualites/sante-le-fabricant-pharmaceutique-fareva-bloque-par-une-cyberattaque-39915609.htm.

[4] Pierre Fabre. *Pierre Fabre annonce le retour progressif à la normale de son activité après avoir été victime d'une cyberattaque*. May 3, 2021.
URL: https://www.pierre-fabre.com/fr/communique_presse/pierre-fabre-annonce-le-retour-progressif-a-la-normale-de-son-activite-apres.

[5] Intrinsec. *Egregor – Prolock: Fraternal Twins ?* November 12, 2020.
URL: https://www.intrinsec.com/egregor-prolock/.

[6] The DFIR Report. *Sodinokibi (Aka REvil) Ransomware*. March 29, 2021.
URL: https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/.

[7] Seguranca Informatica. *A Taste of the Latest Release of QakBot*. May 4, 2021.
URL: https://seguranca-informatica.pt/a-taste-of-the-latest-release-of-qakbot/.

[8] Twitter. *@malware_traffic - #CobaltStrike activity on azuresecure[.]tech*. April 29, 2021.
URL: https://twitter.com/malware_traffic/status/1387554560554815488.

[9] URLhaus. *http://190.14.37.252/44313,6048108796.dat*. April 28, 2021.
URL: https://urlhaus.abuse.ch/url/1180447/.

[10] Twitter. *@Artillerie*. May 14, 2021.
URL: https://twitter.com/Artilllerie/status/1393189959272644613.

[11] Twitter. *@Unit42_Intel*. May 11, 2021.
URL: https://twitter.com/Unit42_Intel/status/1392174941181812737.

[12] Twitter. *@malware_traffic - Quick post: #Qakbot (#Qbot) infection with #CobaltStrike on 82.117.252[.]32 at test-subnet[.]com*. May 22, 2021.
URL: https://twitter.com/malware_traffic/status/1395894771898531845.

[13] Twitter. *@malware_traffic - #Qakbot (#Qbot) infection with #CobaltStrike traffic to 5.34.182[.]3*. May 22, 2021.
URL: https://twitter.com/malware_traffic/status/1395883850010669057.

[14] Group-IB. *ATT&CKing ProLock Ransomware*. September 24, 2020.
URL: https://www.group-ib.com/blog/prolock.

[15] SANS Internet Storm Center. *TA551 (Shathak) Word Docs Push Qakbot (Qbot)*. January 26, 2021.
URL: https://isc.sans.edu/forums/diary/TA551+Shathak+Word+docs+push+Qakbot+Qbot/27030.

[16] Bleeping Computer. *QBot Malware Is Back Replacing IcedID in Malspam Campaigns*. April 13, 2021.
URL: https://www.bleepingcomputer.com/news/security/qbot-malware-is-back-replacing-icedid-in-malspam-campaigns/.

[17] Trend Micro. *QAKBOT Trojan Resurgence*. December 17, 2020.
URL: https://success.trendmicro.com/solution/000283381.

[18] AT&T Cybersecurity - AlienLabs. *The Rise of QakBot*. April 15, 2021.
URL: https://cybersecurity.att.com/blogs/labs-research/the-rise-of-qakbot.

[19] Europol. *Wrold's Most Dangerous Malware Emotet Disrupted through Global Action*. January 27, 2021.
URL: https://europol.europa.eu/newsroom/news/wrold's-most-dangerous-malware-emotet-disrupted-through-global-action.

[20] ANSSI. *Le Code Malveillant Emotet : Origines et Usages*. October 27, 2020.

[21] Bitdefender. *New TA551 Campaign Uses IceID, Complex Attack Chain to Compromise*. January 1, 2020.
URL: https://www.bitdefender.fr/files/News/CaseStudies/study/391/IceID-CREAT-5156.pdf.

[22] SANS Internet Storm Center. *TA551 (Shathak) Word Docs Push IcedID (Bokbot)*. August 1, 2020. URL: https://isc.sans.edu/forums/diary/TA551+Shathak+Word+docs+push+IcedID+Bokbot/26438/.

[23] Palo Alto. *TA551: Email Attack Campaign Switches from Valak to IcedID*. January 7, 2021. URL: https://unit42.paloaltonetworks.com/ta551-shathak-icedid/.

[24] Mimecast. *TA551/Shathak Threat Research*. January 1, 2020. URL: https://www.mimecast.com/resources/white-papers/taa551-shathak-threat-research/.

[25] Bleeping Computer. *EtterSilent Maldoc Builder Used by Top Cybercriminal Gangs*. April 6, 2021. URL: https://www.bleepingcomputer.com/news/security/ettersilent-maldoc-builder-used-by-top-cybercriminal-gangs/.

[26] Binary Defense. *IcedID GZIPLOADER Analysis*. March 12, 2021. URL: https://www.binarydefense.com/icedid-gziploader-analysis/.

[27] Intel 471. *EtterSilent: The Underground's New Favorite Maldoc Builder*. April 6, 2021. URL: https://www.intel471.com/blog/ettersilent-maldoc-builder-macro-trickbot-qbot.

[28] Cybereason. *Cybereason vs. Egregor Ransomware*. November 26, 2020. URL: https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware.

[29] ANSSI. *Le Rançongiciel Egregor*. January 5, 2021. URL: https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-012/.

[30] Twitter. *@smoothimpact*. September 21, 2020. URL: https://twitter.com/smoothimpact/status/1308033998371905538.

[31] Twitter. *@GossiTheDog - Three IPs used by DoppelPaymer*. September 14, 2020. URL: https://twitter.com/GossiTheDog/status/1305507379870605313.

[32] Mandiant. *The Evolving Maturity in Ransomware Operations*. December 1, 2020.

[33] Zscaler. *DoppelPaymer Continues to Cause Grief Through Rebranding*. July 28, 2021. URL: https://www.zscaler.com/blogs/security-research/doppelpaymer-continues-cause-grief-through-rebranding.

[34] CERT-FR. *Etat de La Menace Rançongiciel à l'encontre Des Entreprises et Des Institutions*. March 1, 2021. URL: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-001.pdf.

Version 1.0 - October 26, 2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
www.cert.ssi.gouv.fr / cert-fr.cossi@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

SGDSN