TLP:WHITE

IDENTIFICATION D'UN NOUVEAU GROUPE CYBERCRIMINEL : LOCKEAN

Version 1.0

25 octobre 2021

TLP:WHITE

Sommaire

1 Contexte : liens entre plusieurs incidents sur le périmètre français . . . 3

2 Investigations et découverte du groupe cybercriminel Lockean . . . 6
2.1 Investigation relative à l'infrastructure C2 Cobalt Strike impliquée . . . 6
2.2 Investigation relative aux implants QakBot utilisés . . . 10
2.3 Investigation relative à l'utilisation de l'outil d'exfiltration Rclone . . . 11
2.4 Conclusion à l'issue des investigations . . . 13

3 Chaîne d'infection associée à Lockean . . . 14
3.1 Vecteur d'infection . . . 14
3.1.1 Courriels d'hameçonnage distribués par un service de distribution . . . 14
3.1.2 *Loaders* intermédiaires . . . 14
3.2 Latéralisation . . . 14
3.3 Exfiltration . . . 15
3.4 Chiffrement . . . 15
3.4.1 Maze, Egregor et ProLock . . . 15
3.4.2 DoppelPaymer . . . 16
3.4.3 Sodinokibi . . . 16
3.5 Principe de double extorsion . . . 17
3.6 Récapitulatif de la chaîne d'infection . . . 18

4 Conclusion . . . 19

5 Annexe . . . 20
5.1 Synthèse des liens entre les incidents reliés au groupe Lockean . . . 20
5.2 Tableau des TTPs d'après le référentiel MITRE ATT&CK . . . 21
5.3 Indicateurs de compromission . . . 21

6 Bibliographie . . . 24

1 Contexte : liens entre plusieurs incidents sur le périmètre français

Sur la période 2020-2021, les compromissions suivantes du système d'information (SI) d'entreprises françaises par le code malveillant **QakBot** ont été signalées à l'ANSSI :

- Compromission d'une société française du secteur manufacturier en juin 2020, qui sera appelée par la suite "Société A", ;
- Compromission de la société de transport Gefco en septembre 2020 [1];
- Compromission du journal Ouest-France en novembre 2020 [2];
- Compromission du groupe pharmaceutique Fareva mi-décembre 2020 [3];
- Compromission d'une société de services française en février 2021, qui sera appelée par la suite "Société B", ;
- Compromission de l'entreprise pharmaceutique Pierre Fabre fin mars 2021 [4].

Outre la présence constante de **QakBot** en tant que première charge utile, certains incidents présentaient d'autres points communs :

- dans quatre incidents (Société A, Gefco, Fareva, Pierre Fabre) [1], la convention de nommage de la charge utile **QakBot** était la même ;
- dans cinq incidents (Gefco, Fareva, Pierre Fabre, Ouest-France, société B), l'emploi de **Cobalt Strike** a été observé ;
- dans quatre incidents parmi ceux-ci (Gefco, Fareva, Pierre Fabre, Société B) [2], les noms de domaine des serveurs de commande et de contrôle (C2) associés à **Cobalt Strike** présentaient la même convention de nommage : ils usurpaient des domaines d'Akamai [3] et d'Azure [4]. Cette infrastructure est nommée Cluster Akamai/Azure dans la suite du document ;
- dans trois incidents (Gefco, Ouest-France, Pierre Fabre) [5], l'outil d'exfiltration **Rclone** [6] a été employé avec une même convention de nommage de l'exécutable et de son fichier de configuration, basée sur l'usurpation du service Windows "svchost".

En outre, deux rapports disponibles en sources ouvertes décrivent des chaînes d'infection présentant les mêmes caractéristiques : l'un de l'éditeur Intrinsec relatif aux rançongiciels **ProLock** et **Egregor** [5] et l'autre de The DFIR Report concernant le rançongiciel **Sodinokibi** [6].

1. La convention de nommage employée lors des incidents Ouest-France et Société B n'est connue ni de l'ANSSI, ni des victimes.
2. L'infrastructure de l'implant **Cobalt Strike** découverte chez Ouest-France n'est connue ni de l'ANSSI, ni des victimes.
3. Akamai Technologies est une société américaine spécialisée dans la mise à disposition de serveurs de cache pour les entreprises.
4. Microsoft Azure est la plateforme de services nuagiques de Microsoft.
5. L'outil d'exfiltration éventuellement utilisé lors des incidents A, B et Fareva n'est connu ni de l'ANSSI, ni des victimes.
6. **Rclone** est un outil *open-source* en ligne de commande utilisé pour gérer ou migrer du contenu sur des services nuagiques.

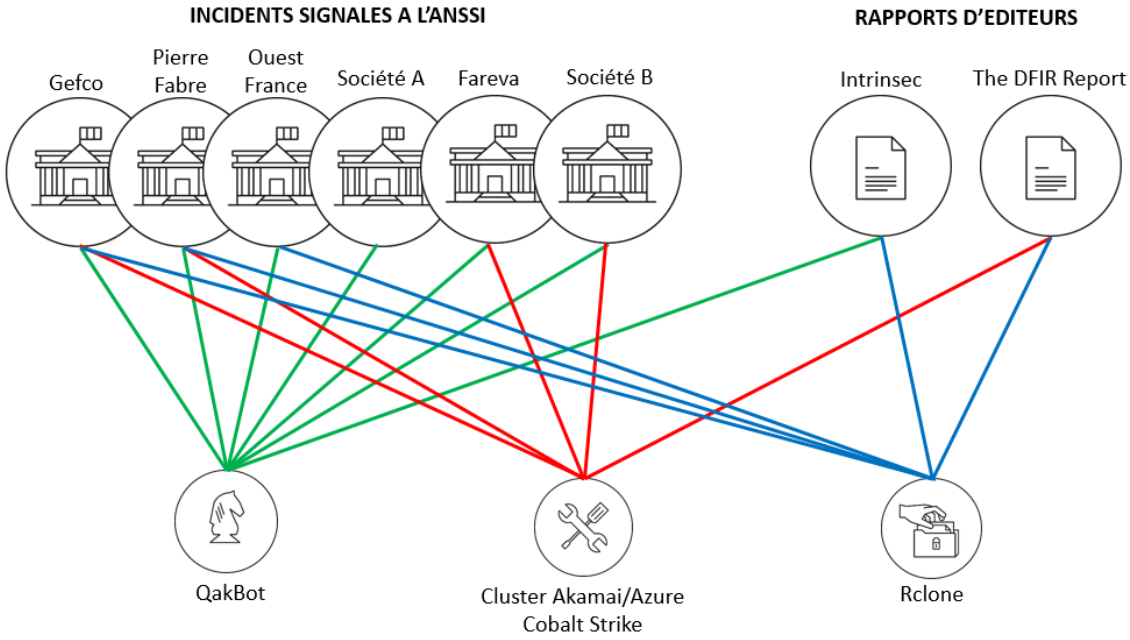

Fig. 1.1 – Liens entre plusieurs incidents et rapports d'éditeurs

Au vu de ces points communs, un même groupe d'attaquants pourrait être à l'origine des six incidents signalés à l'ANSSI et faire l'objet des rapports d'Intrinsec et de The DFIR Report.

De plus, étant donné que :

- les incidents chez Gefco et Ouest-France ont abouti à la propagation du rançongiciel **Egregor** [7],
- l'incident chez Pierre Fabre et celui décrit par The DFIR Report ont abouti à la propagation du rançongiciel **Sodinokibi** [8],
- les incidents chez la société A et Fareva ont abouti à la propagation du rançongiciel **DoppelPaymer** [9],
- l'incident décrit par Intrinsec a abouti à la propagation du rançongiciel **ProLock** [10],
- tous ces rançongiciels fonctionnent selon le modèle économique du *Ransomware-as-a-Service* (RaaS),

ce groupe aurait été affilié depuis sa première observation en juin 2020 à plusieurs RaaS dont Egregor, Sodinokibi, DoppelPaymer et ProLock.

7. Egregor est un RaaS apparu au début du second semestre 2020 et supposément opéré par le groupe cybercriminel à l'origine de son prédécesseur : Maze. Egregor a été démantelé en février 2021 par une opération de police.
8. Apparu en 2019, Sodinokibi (alias REvil) est un RaaS opéré par le groupe cybercriminel Pinchy Spider. Un site de divulgation de données des victimes est associé à ce rançongiciel.
9. DoppelPaymer est un rançongiciel de la famille de BitPaymer et opéré par le groupe cybercriminel Doppel Spider. Il serait devenu un RaaS à partir de 2020. Un site de divulgation de données des victimes est associé à ce rançongiciel depuis février 2020.
10. ProLock est un rançongiciel apparu début 2020 et disparu au cours du troisième trimestre de la même année.

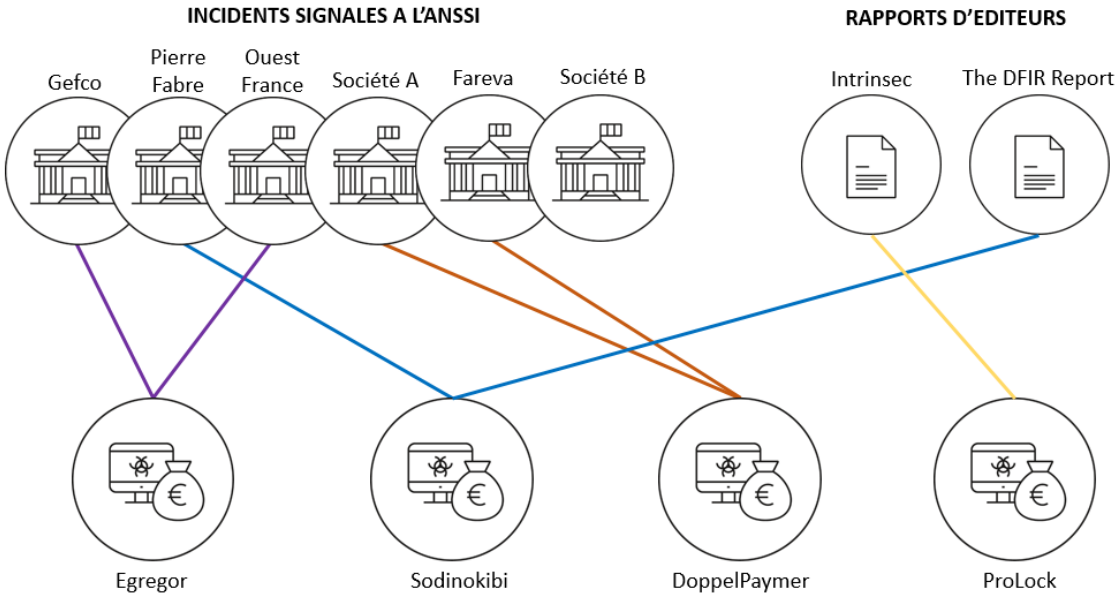

Fig. 1.2 – RaaS employés au cours de ces différents incidents

2 Investigations et découverte du groupe cybercriminel Lockean

Sur la base de ces incidents et de leurs points communs, des investigations ont été menées par l'ANSSI afin de confirmer l'existence de ce groupe cybercriminel, de comprendre son *modus operandi* et de distinguer ses principales Techniques, Tactiques et Procédures (TTPs).

Commentaire : L'ANSSI n'a pas connaissance de précédents travaux reliant techniquement toutes ces activités malveillantes et les associant à un même groupe d'attaquants.

2.1 Investigation relative à l'infrastructure C2 Cobalt Strike impliquée

Le tableau ci-dessous répertorie l'infrastructure observée dans plusieurs des incidents où **Cobalt Strike** a été utilisé. Plusieurs noms de domaine des serveurs C2 usurpent des domaines d'Akamai et d'Azure. En outre, le terme « `technology` » (et ses dérivés) se retrouve régulièrement dans les domaines et un même nom de domaine est parfois réutilisé en dérivant son *Top Level Domain* (TLD).

Incident	Nom de domaine	Adresse IP	En-tête "Server"	En-tête "Keep-Alive"	Date de première vue	Date de dernière vue
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
Société B	asurecloud.tech	94.158.244.89	SAF	Timeout=11 max=120	2021-02-09	2021-03-08
Société B	asurecloud.tech	80.209.233.56	apache	Timeout=10 max=100	2021-03-01	2021-03-03
Société B	akamacloud.tech	80.209.233.56	apache	Timeout=10 max=100	2021-03-01	2021-03-03
Société 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

Des caractéristiques de configuration communes, appelées heuristiques de recherche de serveurs C2, et s'appuyant ici sur les valeurs des en-têtes HTTP « `Server` » et « `Keep-Alive` », ont permis d'identifier 33 nouveaux serveurs C2 **Cobalt Strike** :

Valeurs en commun	Nom de domaine	Adresse IP	Date de première vue	Date de dernière vue
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

Plusieurs de ces serveurs C2 reprennent la convention de nommage usurpant Akamai et Azure observée dans les incidents étudiés :

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

A noter que le nom de domaine « `akamalupdate.site` », qui partage des en-têtes communes avec le serveur C2 « `smalleststores.com` » observé par The DFIR Report, correspond à la convention de nommage Akamai/Azure. Ceci constitue un lien technique d'infrastructure entre l'incident décrit par The DFIR Report et ceux observés par l'ANSSI.

Les noms de domaine qui n'utilisent pas la convention de nommage Akamai/Azure sont liés avec une confiance faible à ce *cluster* car les similarités d'en-têtes seules ne semblent pas constituer un élément suffisant pour les regrouper techniquement.

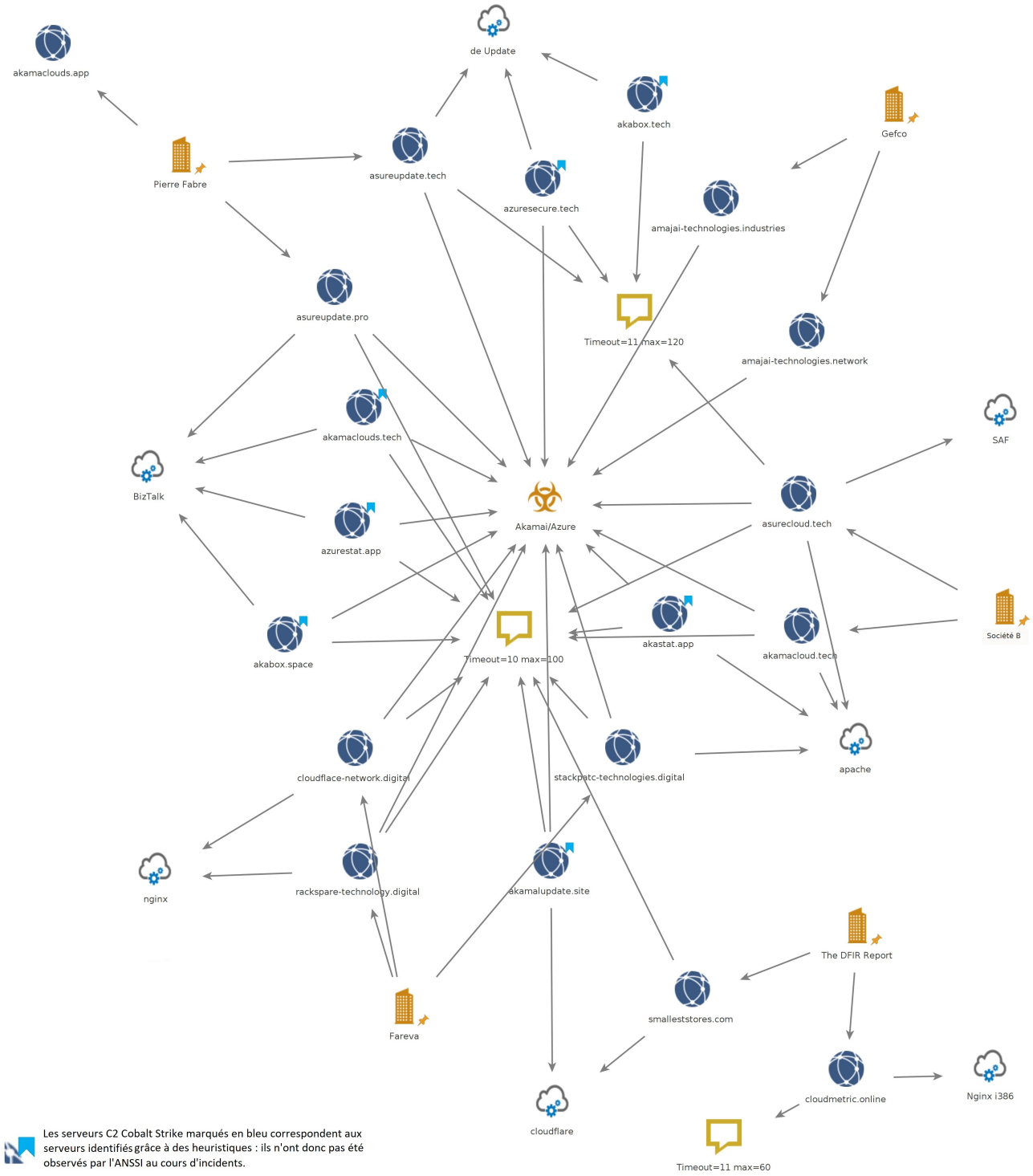

Fig. 2.1 – Synthèse de l'infrastructure **Cobalt Strike**.

Des pivots additionnels sur le format des noms de domaine ont permis d'identifier 49 autres serveurs C2 **Cobalt Strike** du *cluster* Akamai/Azure.

Nom de domaine	Date d'enregistrement	Adresse IP
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

Tous les noms de domaine observés dans les incidents ainsi que ceux issus des pivots ont été achetés chez le registraire Namecheap. Ils utilisent également tous des TLD exotiques, souvent peu onéreux.

Deux types de certificats TLS ont été observés sur les serveurs de C2 : le certificat **Cobalt Strike** par défaut de SHA-1 « `6ece5ece4192683d2d84e25b0ba7e04f9cb7eb7c` » et des certificats délivrés par Let's Encrypt.

Les serveurs C2 sont majoritairement hébergés chez HostWinds et LeaseWeb aux États-Unis.

2.2 Investigation relative aux implants QakBot utilisés

Les implants **QakBot** [11] impliqués dans les incidents rapportés à l'ANSSI ainsi que dans ceux décrits par le rapport de l'éditeur Intrinsec [5], suivent la convention de nommage suivante : « `md.*` ».

Suite à l'observation de cette convention, des pivots sur des plateforme d'analyse de codes ont permis d'identifier des implants **QakBot** nommés « `md.exe` » et « `md.dll` », ainsi que d'autres partageant le même paramètre de configuration "botnet". Les configurations des implants ont ensuite été extraites :

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		

Les implants trouvés dans les incidents traités par l'ANSSI dont la configuration a pu être extraite sont tous liés au même affilié de **QakBot**, repéré via la racine du champ "botnet" de la configuration : « `domain` ». Tous les implants supplémentaires nommés « `md.exe` » et « `md.dll` », trouvés *via* pivots, sont liés eux aussi à l'affilié **QakBot** « `domain` », ce qui confirme l'efficacité de la méthode de recherche à partir de la convention de nommage observée.

Incident	Hash	Nom	botnet	campagne
Gefco	5ed9fb5fc74c6fdb3537629e9b23437a	md.exe	domain01	1597161528
Fareva	04416cf8bf1c7d31a606edff765529df	md.dll	domain02	1606721866

Cependant, à plusieurs reprises, des implants **Cobalt Strike** communiquant avec le *cluster* Akamai/Azure ont été déposés, non pas par l'affilié **QakBot** « `domain` » mais par l'affilié **QakBot** « `Obama` » :

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

Trois hypothèses peuvent expliquer cette observation :

- l'ID « `Obama` » est lié à l'ID « `domain` » ;
- le *cluster* d'infrastructure **Cobalt Strike** Akamai/Azure est utilisée par plusieurs groupes d'attaquants, et donc potentiellement fourni par un tiers cybercriminel ;

11. Apparu en 2009, **QakBot** (alias **Qbot**, **Pinkslipbot**) est un cheval de Troie modulaire utilisé pour distribuer d'autres charges utiles, en particulier de type rançongiciel. En 2020, **QakBot** a distribué les rançongiciels **ProLock**, **Egregor** et **DoppelPaymer**. En 2021, au vu de l'incident chez Pierre Fabre, il apparaît que **QakBot** puisse également distribuer **Sodinokibi**. **QakBot** fonctionne selon un modèle d'affiliés [7].

- l'infrastructure **Cobalt Strike** Akamai/Azure est directement fournie à certains de ses affiliés par Mallard Spider (alias Gold Lagoon), le groupe cybercriminel ayant développé et mettant à disposition **QakBot**.

*Commentaire : L'ANSSI ne peut pas tirer de conclusions pour le moment. Néanmoins, **QakBot** a distribué des implants **Cobalt Strike** utilisant des serveurs C2 ne faisant pas partie du cluster Akamai/Azure, à de nombreuses reprises [12, 13]. Ainsi, cette troisième hypothèse peut raisonnablement être mise de côté.*

2.3 Investigation relative à l'utilisation de l'outil d'exfiltration Rclone

Dans cinq incidents, l'exécutable **Rclone**, ainsi que son fichier de configuration, portaient le même nom, usurpant le service Windows « `svchost` ».

Incident	Rclone	Noms des fichiers
Société A		
Intrinsec – ProLock	■	(svchost.exe)
Gefco	■	svchost.exe svchost.conf
Ouest-France	■	svchost.exe svchost.conf
Fareva		
Société B		
Pierre Fabre	■	svchost.exe
The DFIR Report – Sodinokibi	■	svchost.exe svchost.conf

L'incident **ProLock** décrit par l'éditeur Intrinsec est un peu particulier : en effet, il n'y a pas de référence directe à « `svchost.exe` », ni aux serveurs utilisés pour l'exfiltration. Cependant, Group-IB indique que dans les incidents **ProLock**, l'exécutable **Rclone** était toujours renommé afin de ressembler aux binaires légitimes du système [14]. Il est donc envisageable que celui-ci soit là aussi nommé « `svchost.exe` ».

L'utilisation de **Rclone** et les noms de ses fichiers ne sont pas les seuls points communs entre les différents incidents étant donné qu'il existe également des similarités sur les infrastructures d'exfiltration utilisées :

- Les serveurs d'exfiltration FTP observés dans les incidents Gefco et Ouest-France présentaient des certificats TLS autosignés similaires (valeur « `Kanzas City` » utilisée dans le *subject*), en plus d'avoir une version de **vsFTPd** identique.
- Les serveurs d'exfiltrations WebDAV observés dans l'incident traité par The DFIR Report [6] ainsi que dans les incidents Gefco et Ouest-France, présentaient les mêmes bannières HTTP, notamment l'authentification basique nommée « `realm_name` ». Cela ne semble pas correspondre à une configuration par défaut connue. De plus, dans le cas de The DFIR Report et de Gefco, les serveurs HTTP exposaient tous les deux un certificat auto-signé généré avec **OpenSSL**.

Des pivots réalisés à partir de ces éléments de configuration ont permis d'identifier d'autres serveurs d'exfiltration potentiellement utilisés par le même groupe d'attaquants :

Source	Serveur d'exfiltration (FTP/WebDAV)	Date de première vue	Date de dernière vue
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

Le schéma suivant résume ces liens techniques :

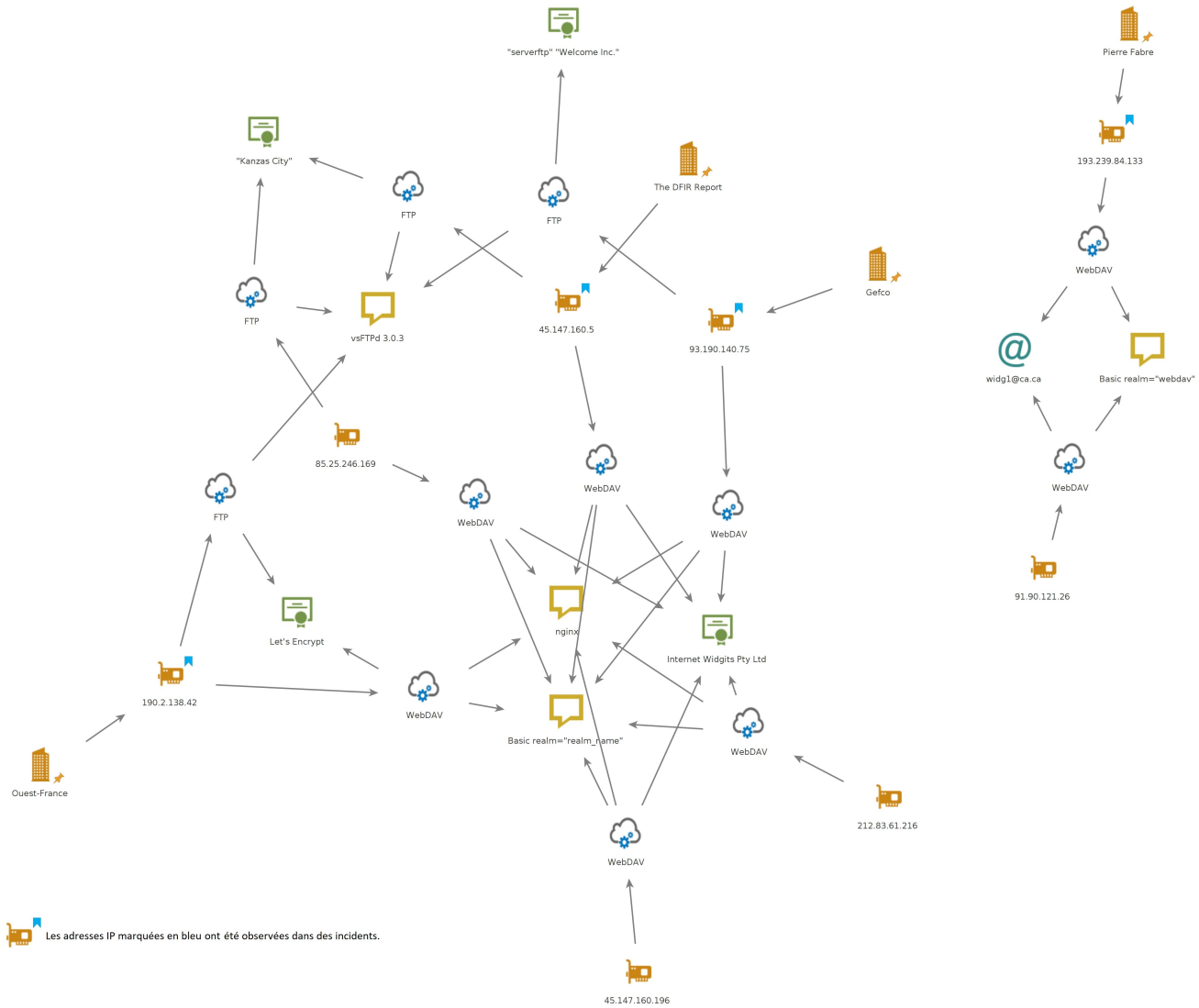

Fig. 2.2 – Synthèse des liens entre les serveurs d'exfiltration.

2.4 Conclusion à l'issue des investigations

D'après les investigations de l'ANSSI, il existe bien un groupe cybercriminel responsable des attaques à l'encontre de Gefco, Société A, Société B, Pierre Fabre, Ouest France, Fareva ainsi que de celles rapportées par les éditeurs Intrinsec et The DFIR Report.

Ce groupe est caractérisé par les principales TTPs suivantes :

- l'utilisation de **Cobalt Strike** ;
- l'utilisation d'une convention de nommage des serveurs C2 **Cobalt Strike** usurpant des noms de domaine Akamai et Azure ;
- l'emploi fréquent du terme « `technology` » et de ses dérivés dans ses noms de domaines ;
- l'achat de noms de domaine chez NameCheap ;
- l'utilisation de TLD exotiques ;
- l'emploi du certificat TLS par défaut de **Cobalt Strike** et de certificats Let's Encrypt ;
- l'hébergement de ses serveurs C2 chez HostWinds et LeaseWeb ;
- l'utilisation de **QakBot** en tant que première charge utile ;
- l'application de la convention de nommage "md" aux implants **QakBot** ;
- son rattachement à l'affilié « `domain` » de **Qakbot**, actif depuis juin 2020 ;
- l'utilisation de l'outil d'exfiltration **Rclone** ;
- l'application de convention de nommage "svchost" à l'exécutable **Rclone** ;
- l'exfiltration *via* FTP et WebDAV.

Il sera désormais dénommé "Lockean", d'après le nom d'utilisateur WebDAV employé pour l'exfiltration des données dans l'incident **Egregor** chez Ouest France.

3 Chaîne d'infection associée à Lockean

3.1 Vecteur d'infection

3.1.1 Courriels d'hameçonnage distribués par un service de distribution

Au vu des incidents dans lesquels il est impliqué, Lockean aurait utilisé le service de distribution **Emotet** en 2020 [2, 5] ainsi que celui de TA551 en 2020 et 2021 [15, 16, 7, 17, 18] dans le but de distribuer **QakBot** par courriel d'hameçonnage :

- Lors de l'attaque par le rançongiciel **Egregor** chez Ouest-France [2], la première charge utile aurait en effet été le code malveillant **Emotet** [12]. **Emotet** ayant été généralement distribué par courriel d'hameçonnage, *via* les botnets Epoch opérés par ses développeurs TA542 [20], il est probable que ce vecteur d'infection ait initié la compromission de Ouest-France. L'implication du service de distribution d'**Emotet** est confirmée par le rapport de l'éditeur Intrinsec [5] dans lequel est décrite une chaîne d'infection se rapportant à Lockean et l'ayant là aussi impliqué en amont, bien que son issue n'ait pas été de distribuer le rançongiciel **Egregor**, comme chez Ouest-France, mais de distribuer le rançongiciel **ProLock**.
- Alors que TA542 semble avoir cessé ses activités suite au démantèlement d'**Emotet** début 2021, un autre service de distribution, alors moins réputé, paraît avoir été privilégié par le groupe cybercriminel Lockean [6]. Ce service de distribution est celui de TA551 (alias Shathak, UNC2420, Gold Cabin) [13].

Néanmoins, Lockean ne serait pas l'unique affilié **QakBot** à recourir à ces services de distribution [7, 26]. Ainsi, actuellement, toute infection par TA551 visant à distribuer **QakBot** ne suffit pas à présumer une compromission par Lockean.

3.1.2 Loaders intermédiaires

Dans les incidents que l'ANSSI lie au groupe cybercriminel Lockean, l'accès initial aux SI a été réalisé à l'aide du *loader* **QakBot**, à l'exception de l'incident décrit par The DFIR report, lors duquel le *loader* **IcedID** a été distribué comme première charge utile [14].

Le fait que seulement une heure environ ait séparé la distribution d'**IcedID** de celle de **Cobalt Strike** lors de l'incident analysé par The DFIR Report [6] permet de supposer la présence d'un seul attaquant, utilisateur commun au *loader* et au rançongiciel (dans ce cas, **Sodinokibi**), et non de la présence de deux attaquants.

Lockean ne serait néanmoins pas le seul affilié commun de **QakBot** et d'**IcedID** [7].

3.2 Latéralisation

Lors de la phase de latéralisation des différents incidents, quatre outils ont été observés : **Cobalt Strike**, **Adfind**, **BloodHound** et **BITSadmin**. Une utilisation fréquente de **Cobalt Strike**, d'**Adfind** et de **BITSadmin** a été observée tandis que **BloodHound** semble moins utilisé.

12. Ce dernier, opéré par le groupe cybercriminel TA542, a été, de 2017 jusqu'à son démantèlement en janvier 2021 [19], un *loader* de codes malveillants pour le compte de clients.
13. Actif depuis 2018, il consiste à distribuer des codes malveillants pour le compte de clients par l'intermédiaire de campagnes massives de courriels d'hameçonnage [21, 17, 22, 15, 23, 24]. Ces courriels sont caractérisés par le fait qu'ils répondent souvent à des fils de discussion légitimes (*email thread hijacking*), qu'ils contiennent généralement une pièce-jointe au format Zip, parfois protégée par un mot de passe indiqué dans le courriel, que ce fichier Zip contient un fichier Word ou Excel piégé, que ce fichier Word ou Excel utilise un *template* DocuSign généré par l'outil **Ettersilent** [25, 16].
14. Dans le cadre de l'incident traité par The DFIR Report [6], **IcedID** semble avoir été distribué par **EtterSilent** [27], ce qui pourrait confirmer que Lockean ait eu là aussi recours aux services de TA551 pour distribuer **IcedID** (bien que TA551 ne soit pas le seul groupe cybercriminel à utiliser l'outil **Ettersilent**).

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

À noter que l'absence d'observation d'un outil ne signifie pas qu'il n'a pas été utilisé.

3.3 Exfiltration

En amont du chiffrement, Lockean exfiltre les données de ses victimes grâce à l'outil **Rclone** qu'il renomme en usurpant le nom du service Windows "svchost".

3.4 Chiffrement

Des investigations de l'ANSSI ont permis d'identifier plusieurs rançongiciels (de type RaaS) auxquels Lockean a été affilié.

3.4.1 Maze, Egregor et ProLock

Au cours des deux incidents **Egregor** chez Gefco [1] et Ouest-France [2] imputés à Lockean par l'ANSSI, l'adresse IP « `185.238.0.233` » a été utilisée par les attaquants afin de distribuer des scripts, ainsi que des souches de rançongiciels.

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

D'après les éditeurs Intrinsec [5] et Cybereason [28], cette adresse IP a également été observée dans un incident **ProLock**, où elle a distribué les fichiers « `connect.bat` » et « `office.txt` » [5].

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

Des souches du rançongiciel **Maze** [15] ont également été distribuées depuis cette adresse IP :

15. Maze est un RaaS apparu en mai 2019 et disparu en août 2020. Il est en particulier connu pour avoir introduit le principe de double extorsion en septembre 2019, autrement dit d'exfiltration des données des victimes et de menace de divulgation sur un site en .onion en cas de non-paiement de la rançon. **Egregor** est réputé être le RaaS successeur de **Maze** [29].

URL	Condensat 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

Ainsi, Lockean a été affilié des trois RaaS Maze, Egregor et ProLock.

3.4.2 DoppelPaymer

Lockean pourrait également avoir été affilié de **DoppelPaymer** pour les raisons suivantes :

- des souches du rançongiciel **DoppelPaymer** ont également été distribuées depuis l'adresse IP susnommée, d'après une plateforme d'analyse de code :

URL	Condensat 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

  À noter que dans l'incident **DoppelPaymer** chez Fareva, la souche du rançongiciel était nommée « `k166sm.exe` ». Ce nom correspond à la convention de nommage utilisée pour les souches **DoppelPaymer** hébergées sur l'adresse IP « `185.238.0.233` ». Ainsi, il est possible que celle-ci ait été impliquée dans l'incident chez Fareva sans que cela ne puisse être confirmé, faute d'informations suffisantes au sujet de cet incident pour lequel l'ANSSI n'est pas intervenue ;
- des C2 **Cobalt Strike** typosquattant Akamai (« `atakai-technologies.host` », « `akamai-technologies.site` » et « `akamai-technologies.space` ») ont été retrouvés lors d'incidents ayant abouti au chiffrement par **DoppelPaymer** [30, 31], complétant ainsi les observations de l'ANSSI concernant les incidents **DoppelPaymer** chez la société A et Fareva ;
- **DoppelPaymer** a déjà été distribué par **QakBot** (qu'il ait été ou non distribué en amont par **Emotet**) [32] ;
- le renommage de **QakBot** en « `md.exe` », propre à l'affilié « `domain` » et donc à Lockean, a été retrouvé lors de l'incident **DoppelPaymer** chez la société A en juin 2020.

3.4.3 Sodinokibi

Le 31 mars 2021, l'ANSSI a été alertée du chiffrement de l'entreprise Pierre Fabre. Au cours de cette attaque, l'affilié « `domain02` » de **QakBot** a distribué **Cobalt Strike** (l'un des C2 typosquattant Akamai), **Rclone** (fichier renommé « `svchost.exe` ») ainsi que le rançongiciel **Sodinokibi**. Sur la base de liens d'infrastructure et de TTPs communes, l'ANSSI a déduit que Lockean était à l'origine de la compromission du SI de Pierre Fabre mais également de la chaîne d'infection décrite par The DFIR Report [6].

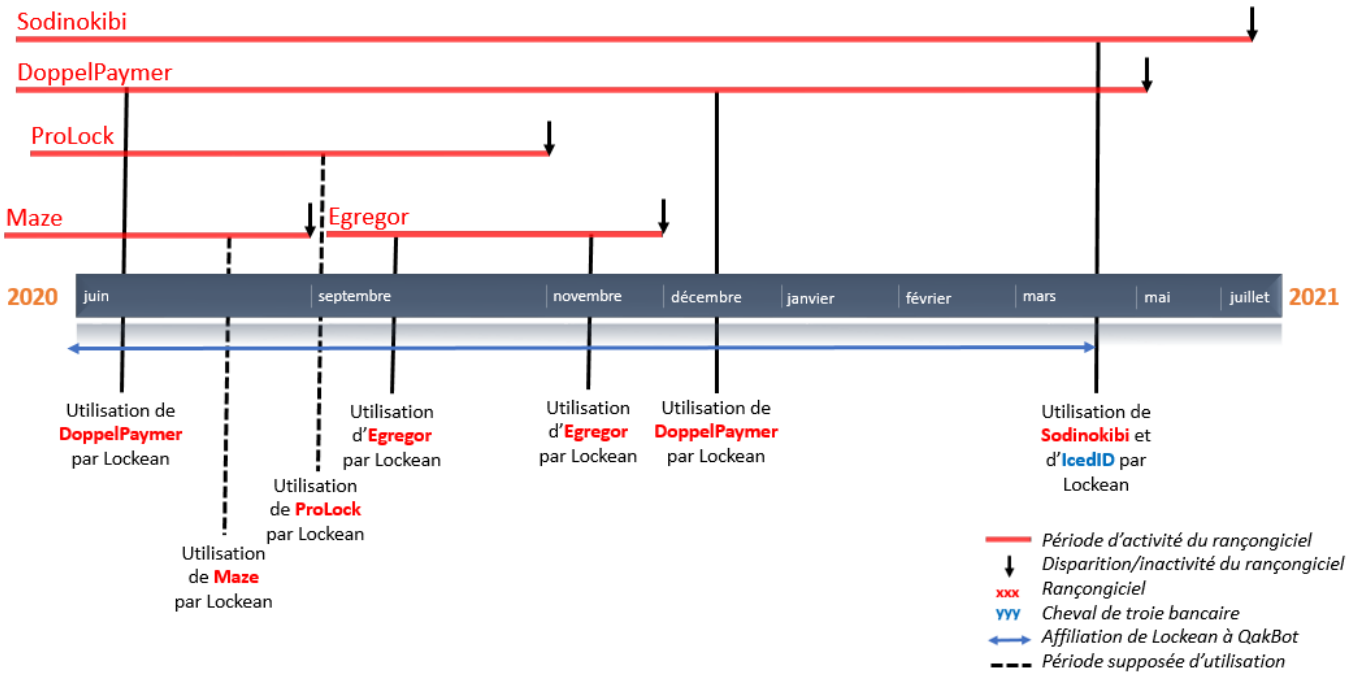

Fig. 3.1 – Activité connue de Lockean comparée à la période d'activité des rançongiciels

Lockean aurait utilisé :

- **DoppelPaymer** : depuis au moins juin 2020 ;
- **Egregor** : depuis son apparition en septembre 2020 [1]. Par déduction, le fait que Lockean puisse avoir utilisé Maze et qu'Egregor ait pris la suite de Maze en septembre 2020 après son arrêt laisse penser que Lockean a transféré son affiliation de Maze à Egregor comme voulu par les développeurs de Maze [29]. Néanmoins, il n'est pas connu de l'ANSSI depuis quand Lockean utilisait **Maze** ;
- **Sodinokibi** : depuis au moins mars 2021 [4, 6] ;
- **ProLock** : la période d'utilisation de ce rançongiciel par Lockean n'est pas identifiée bien qu'elle puisse avoir été concomitante à celle d'**Egregor** [5].

*Commentaire : L'arrêt définitif de **Maze** aux alentours de novembre 2020 et le démantèlement d'**Egregor** en février 2021 pourrait avoir poussé Lockean à se tourner vers le concurrent direct de **Maze** qu'est **Sodinokibi**. L'inactivité de **Sodinokibi** du 13 juillet 2021 jusqu'à début septembre pourrait avoir poussé Lockean à le substituer momentanément par un autre RaaS. De plus, le RaaS **Grief**[16] ayant supposément pris la suite de **DoppelPaymer** [33], il est possible que Lockean utilise **Grief** à l'avenir.*

3.5 Principe de double extorsion

L'exfiltration constante de données de la victime en amont du chiffrement et l'existence de sites de divulgation associés aux RaaS auxquels Lockean est affilié (à l'exception de **ProLock**) confirment que ce groupe cybercriminel est adepte du principe de double extorsion, autrement dit qu'il exfiltre des données de ses victimes en les menaçant de les divulguer, dans le but qu'elles payent la rançon, après chiffrement.

Si la rançon est payée, Lockean n'en conservera en moyenne que 70%, le restant étant destiné aux développeurs des RaaS [34].

16. Apparu fin mai 2021, **Grief** (alias Pay, Deuil ransomware) est supposé être le successeur de DoppelPaymer et donc être opéré par les mêmes attaquants. Il n'y a en effet plus de publications de victimes sur le site de divulgation associé à **DoppelPaymer** depuis début mai 2021 et le premier échantillon de **Grief** découvert pointait vers ce dernier [33].

3.6 Récapitulatif de la chaîne d'infection

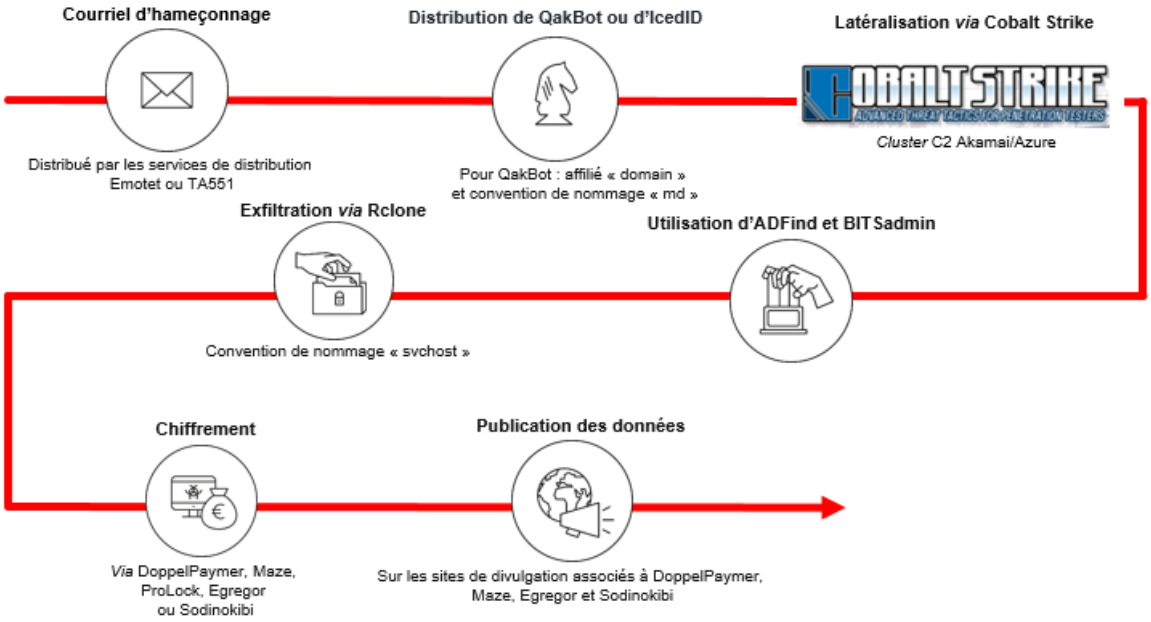

Fig. 3.2 – Chaîne d'infection récapitulative associée au groupe cybercriminel Lockean

4 Conclusion

Le ciblage de Lockean est opportuniste et dépendant des services de distribution qu'il emploie (**Emotet**, TA551).

Néanmoins, Lockean a une propension à cibler des entités françaises dans une logique de *Big Game Hunting*[17] [1, 4, 2], et représente de ce fait une menace à surveiller.

Commentaire : Il est intéressant de souligner que, malgré le fait qu'il soit affilié à des rançongiciels qui excluent le ciblage d'entités localisées dans les pays de la Communauté des Etats Indépendants (CEI), Lockean a attaqué la société de transport française Gefco en 2020 alors que Gefco appartient à 75% aux chemins de fer russes. Ainsi, il est possible que le groupe Lockean n'ait pas eu conscience de contrevenir aux "règles d'engagement" - largement respectées - des rançongiciels qu'il utilise.

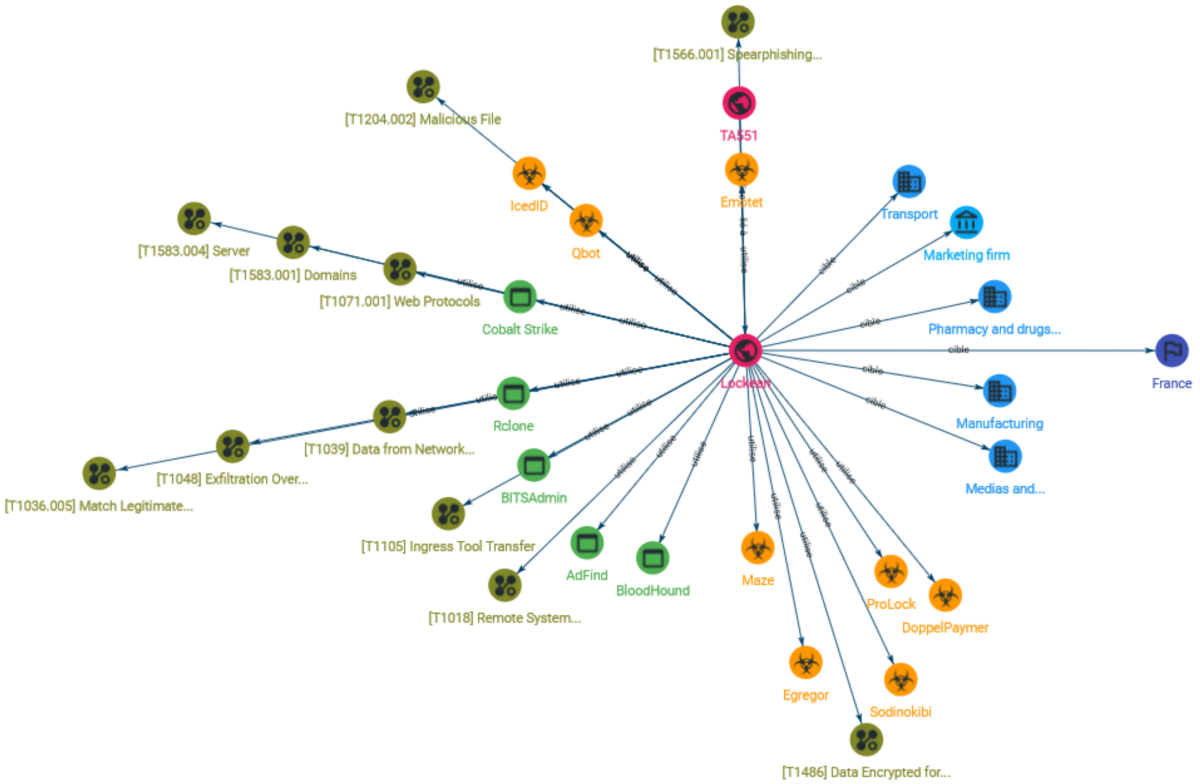

Fig. 4.1 – Illustration OpenCTI du groupe d'attaquants Lockean

17. Le *Big Game Hunting* consiste, pour des groupes cybercriminels possédant des ressources financières et des compétences techniques importantes, à favoriser le ciblage d'entreprises et institutions particulières dans leurs attaques par rançongiciel. Ce ciblage se caractérise notamment par une préparation des opérations d'extorsion en amont, parfois plusieurs mois à l'avance.

5 Annexe

5.1 Synthèse des liens entre les incidents reliés au groupe Lockean

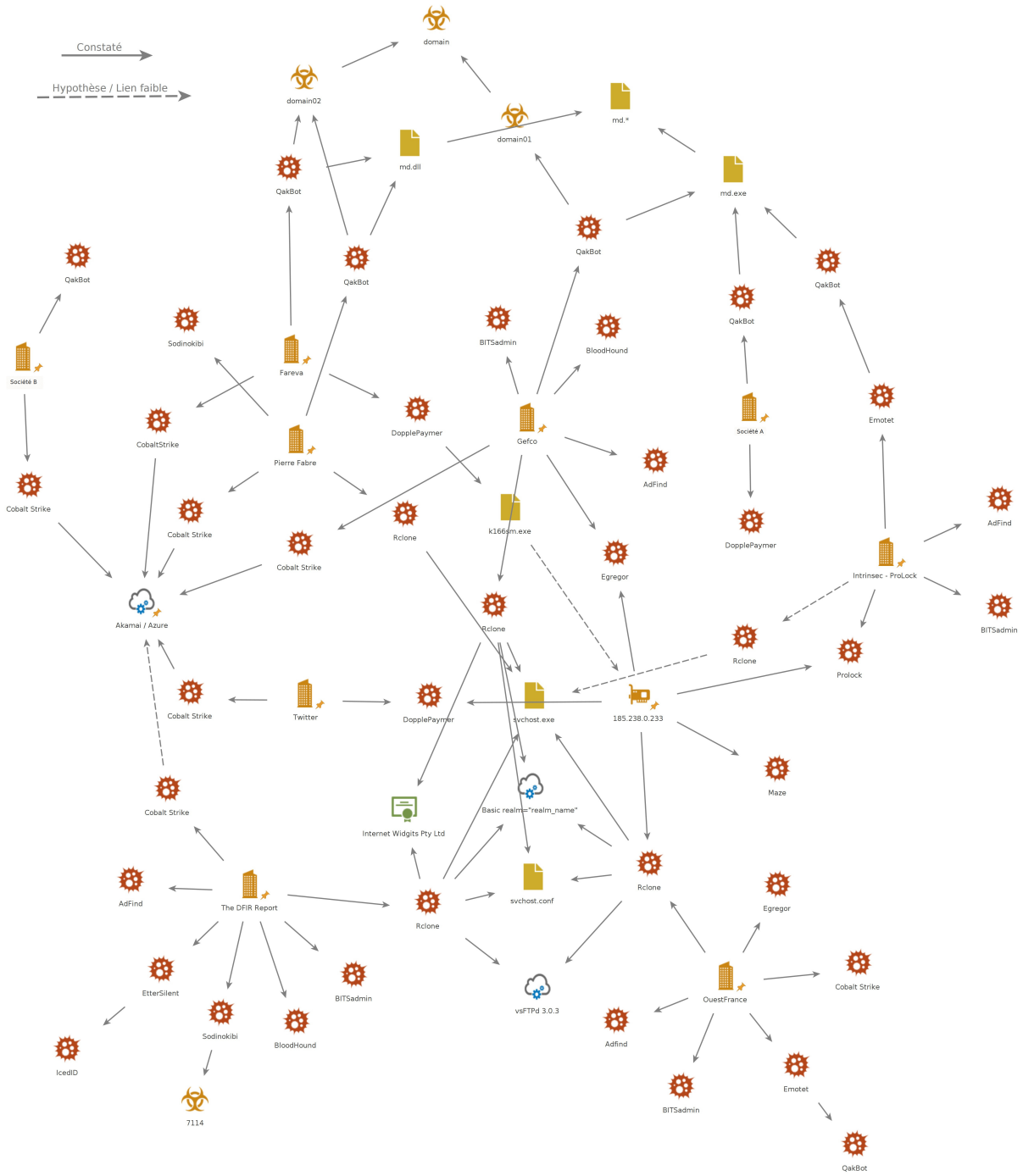

Fig. 5.1 – Synthèse des liens entre les incidents reliés au groupe Lockean

5.2 Tableau des TTPs d'après le référentiel MITRE ATT&CK

Identifiant	Nom	Commentaires
T1583.001	Acquire Infrastructure: Domains	Utilisation du registraire Namecheap et convention de nommage Akamai / Azure
T1583.004	Acquire Infrastructure: Server	Les serveurs C2 CobaltStrike sont majoritairement hébergés chez HostWinds et LeaseWeb
T1566.001	Phishing: Spearphishing Attachment	Courriels d'hameçonnage distribués par Emotet ou TA551
T1204.002	User Execution: Malicious File	Emotet QakBot ou IcedID
T1036.005	Masquerading - Match Legitimate Name or Location	Renommage de Rclone en svchost
T1018	Remote System Discovery	Utilisation d'adfind et de BloodHound
T1039	Data from Network Shared Drive	Collecte des données à exfiltrer
T1071.001	Application Layer Protocol: Web Protocols	Communications en HTTPS avec les serveurs C2 CobaltStrike
T1105	Ingress Tool Transfer	Utilisation de BITSadmin
T1048	Exfiltration Over Alternative Protocol	Exfiltration des données via le protocole FTP ou WebDAV à l'aide de l'outil Rclone
T1486	Data Encrypted for Impact	Chiffrement du système d'informations par DopplePaymer Maze Prolock Egregor ou Sodinokibi

5.3 Indicateurs de compromission

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

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

93.190.140.75	Serveur d'exfiltration [2020-09-23:2020-12-20]
190.2.138.42	Serveur d'exfiltration [2020-11-19:2021-01-04]
193.239.84.133	Serveur d'exfiltration [2021-04-03:2021-04-10]
212.83.61.216	Serveur d'exfiltration [2021-05-05:2021-06-01]
91.90.121.26	Serveur d'exfiltration [2021-04-24:2021-06-07]
45.147.160.196	Serveur d'exfiltration [2021-02-06:2021-07-03]
45.147.160.5	Serveur d'exfiltration [2021-03-11:2021-07-31]
85.25.246.169	Serveur d'exfiltration [2021-02-21:2021-08-16]
185.238.0.233	Serveur de distribution de scripts et de rançongiciels [2020-07-20:2021-01-09]

6 Bibliographie

[1] GEFCO. *Message de Luc Nadal : Point à date sur la reprise de GEFCO après une cyber-attaque*. 28 septembre 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*. 2 février 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*. 5 janvier 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*. 3 mai 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 ?* 12 novembre 2020.
URL : https://www.intrinsec.com/egregor-prolock/.

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

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

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

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

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

[11] Twitter. *@Unit42_Intel*. 11 mai 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 testsubnet[.]com*. 22 mai 2021.
URL : https://twitter.com/malware_traffic/status/1395894771898531845.

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

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

[15] SANS Internet Storm Center. *TA551 (Shathak) Word Docs Push Qakbot (Qbot)*. 26 janvier 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*. 13 avril 2021.
URL : https://www.bleepingcomputer.com/news/security/qbot-malware-is-back-replacing-icedid-in-malspam-campaigns/.

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

[18] AT&T Cybersecurity - AlienLabs. *The Rise of QakBot*. 15 avril 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*. 27 janvier 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*. 27 octobre 2020.

[21] Bitdefender. *New TA551 Campaign Uses IceID, Complex Attack Chain to Compromise*. 1er janvier 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)*. 1er août 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*. 7 janvier 2021.
URL : https://unit42.paloaltonetworks.com/ta551-shathak-icedid/.

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

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

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

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

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

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

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

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

[32] Mandiant. *The Evolving Maturity in Ransomware Operations*. 1er décembre 2020.

[33] Zscaler. *DoppelPaymer Continues to Cause Grief Through Rebranding*. 28 juillet 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*. 1er février 2021.
URL : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-001.pdf.

Version 1.0 - 25 octobre 2021

Licence ouverte (Étalab - v2.0)

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