TLP:WHITE

# LE GROUPE CYBERCRIMINEL FIN7

Version 1.0

27 avril 2022


TLP:WHITE

# Sommaire

# 1 Synthèse

FIN7 est, avec Cobalt Gang, l'un des successeurs présumés du groupe cybercriminel Carbanak, actif de 2013 à 2015 et spécialisé dans les attaques à visée lucrative à l'encontre de systèmes d'information bancaires.

Structuré à la manière d'une entreprise et composé de membres russophones, FIN7 dissimule une partie de ses activités derrière des sociétés écrans : Combi Security, IPC puis plus récemment Bastion Secure. C'est notamment par leur biais que FIN7 recrute des experts informatiques non avertis des activités malveillantes auxquelles ils participent.

Réputé sophistiqué, le groupe use d'un arsenal et de TTPs variés pour extraire des données de cartes bancaires depuis des systèmes de terminaux de point de vente ainsi que d'autres types de données sensibles à des fins de revente ou d'utilisation ultérieure. Ses victimes sont sectoriellement et géographiquement variées avec une prédominance pour les secteurs de la restauration, de la vente et de l'hôtellerie aux États-Unis, au Royaume-Uni, en Australie et en France.

Cette activité traditionnelle de vol d'informations étant devenue moins lucrative au gré des années, et compte tenu de la généralisation de la tendance des rançongiciels, FIN7 fait évoluer son activité à partir d'avril 2020 en réalisant des attaques par rançongiciel de type *Big Game Hunting*.

Affilié reconnu de Sodinokibi, FIN7 introduit son propre rançongiciel, Darkside, en juillet 2020. Ce dernier devient un *ransomware-as-a-service* (RaaS) à partir d'octobre et attire l'attention des autorités américaines en mai 2021 à la suite de l'attaque de l'un de ses affiliés contre l'entreprise Colonial Pipeline, rendant les conséquences de cette attaque par rançongiciel inédites. À Darkside succède le RaaS BlackMatter, qui disparaît à son tour en novembre 2021.

Néanmoins, FIN7 reste un groupe cybercriminel capable de se réinventer, de perdurer dans l'écosystème cybercriminel russophone et de demeurer une menace pour la France.

# 2 Le groupe cybercriminel Carbanak, prédecesseur de FIN7

## 2.1 Attaques imputées à Carbanak

### 2.1.1 Attaques à visée lucrative

Actif de janvier 2013 [1] à courant 2015, le groupe cybercriminel Carbanak était spécialisé dans le ciblage de systèmes d'information (SI) de banques, notamment russes, et de systèmes de paiement, leur dérobant plus de 45 millions de dollars [1, 2]. Le groupe réalisait des virements frauduleux depuis le système de messagerie interbancaire Swift et compromettait le système de gestion des distributeurs automatiques de billets (DAB) de la marque Wincor en y insérant des scripts malveillants visant à modifier leurs commandes. Ainsi, si une mule venait à demander le retrait de dix billets de 100 roubles, le distributeur de la banque compromise émettait dix billets d'un montant supérieur, par exemple de 5000 roubles [1].

En 2014, il aurait également ciblé des systèmes de terminaux de point de vente (TPV) utilisés au sein d'hôtels et de restaurants aux États-Unis et en Europe [1].

### 2.1.2 Attaques à visée d'espionnage

D'après Group-IB, Carbanak aurait également mené des attaques à des fins d'espionnage industriel dans le but supposé de réaliser des délits d'initié. Il pourrait également avoir attaqué des agences gouvernementales à des fins d'espionnage [1].

## 2.2 Arsenal

Début 2013, avant que le code malveillant Carbanak (*alias* Anunak, Sekur) ne soit développé, le groupe cybercriminel aurait souscrit à des *Malware-as-a-Service*, tels qu'Andromeda (*alias* Gamarue) [1] et Pony [2] [1], et les aurait distribués par point d'eau *via* le kit d'exploitation Neutrino [3]. Il aurait également utilisé le code malveillant Qadars [4] [4].

D'après Group-IB, Carbanak aurait souscrit à des services de botnets (tels que GoZ [5], Shiz et Ranbyus) et leur aurait notamment acheté des informations sur les adresses IP des systèmes infectés par ces derniers. L'objectif était d'y repérer des entités financières et gouvernementales d'intérêt et de demander à y distribuer l'un de ses codes malveillants [1].

Début février 2014, le groupe cybercriminel a commencé à utiliser la porte dérobée Carbanak (*alias* Sekur) [6]. Ce code malveillant est une variante de la porte dérobée Anunak, elle-même variante du cheval de Troie Carbep [6] [4].

Au vu de son ciblage ponctuel de systèmes de TPV, il apparaît que Carbanak disposait également de codes malveillants de type POS (pour *Point-of-Sale*) [1].

1. Code malveillant et contrôleur de botnet démantelé en 2017.
2. Code malveillant et contrôleur de botnet actif depuis 2011, spécialisé dans le vol de codes d'accès et de crypto-actifs ainsi que dans la distribution de codes malveillants. Sa version 1.9 a fuité fin 2012.
3. Kit d'exploitation apparu en 2013, promu sur des forums souterrains russophones, devenu le kit d'exploitation le plus utilisé à partir de l'été 2016 et réputé inactif depuis la mi-2017 [3].
4. Cheval de Troie bancaire basé sur les codes sources de ZeuS et de Carbep.
5. En septembre 2011, une variante du MaaS ZeuS, Murofet (*alias* Licat), émerge : elle a été utilisée par le Business Club et deviendra leur outil phare, bientôt appelé GameOverZeuS (GoZ), et succédant à JabberZeuS. Le groupe cybercriminel a construit *via* GoZ une structure de botnets fonctionnant en *peer-to-peer* (P2P). Cette structure comprenait 27 botnets, dont chaque C2 *backends* était contrôlé par une personne ou un groupe différent, opérant à côté d'autres codes malveillants [5].
6. Carbep est un cheval de Troie bancaire apparu en 2010. Le chef du groupe opérant Carbep ainsi qu'une vingtaine de ses membres ont été arrêtés en avril 2013. Le code source de Carbep a ensuite été vendu sur le *Dark Web* pour 50000 dollars [7].

## 2.3 Composition du groupe

D'après Group-IB, Carbanak était composé d'individus russes et ukrainiens et collaborait avec des groupes implantés en Russie, en Ukraine mais aussi en Biélorussie [1] et en Chine [2].

En 2015, après l'arrestation d'une cinquantaine de ses membres [2], le groupe Carbanak se serait fragmenté en plusieurs petits groupes [4], parmi lesquels FIN7 et Cobalt Gang (voir annexe 5.1).

# 3 L'héritage de Carbanak : FIN7

## 3.1 Distinction entre Carbanak et FIN7

FIN7[7] est un groupe cybercriminel qui, pour certains éditeurs, serait confondu avec Carbanak, mais qui, pour d'autres, en serait distinct. Les premiers ancrent donc les prémices d'activité de FIN7 entre 2013 et 2014 contre 2015-2016 pour les seconds.

Ces derniers, comme FireEye, partent du postulat que la porte dérobée Carbanak n'est pas utilisée par un seul groupe et qu'une filiation basée uniquement sur l'emploi de ce code malveillant est caduque [8, 6].

Parmi les éditeurs qui identifient Carbanak et FIN7 comme deux modes opératoires liés, Crowdstrike les regroupe au sein de l'appellation Carbon Spider.

## 3.2 Organisation de FIN7

### 3.2.1 Composition du groupe

Selon le Département de la Justice américain [9, 10], en 2018, FIN7 était composé de plusieurs douzaines de membres et fonctionnait à la manière d'une entreprise avec des équipes aux compétences variées rendant des comptes à une hiérarchie.

Quatre de ces membres, ukrainiens, ont été arrêtés entre 2018 et 2020 :

- Fedir Hhadyr, l'un des chefs supposés de FIN7 et administrateur système, âgé d'une trentaine d'années, arrêté à Dresden en Allemagne et condamné à dix ans de prison [11, 12, 10];
- Dmytro Fedorov, superviseur d'un groupe de spécialistes en tests d'intrusion, arrêté à Bielsko-Biala en Pologne [9, 10] ;
- Andrii Kolpakov, lui aussi superviseur d'un groupe de spécialistes en tests d'intrusion, arrêté à Lepe en Espagne et condamné à sept ans de prison [13] ;
- Denis Iarmak, spécialiste en test d'intrusion, pour sa part arrêté à Seattle aux États-Unis[10].

**Malgré ces arrestations, le FBI a jugé FIN7 encore extrêmement actif en 2020 [14].**

### 3.2.2 Fonctionnement du groupe

#### Moyens de communication

À l'époque de ces arrestations, les membres de FIN7 communiquaient *via* un serveur Jabber[8], utilisaient un serveur HipChat[9] pour faire passer des entretiens aux potentielles recrues et partager les données de cartes bancaires exfiltrées aux victimes, des échantillons de codes malveillants ou encore des captures d'écran des SI compromis.

En outre, ils coordonnaient leurs intrusions par l'intermédiaire de JIRA, un logiciel de gestion de projet hébergé sur des serveurs privés virtuels dans différents pays [10, 11].

#### Sociétés écran

Depuis 2015, une partie des activités de FIN7 apparaît dissimulée derrière des sociétés écrans [15].

7. *alias* Navigator, TelePort Crew, Calcium, Carbon Spider, Blue Gulon, Gold Niagara, ATK 32, APT-C-11, ITG14, TAG-CR1, TA3546.
8. Jabber est un système de messagerie instantanée libre dont les serveurs sont décentralisés à travers le monde.
9. Programme de messagerie instantanée et de transferts de fichiers.

Combi Security

Combi Security est une fausse société de sécurité informatique créée par FIN7 et active de 2015 à 2018. Elle disposait d'un site Internet d'apparence légitime, sur lequel était indiqué qu'elle était implantée à Moscou (Russie), à Haifa (Israël) et à Odessa (Ukraine), et postait des offres de poste sur des sites de recrutement russes, ukrainiens et ouzbèkes populaires. Le but était de recruter des spécialistes en intrusion à bas coût [10] et qui n'avaient pas conscience de pénétrer le SI d'entreprises à leur insu, convaincus de la légalité de l'activité de Combi Security. D'après le département de la Justice américain, de nombreuses victimes américaines de FIN7 comptaient parmi les faux clients listés sur le site de Combi Security [8, 9].

En 2021, le russe Maxim Zhukov a été condamné à une courte peine pour avoir travaillé comme développeur Ruby pour Combi Security [15].

FIN7 aurait par la suite utilisé la société-écran IPC d'une manière similaire à Combi Security [16].

Bastion Secure

En octobre 2021, des chercheurs de l'éditeur en sécurité informatique Gemini ont découvert une nouvelle société écran qu'ils attribuent à FIN7 : Bastion Secure. Là encore, Bastion Secure dispose d'un site Internet d'apparence légitime, copiant le site de la véritable entreprise Convergent Network Solutions Ltd. Son nom de domaine est hébergé chez le registraire Beget, souvent utilisé par des cybercriminels. Enfin, plusieurs onglets du site renvoient une erreur 404 en russe laissant penser que ses concepteurs sont russophones [17].

Bastion Secure cherche à recruter des programmeurs, des administrateurs systèmes ainsi que des ingénieurs en *reverse* de code. Le salaire proposé, adapté aux critères des pays de l'ex-URSS, oscille entre 800 et 1200 dollars par mois. Le premier entretien de recrutement se déroule par message sur Telegram. À l'issue du processus de recrutement, des outils d'intrusion sont fournis au candidat, parmi lesquels deux outils de post-exploitation qui, après analyse, s'avèrent être les codes malveillants Carbanak et Lizar (*alias* Tirion), spécifiques à l'arsenal de FIN7 [17].

## 3.3 Mode opératoire traditionnel

### 3.3.1 Reconnaissance

FIN7 aurait par le passé publié de fausses offres d'emploi sur des sites de recrutement réputés afin de récupérer des informations sur des entreprises.

La phase de reconnaissance permet aux attaquants de FIN7 d'adapter leurs courriels d'hameçonnage aux cibles en plagiant la construction des courriels de l'entreprise ou de l'une de ses parties prenantes [18] mais également d'usurper leurs domaines légitimes [19]. Cela a par exemple été le cas lors de la campagne de FIN7 usurpant l'image de la Security Exchange Commission (SEC) américaine et l'adresse *e-mail* associée à son système de transfert de fichiers [20].

Les employés destinataires de ces courriels sont choisis pour leur poste, généralement en *front office* (gestionnaire de réservation par exemple) ou managers [18]. Ainsi, les courriels ont traité à de nombreuses reprises de plaintes, de demandes de menus spécifiques aux intolérances alimentaires ou de commandes, sujets d'intérêt pour les entités des secteurs ciblés (hôtellerie, restauration, vente).

### 3.3.2 Vecteurs d'infection

Le vecteur d'infection principalement employé par FIN7 est le courriel d'hameçonnage. Il contient une pièce jointe malveillante [8] et plus rarement une URL pointant vers des sites compromis ou des services légitimes tels que Google Docs [8]. Les destinataires sont parfois appelés au téléphone par les attaquants et incités à cliquer sur la pièce jointe malveillante et à activer les macros [8].

10. Le recrutement de cybercriminels a pu être estimé plus coûteux que celui de spécialistes en intrusion.

Depuis 2020, FIN7 utilise également un vecteur d'infection plus original : les clés USB piégées envoyées par courrier postal *via* les services postaux américains à des employés en ressources humaines, en informatique ou en management dans les secteurs de l'hôtellerie et de la vente [21, 22]. Ces clés USB, achetées sur Internet sous l'appellation « BadUSB », sont envoyées accompagnées d'une fausse carte cadeau BestBuy et sont modifiées de sorte à agir comme des claviers sur des systèmes d'exploitation Windows ou MacOS et à permettre aux attaquants de lancer des commandes Powershell.

### 3.3.3 Outils et techniques de post compromission

D'après une étude publiée par l'entreprise RSA, certains des codes malveillants de FIN7 sont basés sur des codes malveillants utilisés par plusieurs membres de l'écosystème cybercriminel mais suffisamment personnalisés pour les rendre spécifiques à FIN7 [4]. Le groupe FIN7 utilise également des outils légitimes de tests d'intrusion, des outils Windows ainsi que des MaaS.

De plus, plusieurs de ses codes ont des modules d'enregistrement vidéo permettant aux attaquants de mieux gérer les différentes étapes de leur intrusion en observant la manière de faire des employés espionnés [8].

#### Intrusion et exploitation

| Nom | Type | Période d'utilisation | Commentaires | Sources |
|---|---|---|---|---|
| Harpy (Griffon) | Code malveillant | Depuis mai 2018 | Porte dérobée Javascript. | [23] |
| Bateleur | Code malveillant | Depuis juillet 2017 | Porte dérobée modulaire. | [8, 24] |
| Agent ORM | Code malveillant | 2015-2016 | Implant de reconnaissance | [6] |
| Halbaked | Code malveillant | - | Dropper VBS Script ou Javacript. | [6] |
| VBS flash implant | Code malveillant | 2015-2017 | Outil de reconnaissance. | [25] |
| JS flash implant | Code malveillant | 2017 | Outil de reconnaissance. | [25] |
| ADFind | Outil légitime | - | Cartographie de l'AD. | [4] |
| ADRecon | Outil légitime | - | Cartographie de l'AD. | [4] |
| Boostwrite | Code malveillant | Depuis octobre 2019 | Loader. | [26] |
| Domenus VBS/JS | Code malveillant | Depuis mars 2020 | Loader. | [25] |
| Birddog | Code malveillant | Depuis septembre 2017 | Porte dérobée. | [8] |
| Dridex | Malware-as-a-Service | 2016-2018 | Pour distribuer Carbanak. | [27, 28] |
| JSS loader | Code malveillant | 2021 | Réputé utilisé par plusieurs groupes d'attaquants. | [29] |
| Powersource | Code malveillant | - | Version modifiée de l'outil public DNS_TXT_Pwnage. | [30] |

*Commentaire : si FIN7 a effectivement utilisé Dridex à plusieurs reprises en tant que première charge utile, le groupe aurait donc été client d'Evil Corp [5], qui opère le botnet Dridex.*

#### Élévation de privilèges

| Nom | Type | Commentaires | Sources |
|---|---|---|---|
| Carbanak | Code malveillant | *Via* son module sekurlsa (copie de Mimikatz). | [31] |
| Mimikatz | Outil légitime | - | [6] |
| WCE | Outil légitime | - | [6] |
| Cobalt Strike | Outil légitime | - | [6] |
| Metasploit | Outil légitime | - | [6] |
| Powersploit | Outil légitime | - | [32] |
| SessionGopher | Outil légitime | - | [25] |
| CrackMapExec | Outil légitime | - | [29] |

| Nom | Type | Commentaires | Sources |
|---|---|---|---|
| [T1190] CVE-2017-5638 (Apache Struts) | Technique | Élévation de privilèges sur un système d'exploitation Linux. | [33] |
| [T1210] CVE-2020-1472 (ZeroLogon) | Technique | - | [29] |

## Persistance et latéralisation

| Nom | Type | Commentaires | Sources |
|---|---|---|---|
| Carbanak | Code malveillant | Porte dérobée modulaire utilisé depuis 2016. | [8, 31] |
| Bellhop | Code malveillant | Porte dérobée Javacript. | [6] |
| Babymetal | Code malveillant | Outil en ligne de commande basé sur TinyMet. | [6] |
| Lizar (Tirion) | Code malveillant | Outil d'exfiltration utilisé depuis juillet 2020 pouvant être distribué via des clés USB piégées. | [32, 34] |
| KillACK | Code malveillant | Porte dérobée Poweshell utilisée depuis juin 2020. | [25] |
| [T1546.011] Application shimming | Technique | Persistance dans l'environnement contenant les données de cartes bancaires. | [20] |
| PsExec | Outil légitime | Pivot vers l'environnement contenant les données de cartes bancaires. | [4] |
| Cobalt Strike | Outil légitime | Peut être exécuté par Powershell ou bcnHEX. | [35] |
| PAExec | Outil légitime | Latéralisation. | [4, 6] |
| Metasploit | Outil légitime | - | [6] |
| Textmate | Code malveillant | Distribué par Powersource. S'exécute en mémoire via Powershell. | [30] |
| sqlRAT | Code malveillant | Exécution de scripts SQL. | [29] |

## Obfuscation

FIN7 emploie plusieurs techniques d'assombrissement parmi lesquelles :

- la dissimulation du caractère malveillant des codes sous une apparence légitime : par exemple, Bi-zone a observé la version 3.7.4 de la porte dérobée Carbanak être référencée comme Check Point Software Technology dans son interface [32];
- la signature numérique des documents piégés et des codes malveillants utilisés [8];
- l'obfuscation de charge utile sur la base de l'interpréteur de commandes Windows cmd.exe : cette technique a été dénommée FINcoding par FireEye car elle a été développée par FIN7 [8];

## Exfiltration et communication vers le C2

| Technique | Code malveillant | Source |
|---|---|---|
| [T1041] Communication C2 *via* HTTP | Par exemple Bellhop et Carbanak peuvent communiquer via HTTP. | [27, 8] |
| [T1041] Communication C2 *via* HTTPS | Par exemple Domenus VBS peut communiquer via HTTPS. | [29] |
| [T1041] Adresses IP codées en dur | Par exemple dans des échantillons de code de Carbanak. | [27, 8] |
| [T1041] Outil d'exfiltration | Lizar est un outil d'exfiltration de données. | [32, 34] |
| [T1048] DNS tunnelling | Par exemple *via* Cobalt Strike beacon. | [29] |
| [T1567] Exfiltration vers des services légitimes | Par exemple Google Docs/Scripts ou encore Pastebin. | [29] |
| [T1567] Utilisation du client MEGASync | Exfiltration de fichiers via MEGASync. | [29] |

### 3.3.4 Action sur l'objectif

#### Extraction de données de cartes bancaires

Le principal état final recherché de FIN7 est de localiser les systèmes de terminaux de point de vente (TPV ou POS) au sein des SI de ses victimes et d'en extraire les données de cartes bancaires. Depuis 2015, FIN7 a dérobé plus de 20 millions de données de cartes bancaires aux États-Unis depuis plus de 6500 terminaux de point de vente [18, 13].

Ces données sont ensuite revendues sur des places de marché souterraines [18, 8], notamment sur Joker's Stash [20] dont l'activité a cessé en février 2021 [36] ou sont utilisées pour réaliser des transactions frauduleuses. Par exemple, en mars 2017, les données de cartes bancaires dérobées à une entreprise victime et associées à des comptes d'une banque à Washington ont été utilisées pour réaliser des achats frauduleux chez un commerçant de la ville de Puyallup aux Etats-Unis [10].

D'après une hypothèse de Malwarebytes, FIN7 présenterait des liens avec le groupe Magecart numéro 5 [11], signifiant que le groupe pourrait éventuellement dérober des données de cartes bancaires depuis des sites marchands [27, 37].

Enfin, il est possible que FIN7 puisse chercher, au moins depuis octobre 2019, à récupérer des données de cartes bancaires depuis des DAB ou même à réaliser des retraits frauduleux. En effet, FIN7 utilise le code malveillant Boostwrite, qui est chargé notamment de manipuler le logiciel de gestion à distance du fabricant de DAB NCR [26].

#### Vol de données sensibles

D'après plusieurs sources, FIN7 serait impliqué dans le vol de données sensibles (propriété intellectuelle, informations non publiques, listes de clients) que le groupe vendrait là aussi sur des places de marché souterraines ou utiliserait [38, 18, 14] pour tirer un avantage compétitif sur les marchés de capitaux. Par exemple, en avril 2017, FireEye a mis en lumière une campagne d'hameçonnage de FIN7 usurpant l'image de la Security Exchange Commission (SEC) américaine ayant ciblé des employés de plusieurs centaines d'entreprises chargés de soumettre les documents réglementaires d'information financières à la SEC [8, 10]. Au cours de la chaîne d'infection, le code malveillant Powersource a distribué les charges utiles Textmate et Cobalt Strike Beacon [20].

Outre des campagnes d'hameçonnage ciblé sur des employés manipulant des informations sensibles non-publiques concernant leur entreprise, FIN7 a déjà été observé se latéralisant au sein des départements financiers de ses victimes à la recherche d'autre type d'information, quand il lui était impossible d'extraire des données de cartes bancaires.

*Une matrice Mitre ATT&CK récapitulant les TTPs traditionnelles de FIN7 est disponible en annexe 5.2.*

### 3.3.5 Victimologie

En matière sectorielle, FIN7 cible principalement les secteurs de la restauration, de la vente et de l'hôtellerie, et dans une moindre mesure le secteur gouvernemental, des jeux d'argent, de l'énergie, de la finance, de la technologie, des voyages, de l'éducation, de la construction et des télécommunications [8]. En janvier 2022, le FBI a annoncé que FIN7 ciblait les secteurs de la défense, de l'assurance et du transport depuis août 2021 au travers de la campagne BadUSB [39], ce qui s'éloigne fortement de sa victimologie habituelle.

La victimologie de FIN7 se trouve notamment aux Etats-Unis, au Royaume-Uni, en Australie et en France [18, 13].

11. Les groupes menant des opérations à l'encontre de sites marchands à des fins d'altération de leur contenu et d'exfiltration des données de cartes bancaires des clients sont numérotés de 1 à 7.

## 3.4 Evolution vers les rançongiciels

### 3.4.1 Contexte

L'adoption progressive de la technologie EMV [12] aux États-Unis a rendu l'activité traditionnelle de FIN7 de ciblage de terminaux de point de vente bien moins lucrative qu'auparavant. Cette perte de rentabilité, en plus de la généralisation de la tendance des rançongiciels à l'écosystème cybercriminel russophone originel, pourrait être à l'origine de l'évolution de FIN7 vers les rançongiciels. C'est ainsi qu'à partir d'avril 2020 des attaques par rançongiciel sont venues s'ajouter aux attaques traditionnelles de FIN7. Il existe des nuances entre éditeurs sur le niveau d'implication directe de FIN7 dans le déploiement des rançongiciels [40].

Les attaques par rançongiciel conduites par FIN7 sont de type *Big Game Hunting* [13]. Ses cibles seraient choisies sur la base de leurs revenus depuis le service Zoominfo [32], et ne se limitent donc plus aux entités disposant de systèmes de TPV.

### 3.4.2 2020 : affiliation à des Ransomware-as-a-Service

#### Sodinokibi

Les premières observations de FIN7 distribuant un rançongiciel remontent à la mi-2020. Alors que des chercheurs d'IBM ont découvert la porte dérobée Carbanak dans un incident ayant abouti au chiffrement par le *Ransomware-as-a-Service* Sodinokibi [41], Crowdstrike a constaté en avril 2020 qu'une campagne d'hameçonnage de FIN7 visant à distribuer Domenus VBS puis Harpy, présentait des liens d'infrastructure avec plusieurs incidents par le rançongiciel Sodinokibi [25].

L'affiliation de FIN7 au RaaS Sodinokibi courant 2020 a par la suite été confirmée par l'éditeur au gré des incidents, puis plus récemment par les autorités américaines, selon lesquelles le rançongiciel Darkside, opéré par FIN7 à partir de l'été 2020, a été développé par des partenaires du groupe opérant Sodinokibi (Pinchy Spider) [42, 38, 39].

#### Potentiellement à Ryuk

À l'été 2020, l'éditeur Truesec a observé des TTPs de FIN7, dont l'utilisation de la porte dérobée Carbanak, lors d'un incident ayant abouti six semaines après la compromission initiale au chiffrement de la victime par le rançongiciel Ryuk [43]. Comme lors de l'incident Sodinokibi rapporté par IBM, Gemini Advisory avance que la porte dérobée Carbanak peut être utilisée par FIN7 au cours d'attaques par rançongiciel [17].

Ainsi, soit FIN7 a ouvert l'accès à un SI à des utilisateurs du rançongiciel Ryuk, soit FIN7 l'a utilisé pour son compte.

### 3.4.3 2020-2021 : opérateur de RaaS

#### Darkside

Apparu en juillet 2020, Darkside était un rançongiciel développé par FIN7 d'après Crowdstrike [25] et Microsoft [15], et de prime abord opéré uniquement pour son compte. D'après des chercheurs de Microsoft, le sous-groupe de FIN7 qu'il nomme Elbrus est le créateur et l'opérateur des RaaS Darkside et BlackMatter.

À partir d'octobre 2020, Darkside a été mis à la disposition d'affiliés selon le modèle du Ransomware-as-a-Service (RaaS) [44]. Un site de divulgation de données y était associé.

*Une matrice Mitre ATT&CK récapitulant les TTPs associées aux attaques aboutissant au déploiement de Darkside est disponible en annexe 5.3.*

12. Les terminaux traditionnels qui n'utilisent pas la technologie sécurisée EMV (Europay, Mastercard, Visa) enregistrent pour un temps les données de cartes bancaires dans leur mémoire, sans qu'elles soient chiffrées. De fait, il est possible pour un attaquant de récupérer ces données en compromettant la mémoire des systèmes de TPV.
13. Le *Big Game Hunting* est une tendance émergée fin 2018 consistant à cibler au cours d'attaques par rançongiciel plus sophistiquées que lors de campagnes massives des entités à haut rentabilité et/ou à la continuité d'activité critique afin d'assurer le paiement d'une rançon de montant conséquent.

Darkside a attiré l'attention des autorités américaines à la suite de l'attaque de l'un de ses affiliés contre Colonial Pipeline, une société gérant la livraison par oléoduc de 45% du carburant de la côte Est américaine [45, 44]. L'attaque ayant provoqué un arrêt massif des activités de Colonial Pipeline, l'Agence américaine de protection de l'environnement a dû générer un mécanisme de compensation d'urgence pour se substituer aux 8800 kilomètres de pipeline et la Federal Motor Carrier Safety Administration a déclaré une urgence régionale pour assurer l'approvisionnement en pétrole par le biais de l'exploitation de véhicules commerciaux.

Après avoir payé la rançon de 5 millions de dollars demandée par les attaquants, et avec l'aide du gouvernement fédéral, Colonial Pipeline a progressivement rétabli ses opérations et repris son activité normale une semaine après l'attaque.

En réaction, le président américain Joe Biden a déclaré que les États-Unis prévoyaient de poursuivre les attaquants qui en étaient à l'origine. Le lendemain de cette annonce, les opérateurs de DarkSide ont déclaré qu'ils avaient perdu le contrôle de leurs serveurs web et qu'une partie des fonds en crypto-monnaies obtenus grâce aux paiements de rançon avait été retirée de leur serveur de paiement et transférée vers un portefeuille inconnu. À ce titre, le ministère américain de la Justice a déclaré avoir saisi la majeure partie de la rançon versée par Colonial Pipeline. Néanmoins, comme il n'y a pas eu de confirmation officielle de l'implication des autorités américaines dans la perte de contrôle de l'infrastructure de DarkSide par ses opérateurs, cette annonce pourrait également être un "exit scam", c'est-à-dire un moyen pour les opérateurs de DarkSide de mettre fin à leurs activités.

*Commentaire : Un changement de nom (« rebranding ») ou l'utilisation d'un autre rançongiciel par les mêmes acteurs sont deux hypothèses jugées plausibles ou possibles.*

À la suite de la réponse américaine à l'attaque, certains forums de l'écosystème cybercriminel ("exploit", "XSS") ont décidé d'interdire les annonces faisant la promotion de RaaS tandis que certains opérateurs de RaaS ont annoncé qu'ils feraient devenir leurs RaaS privés, rendant les conséquences de l'attaque contre Colonial Pipeline sans précédent.

L'ANSSI a connaissance de la compromission d'une douzaine entités françaises de son périmètre par le rançongiciel Darkside entre décembre 2020 et mai 2021.

### BlackMatter

D'après McAfee [46], Microsoft [15], le FBI [39] et Chainalysis [47], à l'issue de la fin d'activité de Darkside, FIN7 a lancé le RaaS BlackMatter, qui présente plusieurs similarités avec Darskide.

*Une matrice Mitre ATT&CK récapitulant les TTPs associées aux attaques aboutissant au déploiement de BlackMatter est disponible en annexe 5.4.*

En septembre 2021, la France aurait été le cinquième pays le plus victime d'attaques par BlackMatter après les Etats-Unis, l'Autriche, l'Italie et le Canada [46]. Pourtant, l'ANSSI n'a eu connaissance que d'un incident BlackMatter à l'encontre d'une entité française en septembre 2021 .

Selon Recorded Future, FIN7 a cessé les activités de Blackmatter en novembre 2021, sous pression de la Russie [15].

### ALPHV

ALPHV (*alias* BlackCat et Noberus) est un RaaS actif depuis novembre 2021 et ayant la particularité d'être développé en RUST. D'après Recorded Future et S2W Lab Company, les opérateurs de ALPHV pourraient avoir été d'anciens membres ou d'anciens affiliés de Sodinokibi. D'après Palo Alto, ils pourraient également avoir eu des liens avec les RaaS Darkside, BlackMatter et LockBit du fait de similarités techniques entre ces rançongiciels et ALPHV [48]. Finalement, en date du 4 février 2022, sur la base du tweet d'un chercheur d'Emsisoft, le chercheur Bushido Token a confirmé que FIN7 était à l'origine d'ALPHV [49] alors qu'un membre supposé d'ALPHV affirmait lors d'une interview au média The Record que le groupe opérant ALPHV était composé d'anciens affiliés de RaaS, parmi lesquels BlackMatter, réfutant ainsi l'imputation de ALPHV à FIN7 [50].

*Commentaire : Bien que FIN7 ait par le passé fait évoluer son RaaS Darkside en BlackMatter et puisse avoir réitéré,*

*l'ANSSI ne dispose pas de suffisamment d'éléments pour confirmer que FIN7 opère ALPHV.*

# 4 Prospectives

Malgré plusieurs arrestations de ses membres et les répercussions sans précédent de l'attaque contre Colonial Pipeline, FIN7 demeure un groupe cybercriminel sophistiqué capable de se renouveler, de perdurer dans l'écosystème cybercriminel russophone et de demeurer une menace pour la France, au travers de ses diverses activités.

# 5 Annexes

## 5.1 Cobalt Gang

Apparu en 2016, Cobalt Gang serait issu de la fragmentation du groupe cybercriminel Carbanak. À l'inverse de FIN7, il est spécialisé, tout comme Carbanak, dans les attaques à l'encontre du secteur financier.

En mai 2018, deux mois après l'arrestation de Denis K, supposément ancien membre de Carbanak et administrateur de haut rang de Cobalt Gang, les activités de Cobalt Gang ont repris. Son périmètre de cibles s'est alors étendu de la Russie et de la Communauté des États indépendants (CEI) aux pays occidentaux [51].

L'activité de Cobalt Gang s'articule notamment autour :

- de retraits frauduleux à des distributeurs automatiques de billets. Par exemple, le groupe aurait dérobé par ce biais 25 millions de dollars à une banque européenne en 2017 ;
- de virements frauduleux depuis le système de paiement interbancaire Swift ;
- du ciblage d'établissements de monnaie électronique et d'entités développant des logiciels de passerelles de paiement.

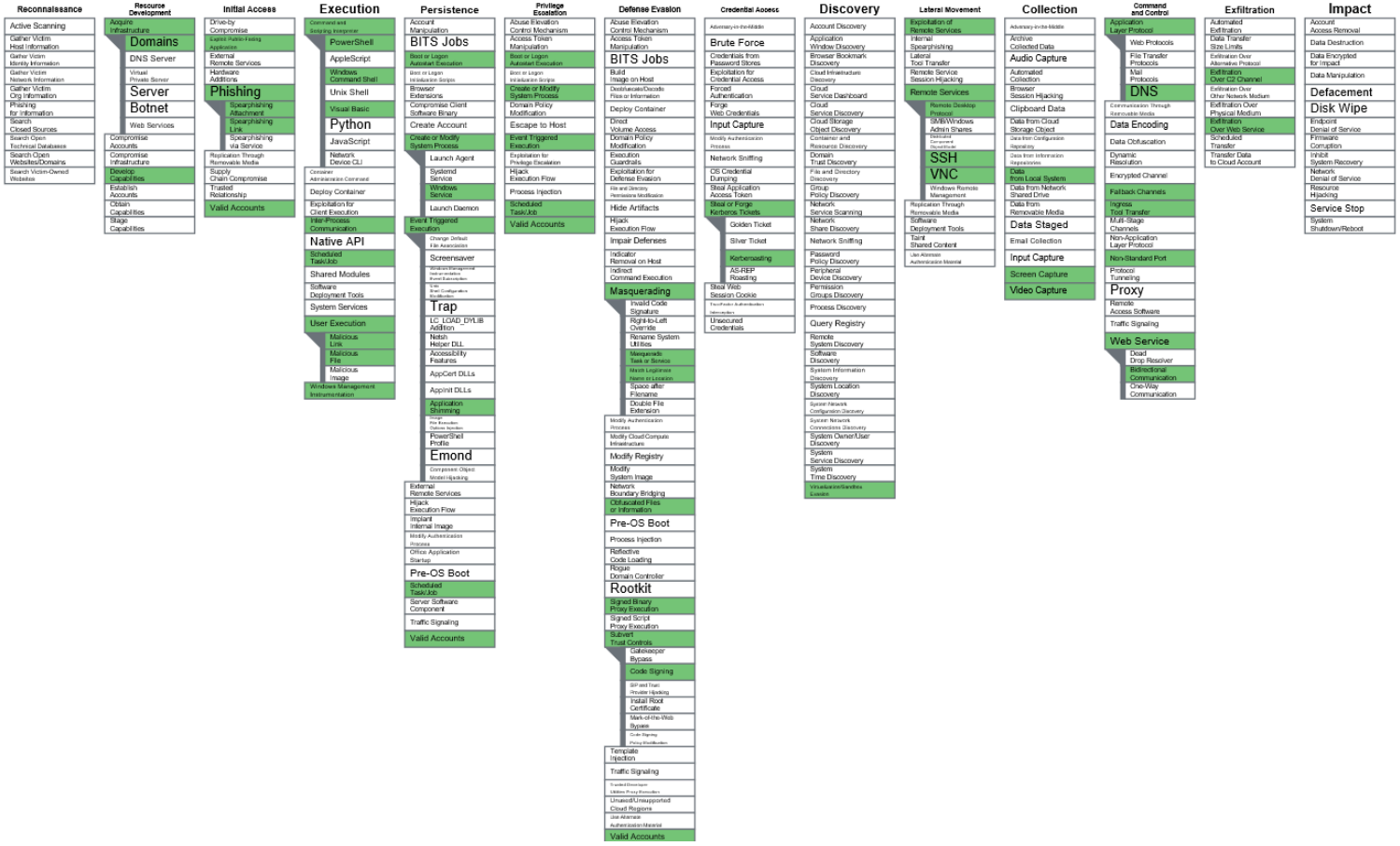
Le vecteur d'infection privilégié par Cobalt Gang est principalement le courriel d'hameçonnage, usurpant l'image d'entités du secteur financier. Un autre vecteur d'infection utilisé plus rarement serait les points d'eau, Cobalt Gang ayant déjà mis en place des sites Internet imitant par exemple celui de la Banque centrale européenne [52]. Enfin, le groupe cybercriminel a ponctuellement profité de l'accès au SI de prestataires de banques pour s'introduire par rebond au sein du leur.

L'arsenal de Cobalt Gang se compose de codes malveillants qui lui sont spécifiques (Kayslice, CobInt), de codes malveillants obtenus auprès du MaaS badbullzvenom (More_Eggs, Terra Loader), d'outils de tests d'intrusion (Cobalt Strike, AmmyAdmin, TeamViewer, Mimikatz, etc.) et d'au moins un rançongiciel (PetrWrap).

Ainsi, ses liens historiques avec Carbanak, son arsenal varié, sa maîtrise des techniques de vol d'argent et son ciblage d'institutions financières européennes faisaient de Cobalt Gang l'un des groupes d'attaquants spécialisés dans le ciblage de banques les plus sophistiqués et les plus menaçants à l'encontre du secteur bancaire français.

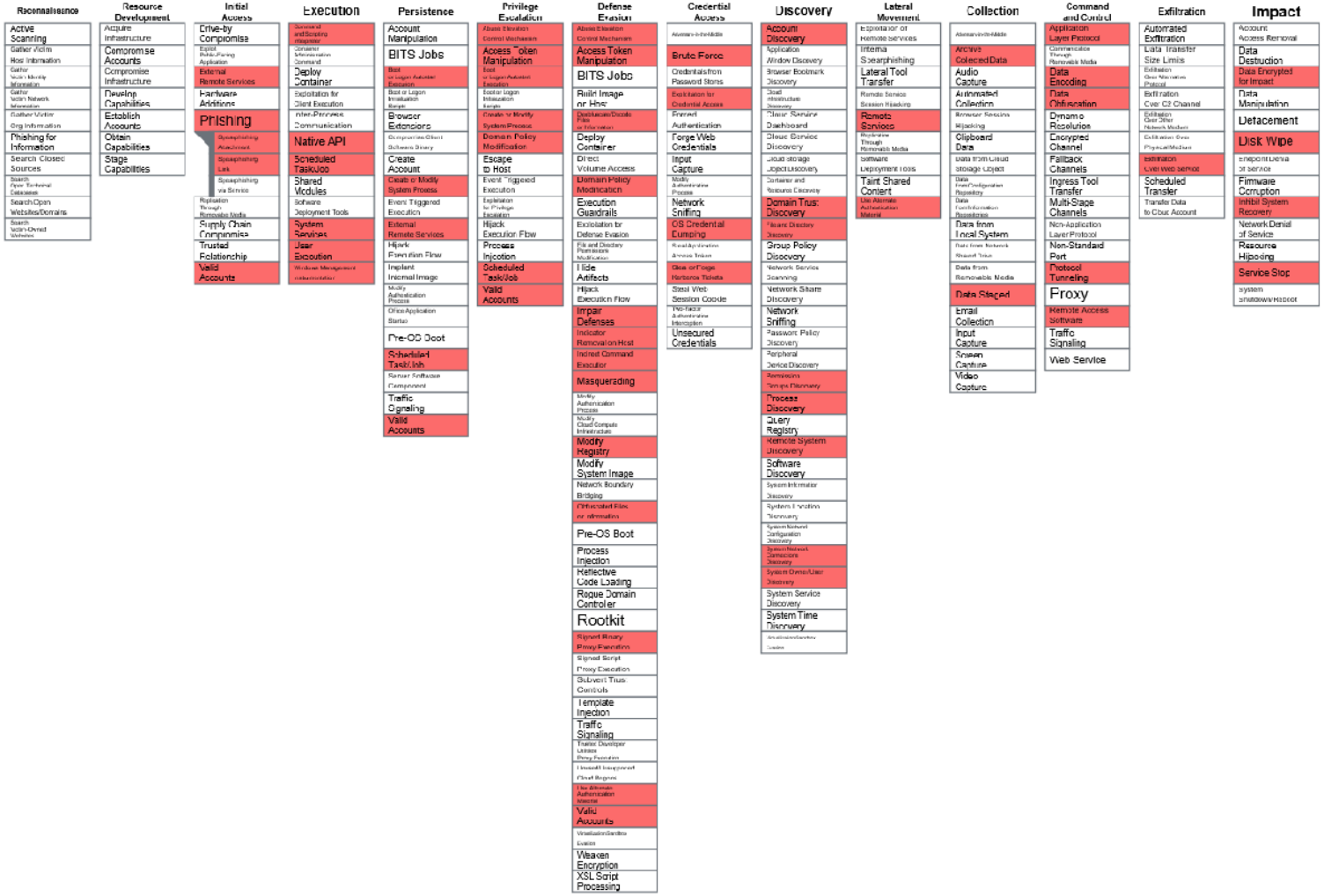
Néanmoins, depuis début 2020, très peu d'activité imputée à Cobalt Gang a été observée.

## 5.2 Matrice MITRE ATTACK récapitulative des TTPs traditionnelles de FIN7

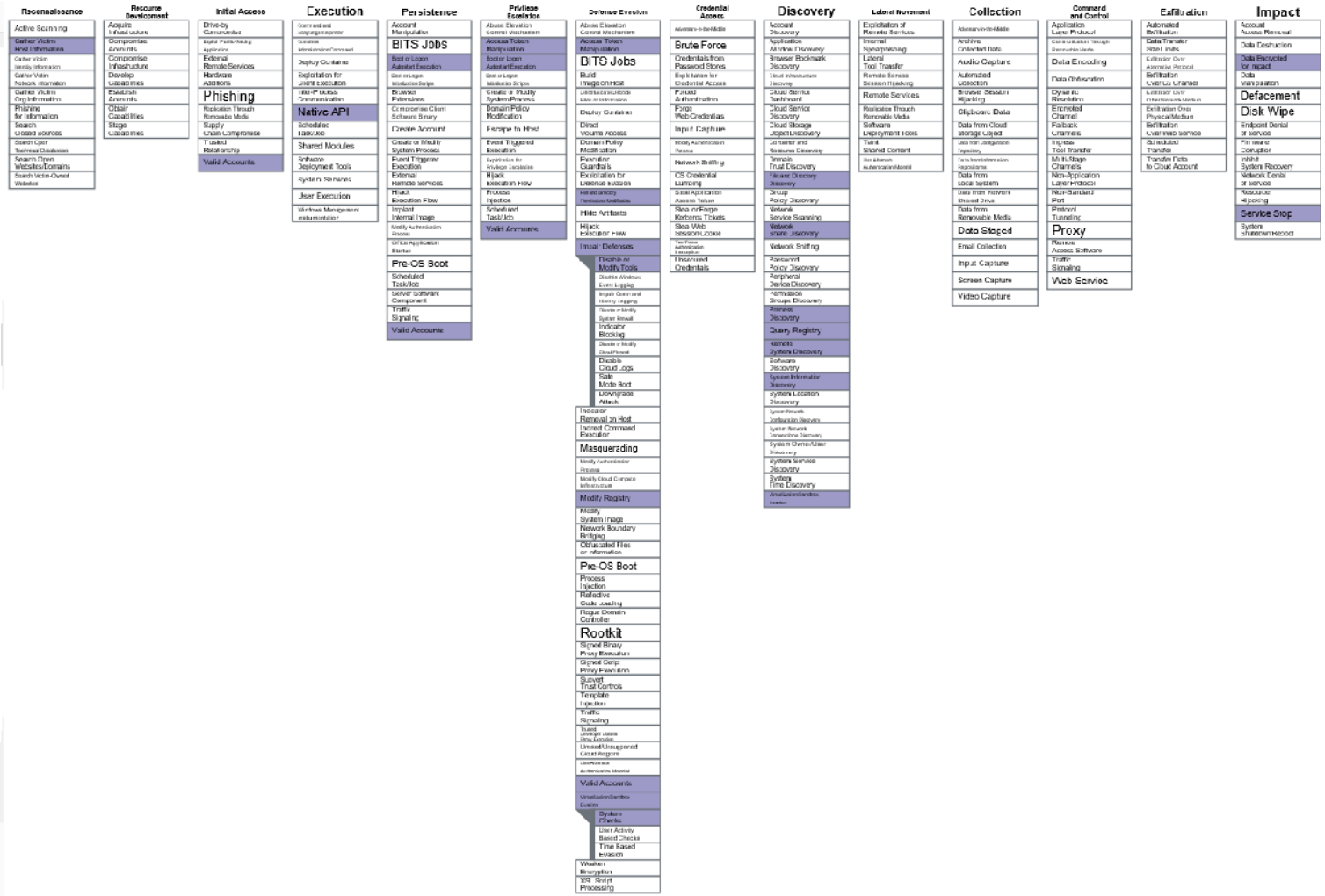



TLP:WHITE

## 5.3 Matrice MITRE ATTACK associée aux campagnes Darkside



## 5.4 Matrice MITRE ATTACK associée aux campagnes BlackMatter



# 6 Bibliographie

[1] Group-IB. *Anunak : APT against Financial Institutions*. 7 juin 2017.
URL : https://www.group-ib.com/resources/threat-research/Anunak_APT_against_financial_institutions.pdf.

[2] Bloomberg. *Russia Detains 50 Suspected Hackers for Malware Bank Attacks*. 1er juin 2016.
URL : https://www.bloomberg.com/news/articles/2016-06-01/russia-detains-50-suspected-hackers-for-malware-bank-attacks.

[3] *Former Major Player Neutrino Exploit Kit Has Gone Dark*. 14 juin 2017.
URL : https://www.bleepingcomputer.com/news/security/former-major-player-neutrino-exploit-kit-has-gone-dark/.

[4] RSA Conference. *The Carbanak/Fin7 Syndicate : A Historical Overview Of An Evolving Threat*. 22 novembre 2017.
URL : https://www.rsa.com/en-us/blog/2017-11/the-carbanak-fin7-syndicate.

[5] ANSSI. *Le Code Malveillant Dridex : Origines et Usages*. 28 mai 2020.
URL : https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-005/.

[6] FireEye. *The Magnificent FIN7, Revealing a Cybercriminal Threat Group*. 3 avril 2017.

[7] Silicon UK. *Carberp Malware Source Code Selling For $50k On Dark Web*. 19 juin 2013.
URL : https://www.silicon.co.uk/workspace/carberp-malware-source-code-50k-on-dark-web-119531.

[8] FireEye. *On the Hunt for FIN7 : Pursuing an Enigmatic and Evasive Global Criminal Operation « On the Hunt for FIN7 : Pursuing an Enigmatic and Evasive Global Criminal Operation*. 1er août 2018.
URL : https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html.

[9] Department of Justice. *Three Members of Notorious International Cybercrime Group "Fin7" in Custody for Role in Attacking Over 100 U.S. Companies*. 1er août 2018.
URL : https://www.justice.gov/usao-wdwa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over.

[10] United States District Court for the Western District of Washington at Seattle. *Iarmak Fin7 Indictment*. 26 mai 2020.
URL : https://www.documentcloud.org/documents/6928399-Iarmak-Fin7-Indictment.html.

[11] CyberScoop. *FIN7's IT Admin Pleads Guilty for Role in Billion-Dollar Cybercrime Crew*. 11 septembre 2019.
URL : https://www.cyberscoop.com/fin7-fedir-hladyr-guilty-carbanak/.

[12] CyberScoop. *FIN7 'technical Guru' Sentenced to 10 Years in Prison*. 16 avril 2021.
URL : https://www.cyberscoop.com/fedir-hladyr-fin7-sentencing-prison/.

[13] Heimdal Security. *Supervisor of FIN7 Hacking Group Was Sentenced to Seven Years in Prison*. 28 juin 2021.
URL : https://heimdalsecurity.com/blog/fin7-hacking-groups-supervisor-gets-7-years-in-jail/.

[14] CyberScoop. *Federal Officials Have Arrested Another Accused FIN7 Hacker*. 26 mai 2020.
URL : https://www.cyberscoop.com/fin7-hacking-arrest-financial/.

[15] The Record. *FIN7 Hacker Trialed in Russia Gets No Prison Time*. 1er décembre 2021.
URL : https://therecord.media/fin7-hacker-trialed-in-russia-gets-no-prison-time/.

[16] Secure List. *FIN7.5 : The Infamous Cybercrime Rig "FIN7" Continues Its Activities*. 8 mai 2019.
URL : https://securelist.com/fin7-5-the-infamous-cybercrime-rig-fin7-continues-its-activities/90703/.

[17] Gemini Advisory. *FIN7 Recruits Talent For Push Into Ransomware*. 21 octobre 2021.
URL : https://geminiadvisory.io/fin7-ransomware-bastion-secure/.

[18] US Federal Bureau of Investigation. *How Cyber Crime Group FIN7 Attacked and Stole Data from Hundreds of U.S. Companies*. 19 août 2021.
URL : https://www.fbi.gov/contact-us/field-offices/seattle/news/stories/how-cyber-crime-group-fin7-attacked-and-stole-data-from-hundreds-of-us-companies.

[19] THREAT STOP. *The "TelePort Crew" Evolves from Carbanak*. 24 janvier 2017.
URL : https://www.threatstop.com/blog/the-teleport-crew-evolves-from-carbanak.

[20] DIGITAL SHADOWS. *Mitre ATT&CK™ and the FIN7 Indictment : Lessons for Organizations*. 22 août 2018.
URL : https://www.digitalshadows.com/blog-and-research/mitre-attck-and-the-fin7-indictment-lessons-for-organizations/.

[21] THREAT INTEL. *OpBlueRaven : Unveiling Fin7/Carbanak - Part I : Tirion*. 31 juillet 2020.
URL : https://threatintel.blog/OPBlueRaven-Part1/.

[22] ZDNET. *Rare BadUSB Attack Detected in the Wild against US Hospitality Provider*. 26 mars 2020.
URL : https://www.zdnet.com/article/rare-badusb-attack-detected-in-the-wild-against-us-hospitality-provider/.

[23] CURATED INTEL. *Deobfuscating FIN7 JavaScript Implants*. 11 septembre 2021.
URL : https://www.curatedintel.org/2021/09/deobfuscating-fin7-javascript-implants.html.

[24] PROOFPOINT. *FIN7/Carbanak Threat Actor Unleashes Bateleur JScript Backdoor*. 31 juillet 2017.
URL : https://www.proofpoint.com/us/threat-insight/post/fin7carbanak-threat-actor-unleashes-bateleur-jscript-backdoor.

[25] CROWDSTRIKE. *CARBON SPIDER Embraces Big Game Hunting, Part 1*. 30 août 2021.
URL : https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/.

[26] MANDIANT. *Mahalo FIN7 : Responding to the Criminal Operators' New Tools and Techniques*. 10 octobre 2019.
URL : https://www.mandiant.com/resources/mahalo-fin7-responding-to-new-tools-and-techniques.

[27] MALWAREBYTES. *The Forgotten Domain : Exploring a Link between Magecart Group 5 and the Carbanak APT*. 22 octobre 2019.

[28] SWISS GOVERNMENT CERT. *The Rise of Dridex and the Role of ESPs*. 20 février 2017.
URL : https://www.govcert.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps.

[29] MITRE ATT&CK. *FIN7, GOLD NIAGARA, ITG14, Carbon Spider, Group G0046*. 16 décembre 2021.
URL : https://attack.mitre.org/groups/G0046/.

[30] FIREEYE. *ATT&CKing FIN7 - The Value of Using Frameworks for Threat Intelligence*. 1er octobre 2018.
URL : https://summit.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf.

[31] MANDIANT. *CARBANAK Week Part Two : Continuing the CARBANAK Source Code Analysis*. 6 mai 2019.
URL : https://www.mandiant.com/resources/carbanak-week-part-two-continuing-carbanak-source-code-analysis.

[32] BI.ZONE. *Cybercriminal Group FIN7 Disguises Its Malware as an Ethical Hacker's Toolkit*. 13 mai 2021.
URL : https://bi-zone.medium.com/from-pentest-to-apt-attack-cybercriminal-group-fin7-disguises-its-malware-as-an-ethical-hackers-c23c9a75e319.

[33] RSA. *Anatomy of an Attack : CARBANAK*. 25 août 2021.
URL : https://www.rsa.com/en-us/blog/2017-12/anatomy-of-an-attack-carbanak.

[34] THREAT INTEL. *OpBlueRaven : Unveiling Fin7/Carbanak - Part II : BadUSB Attacks*. 1er septembre 2020.
URL : https://threatintel.blog/OPBlueRaven-Part2/.

[35] PROOFPOINT. *Cobalt Strike : l'outil préféré des groupes APT comme des cybercriminels*. 29 juin 2021.
URL : https://www.proofpoint.com/fr/blog/threat-insight/cobalt-strike-favorite-tool-apt-crimeware.

[36] GEMINI ADVISORY. *Joker's Stash, the Largest Carding Marketplace, Shuts Down - Fraud Intelligence*. 15 janvier 2021.
URL : https://geminiadvisory.io/jokers-stash-shuts-down/.

[37] KREBS ON SECURITY. *Carbanak Gang Tied to Russian Security Firm ?* 18 juillet 2016.
URL : https://krebsonsecurity.com/2016/07/carbanak-gang-tied-to-russian-security-firm/.

[38] ANOMALI. *FIN7 Using Windows 11 Alpha-Themed Docs to Drop Javascript Backdoor*. 2 septembre 2021.
URL : https://www.anomali.com/blog/cybercrime-group-fin7-using-windows-11-alpha-themed-docs-to-drop-javascript-backdoor.

[39] THE RECORD. *FBI : FIN7 Hackers Target US Companies with BadUSB Devices to Install Ransomware*. 7 janvier 2022.
URL : https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install-ransomware/.

[40] FireEye. *FIN7 Power Hour : Adversary Archaeology and the Evolution of FIN7*. 4 avril 2022.
URL : https://www.mandiant.com/resources/evolution-of-fin7.

[41] ThreatRavens. *E-Commerce Skimming Is the New POS Malware*. 16 décembre 2020.
URL : https://threatravens.com/4daoevbqfde/.

[42] Reuters. *EXCLUSIVE Governments Turn Tables on Ransomware Gang REvil by Pushing It Offline*. 21 octobre 2021.
URL : https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/.

[43] Truesec. « Collaboration between FIN7 and the RYUK Group, a Truesec Investigation ». 22 décembre 2020.

[44] ANSSI et BSI - CERT Bund. *Fourth Edition of the Franco-German Common Situational Picture*. 1er novembre 2021.
URL : https://www.ssi.gouv.fr/uploads/2021/11/anssi_bsi_csp_2021.pdf.

[45] Wired. « DarkSide Ransomware Hit Colonial Pipeline—and Created an Unholy Mess ». 10 mai 2021.
URL : https://www.wired.com/story/darkside-ransomware-colonial-pipeline-response/.

[46] McAfee. *BlackMatter Ransomware Analysis ; The Dark Side Returns*. 22 septembre 2021.
URL : https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/blackmatter-ransomware-analysis-the-dark-side-returns/.

[47] Twitter. *@chainalysis*. 3 août 2021.
URL : https://twitter.com/chainalysis/status/1422541171608457221.

[48] Unit42. *Threat Assessment : BlackCat Ransomware*. 27 janvier 2022.
URL : https://unit42.paloaltonetworks.com/blackcat-ransomware/.

[49] Twitter. *@BushidoToken*. 4 février 2022.
URL : https://twitter.com/BushidoToken/status/1489652494007521286.

[50] Cisco Talos. *From BlackMatter to BlackCat : Analyzing Two Attacks from One Affiliate*. 17 mars 2022.
URL : http://blog.talosintelligence.com/2022/03/from-blackmatter-to-blackcat-analyzing.html.

[51] Group-IB. *Cobalt Renaissance : New Attacks and Joint Operations*. 29 mai 2018.
URL : https://blog.group-ib.com/renaissance.

[52] Bleeping Computer. *Cobalt Hacking Group Tests Banks In Russia and Romania*. 30 août 2018.
URL : https://www.bleepingcomputer.com/news/security/cobalt-hacking-group-tests-banks-in-russia-and-romania/.

Version 1.0 - 27 avril 2022



**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