TLP:WHITE

ÉTAT DE LA MENACE RANÇONGICIEL

À L'ENCONTRE DES ENTREPRISES ET DES INSTITUTIONS

4.3

2021-09-01

TLP:WHITE

1 Synthèse

La tendance à la hausse des attaques par rançongiciel à l'encontre d'organisations publiques et privées, identifiée depuis 2018, s'est à nouveau confirmée en 2020, tant à l'échelle internationale que nationale. En 2020, l'ANSSI note ainsi une augmentation de 255% des signalements d'attaque par rançongiciel dans son périmètre par rapport à 2019.

En outre, l'année 2020 s'est illustrée par trois tendances :

- le *Big Game Hunting* : parmi les multiples attaques observées, l'ANSSI et ses partenaires constatent qu'un nombre accru de groupes cybercriminels favorisent le ciblage d'entreprises et institutions particulières dans leurs attaques par rançongiciel ;
- le *ransomware-as-a-service* (RaaS) : de plus en plus de rançongiciels sont disponibles sur les marchés cybercriminels par un système d'affiliation et sont utilisés à la fois de façon ciblée et lors de campagnes massives en fonction de la volonté et des capacités des groupes cybercriminels souscrivant au service. La majorité des signalement remontés à l'ANSSI en 2020 ont concerné des rançongiciels fonctionnant selon le modèle économique du RaaS ;
- la double extorsion : existant depuis novembre 2019, cette tendance consiste à faire pression sur la victime en exfiltrant ses données et en la menaçant de les publier sur un site Internet, généralement en .onion, afin qu'elle paye la rançon. Il est ainsi de plus en plus fréquent qu'un chiffrement soit précédé d'une exfiltration de données.

A l'exception de rançongiciels utilisés exclusivement par un unique groupe cybercriminel, tels que le rançongiciel Clop par TA505 ou le rançongiciel WastedLocker par Evil Corp, les attaques par rançongiciel respectent une chaîne d'infection relativement similaire, caractérisée par l'usage d'outils légitimes de post-exploitation (Cobalt Strike, Mimikatz, etc.). Il est néanmoins observé une diversification, voire une sophistication, des vecteurs d'infection utilisés.

Cette chaîne d'infection peut être facilitée par le recours à l'écosystème cybercriminel, dont l'industrialisation permet aux opérateurs de rançongiciel de sous-traiter une grande partie des ressources et outils nécessaires à la réalisation de leurs opérations.

En outre, il est parfois observé une collaboration entre opérateurs de différents rançongiciels. La menace qu'ils représentent serait d'autant plus importante si la concurrence censée régner entre les différents développeurs et opérateurs de rançongiciels laissait place à une émulation.

En matière de victimologie, aucun secteur d'activité ni zone géographique n'est épargné. Cependant, il est observé une hausse des attaques à l'encontre des collectivités locales, du secteur de l'éducation, du secteur de la santé et d'entreprises de services numériques.

Pour les entités victimes, les coûts et dégâts causés sont variés (pertes financières, pertes d'exploitation, atteinte à l'image, perte de clients, perte de données, etc.) et contribuent malheureusement parfois au paiement de la rançon. Ce paiement est parfois incité par des assurances cyber souscrites par les victimes mais aussi favorisé par le fait que le montant de la rançon est souvent inférieur aux coûts de remédiation. L'évolution des législations américaines et européennes en matière de lutte contre le blanchiment de capitaux et financement du terrorisme pourrait agir comme un frein à cette incitation en engageant la responsabilité de toute personne physique ou morale facilitant le paiement de la rançon.

La rentabilité des attaques par rançongiciel, bien supérieure à leur coût de mise en œuvre, explique la prolifération des groupes d'attaquants et laisse présager une constance, si ce n'est une hausse, de la menace liée aux rançongiciels dans les années à venir.

2 Périmètre d'analyse et notions de base

Ce document se concentre sur l'analyse des attaques par chiffrement à finalité lucrative et leur impact sur les entreprises et institutions.

Sont exclus du périmètre d'analyse :

- les rançongiciels ne s'appuyant pas sur le chiffrement de fichiers ;
- les codes de sabotage prenant l'apparence de rançongiciel mais n'étant pas distribués dans une logique lucrative ;
- les attaques n'impliquant pas de rançongiciels mais l'usage d'outils légitimes de chiffrement tels que BestCrypt ou BitLocker.

Un rançongiciel est un code malveillant empêchant la victime d'accéder au contenu de ses fichiers afin de lui extorquer de l'argent. La très grande majorité des rançongiciels a actuellement la capacité de chiffrer des fichiers stockés sur le réseau de la victime.

Il est possible de catégoriser les attaques par rançongiciel selon trois types :

- les campagnes d'attaques non ciblées, caractérisées par leur faible coût de mise en oeuvre ainsi que par leur faible sophistication. Généralement, la campagne d'infection est massive et les cibles manquent de protection numérique.
- les campagnes massives automatiques représentées par l'unique exemple qu'est WannaCry [1].
- les attaques ciblées dites « Big Game Hunting », en recrudescence depuis 2018. Elles ne reposent plus sur un grand nombre de compromissions pour générer de l'argent, mais sur la capacité de l'attaquant à se propager au sein du réseau ciblé de manière furtive et à identifier et chiffrer les ressources clés de la cible, ainsi que la capacité financière de la cible à payer des rançons de montant important et la criticité de sa continuité d'activité.

Un opérateur sera compris dans ce document comme l'utilisateur d'un rançongiciel. Ainsi, aussi bien un développeur qui l'utilise pour son compte qu'un affilié pourra être considéré comme l'opérateur d'un rançongiciel.

Les annexes apportent des détails sur certains rançongiciels parmi les plus actifs du moment : DoppelPaymer, Egregor, Netwalker, Ryuk, Sodinokibi et WastedLocker.

1. En mai 2017, le rançongiciel Wannacry a infecté en une journée au moins 200000 machines dans plus de 150 pays lors de la plus vaste campagne d'attaques par rançongiciel jamais observée. La particularité de cette campagne d'attaques est qu'elle n'a nécessité aucune interaction avec la victime pour l'infecter et aucune action manuelle de l'attaquant pour se propager dans son réseau. L'attaque Wannacry mettait en oeuvre un code d'exploitation de vulnérabilité appelé EternalBlue, supposément développé par la NSA et divulgué en source ouverte deux mois plus tôt par l'avatar Shadow Broker.

3 Evolution de la menace rançongiciel

3.1 Augmentation continue du nombre d'attaques par rançongiciel depuis 2018

Les rançongiciels représentent actuellement la menace informatique la plus sérieuse pour les entreprises et institutions, par le nombre d'attaques quotidiennes et leur impact potentiel sur la continuité d'activité.

Alors que 54 incidents liés à des rançongiciels ont été signalés à l'ANSSI en 2019, l'Agence a enregistré une hausse de 255% en 2020 avec 192 incidents rapportés.

3.2 Tendance du Big Game Hunting

L'ANSSI et ses partenaires constatent que de plus en plus de groupes cybercriminels possédant des ressources financières et des compétences techniques importantes favorisent 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.

Ce ciblage précis est notamment illustré par :

- les rançongiciels RagnarLocker et DarkSide dont chaque échantillon est adapté à l'organisation ciblée [1, 2];
- le rançongiciel RansomEXX dont l'échantillon du code contient le nom de la victime codé en dur et dont l'extension de fichiers et l'adresse courriel de contact utilisent le nom de la victime [3];
- le rançongiciel Netwalker dont le montant de la rançon est adapté aux revenus de l'entreprise.

3.3 Tendance du Ransomware-as-a-Service

Certains rançongiciels sont connus pour être employés exclusivement dans le cadre d'attaques de type « Big Game Hunting ». Parmi eux, se trouvent par exemple les rançongiciels Clop opéré par le groupe cybercriminel TA505 et WastedLocker opéré par le groupe cybercriminel Evil Corp.

D'autres, disponibles sur les marchés cybercriminels par un système d'affiliation connu sous le nom de « Ransomware-as-a-Service » (RaaS), sont utilisés à la fois de façon ciblée et lors de campagnes massives en fonction de la volonté et des capacités des groupes cybercriminels souscrivant au service.

En 2020, la majorité des signalements remontés à l'ANSSI a concerné un nombre limité de rançongiciels, fonctionnant tous selon le modèle économique du RaaS : Sodinokibi (alias REvil), DoppelPaymer, Maze, Netwalker et Egregor.

Le modèle du RaaS consiste à proposer l'accès sous forme d'abonnement ou de partenariat à un rançongiciel, ses infrastructures de paiement et de distribution ainsi qu'à un ensemble de services *back-office* (maintien en condition opérationnelle, support technique, interface de gestion d'implants, interface d'échange avec les victimes, *etc.*), le tout sous une forme "prête à l'emploi".

Les cybercriminels souscrivant aux services d'un RaaS sont dit "affiliés" à ce service. Il leur permet de mener des opérations d'extorsion efficaces à moindre coût, sans nécessairement détenir les compétences techniques pour le développement d'un rançongiciel et le maintien de son infrastructure de commande et de contrôle (C2).

Ce service de RaaS peut être public (GandCrab [2], Dharma ou encore Ranion par exemple), restreint (Sodinokibi [3] par exemple) ou privé (Nemty par exemple) [4].

2. GandCrab a cessé son activité en 2019.
3. Sodinokibi est réputé avoir pris la suite de GandCrab.

Par exemple, les développeurs de Sodinokibi ont choisi de limiter le nombre d'affiliés, de leur imposer un niveau d'activité élevé et d'interdire tout affilié anglophone. En outre, ils cherchent des profils d'affiliés particuliers, notamment spécialisés dans la compromission ciblée de réseaux d'entreprises [5]. Les développeurs de Sodinokibi mettent à disposition de leurs affiliés un code de chiffrement, une infrastructure de distribution, des interfaces d'administration, de paiement et de contact avec leurs futures victimes ainsi qu'un site Internet dédié à la publication de données exfiltrées. Ils proposent également l'équivalent d'un support utilisateur. En échange, 30 à 40% des gains générés par ces affiliés leur reviennent.

Le modèle de RaaS multiplie le nombre d'attaques par rançongiciel ainsi que le nombre de méthodes différentes pour compromettre le réseau victime et s'y propager.

Il rencontre un important succès dans l'écosystème cybercriminel depuis 2019. Des rançongiciels historiquement utilisés par un unique groupe cybercriminel se convertissent en RaaS : Phobos, apparu en octobre 2017, est vendu en tant que RaaS depuis avril 2019 [6, 7].

Les RaaS sont également caractérisés par leur évolution et leur régulière amélioration. Par exemple, GandCrab a évolué en Sodinokibi, AKO a évolué en Ranzy et Defray777 a évolué en RansomEXX. Les développeurs de DarkSide ont même annoncé être d'anciens affiliés d'autres rançongiciels, dont ils se seraient inspirés.

4 Chaîne d'infection générale

Par leur usage courant d'outils légitimes de post-exploitation et par le déploiement final d'un même type de code malveillant, les attaques par rançongiciel respectent une chaîne d'infection pouvant être schématisée selon le modèle suivant :

4.1 Vecteurs d'infection

Les vecteurs d'infection des attaques par rançongiciel se sont diversifiés. Par le passé essentiellement limités à des courriels d'hameçonnage ou à l'exploitation d'accès RDP mal sécurisés, ils comprennent désormais d'autres vecteurs possibles tels que les points d'eau, l'exploitation de vulnérabilités ou encore des attaques par chaîne d'approvisionnement.

De plus, les systèmes d'exploitation Windows ne sont plus les seuls à être ciblés. Quelques rançongiciels, comme par exemple RansomEXX, ciblent également des systèmes d'exploitation Linux [8].

4.1.1 Courriels d'hameçonnage

De nombreux rançongiciels sont distribués par courriel d'hameçonnage. Parmi les plus récents, se trouvent par exemple Egregor [9], RagnarLocker [10] ou encore Ranzy [11].

Il n'est pas rare que les courriels d'hameçonnage distribuent une première charge utile de type *loader*, chargée, après propagation dans le réseau, de déployer la charge finale qu'est le rançongiciel. Ce type de *loader* peut être utilisé lorsque le rançongiciel n'a pas la capacité de se latéraliser automatiquement au sein d'un réseau. Par exemple, le rançongiciel Clop, opéré par TA505, est distribué au bout de la chaîne d'infection SDBbot-Get2 [12].

Hormis un ou deux *loaders* propres aux attaquants comme dans le cas de la chaîne d'infection de Clop, la charge utile visant à déployer le rançongiciel peut être :

- un cheval de Troie fonctionnant sur un modèle d'affiliés, tel que TrickBot. Bien que le code utilisé ne lui soit pas propre, l'opérateur du cheval de Troie et celui du rançongiciel sont alors généralement confondus.
- un code malveillant utilisé par un autre groupe d'attaquants pour le compte de l'opérateur de rançongiciel dans le but qu'il réalise la compromission initiale du SI à sa place (service de distribution), voire qu'il s'y propage. Dans ce cas, la chaîne d'infection implique au moins deux attaquants, l'attaquant opérant le service de distribution et l'opérateur final du rançongiciel.

4.1.2 Point d'eau

Les chaînes d'infection aboutissant au déploiement d'un rançongiciel peuvent être initiées par une compromission par point d'eau. La visite, directe ou motivée par une URL reçue par courriel, d'un site Internet compromis peut conduire :

- à la distribution du rançongiciel ou d'une charge intermédiaire : par exemple, dans le cas du rançongiciel WastedLocker, lorsque la victime visite un site légitime compromis, une fausse mise à jour de navigateur apparaît sur son poste et télécharge un fichier ZIP contenant le fichier Javascript malveillant FakeUpdates. Ce dernier distribue l'outil légitime Cobalt Strike. Les attaquants élèvent alors leurs privilèges, se propagent sur le réseau et identifient d'autres ressources sur lesquelles déployer leur rançongiciel. Ces étapes sont réalisées manuellement. PsExec, ou plus rarement SecTool, est ensuite utilisé pour désactiver Windows Defender et exécuter WastedLocker [13, 14, 15] ;

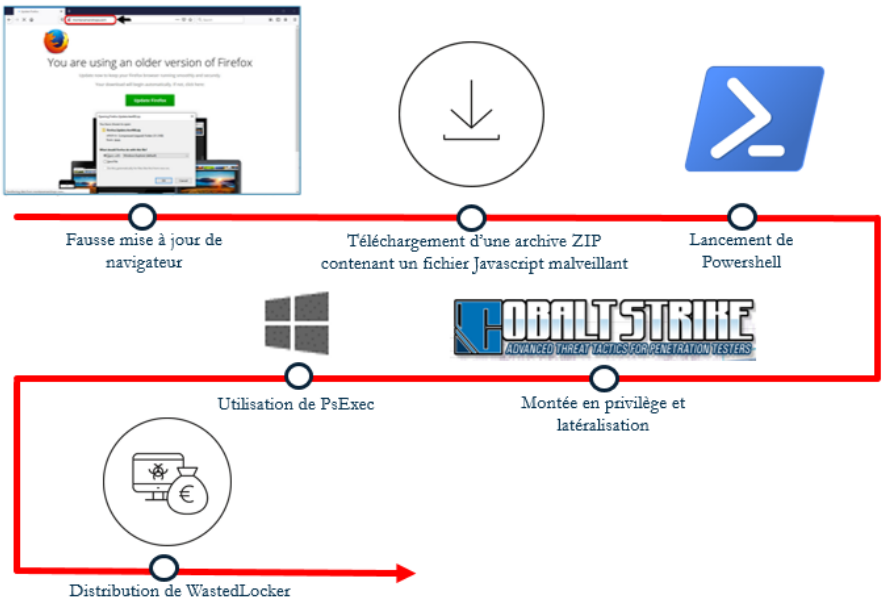

Fig. 4.1 – Point d'eau aboutissant au déploiement de WastedLocker

- à la distribution d'un kit d'exploitation : dans ce cas, le kit cherche à exploiter une vulnérabilité sur le serveur de la victime et exécute une charge utile s'il y est parvenu. Cette charge utile pourra à son tour distribuer le ou les codes malveillants des attaquants. Le kit d'exploitation Lord a ainsi été utilisé en août 2020 pour distribuer le rançongiciel Eris [16].

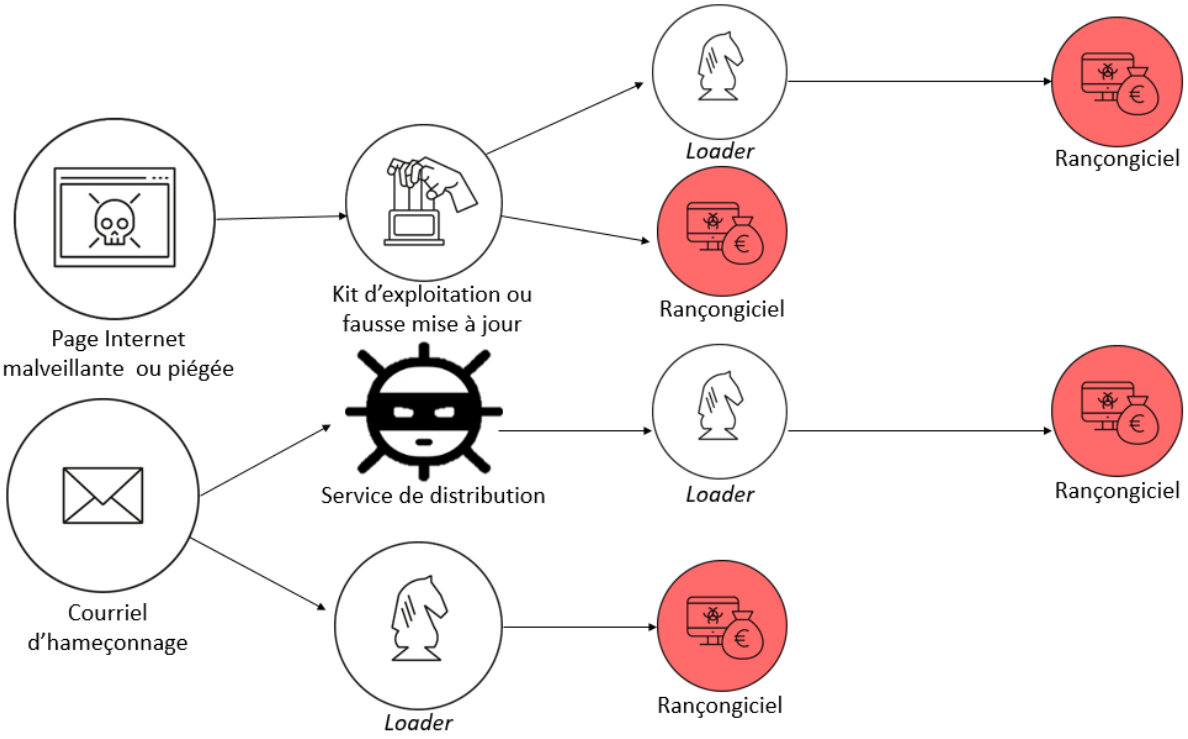

Fig. 4.2 – Différents scenarios d'infection par rançongiciel suite à la réception d'un courriel d'hameçonnage ou la visite d'un site Internet compromis

4.1.3 Accès RDP mal sécurisés

Les opérateurs de rançongiciels favorisent particulièrement l'accès RDP comme vecteur d'infection, malgré la fermeture de la place de marché souterraine xDedic spécialisée dans la vente de ce type d'accès [16]. Parmi les rançongiciels ayant été déployés par ce biais en 2020, se trouvent notamment DoppelPaymer [17], Egregor [9], Nemty [9], Nephilim [18], Pay2Key [19], Phobos [6] et RagnarLocker [20].

4.1.4 Exploitation de vulnérabilités

Les vulnérabilités exploitées peuvent être liées :

- à des serveurs : par exemple, l'un des vecteurs d'infection particulièrement utilisés en 2020 aura été l'exploitation de vulnérabilités affectant des serveurs Citrix non mis à jour. DoppelPaymer [21], Nephilim [22] ou encore RagnarLocker [23, 24] ont été distribués *via* ce vecteur d'infection ;
- à des logiciels VPN : la démocratisation du télétravail dans le contexte de la pandémie de Covid-19 marque une recrudescence d'exploitation de vulnérabilités présentes dans des logiciels VPN commerciaux [1]. Le *bruteforcing* de couples identifiant/authentifiant d'administrateurs de services VPN a aussi été expérimenté dans le cas par exemple de LockBit [25] ou de Nephilim [26] ;
- à des logiciels de surveillance et gestion à distance (RMM pour *Remote Monitoring and Management*) : par exemple, le vecteur d'infection de plusieurs attaques impliquant RagnarLocker a été l'exploitation de vulnérabilités de logiciels tels que ConnectWise [4] et Kaseya [5] [23]. Les logiciels d'infogérance sont particulièrement ciblés dans ce cadre [27].

4.1.5 Supply-chain attacks

Bien que moins fréquentes, les attaques de type *supply-chain* ne sont pas à omettre. Certains affiliés de Sodinokibi ont ainsi compromis une prestataire en service informatique et par son intermédiaire, ont pu compromettre les systèmes d'information (SI) de 22 villes au Texas [16].

4.2 Post-exploitation

Les rançongiciels sont déployés soit manuellement, soit par le biais de processus automatiques, permettant une rapide latéralisation au sein du réseau victime (cas par exemple de LockBit [25]).

Dans l'un ou l'autre cas, l'année 2020 marque un accroissement de la rapidité d'exécution des attaquants. Par exemple, le délai entre l'infection initiale et le chiffrement d'une attaque impliquant BazarLoader et Ryuk, attribuée au *cluster* d'activité UNC1878, s'est réduit au cours du second semestre 2020 de quelques jours à trois heures [28]. Concernant Pay2Key, le délai entre la latéralisation et le chiffrement peut être de l'ordre d'une heure [19].

En amont de la phase de post-exploitation d'une chaîne d'infection aboutissant au déploiement d'un rançongiciel, il arrive qu'un *loader* spécifique ou de type cheval de Troie bancaire puisse être distribué en tant que première charge utile. Ce code malveillant permet alors aux attaquants de récupérer des informations facilitant les mouvements latéraux ultérieurs et de télécharger d'autres charges malveillantes. Par exemple :

- Ryuk a été distribué par TrickBot et BazarLoader [29] ;

4. Application logicielle de bureau à distance.
5. Logiciel de gestion informatique.

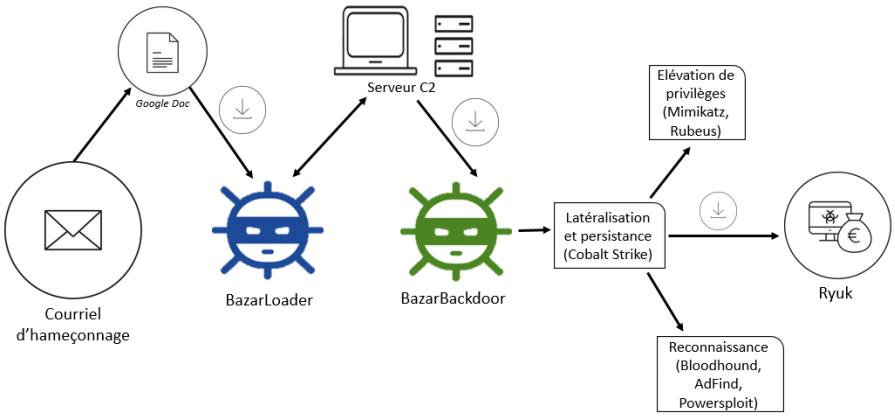

Fig. 4.3 – Chaîne d'infection Bazar-Ryuk

- Egregor a été distribué par QakBot, IcedID (alias BokBot) et Gozi ISFB (alias Ursnif) [30];
- ProLock a été distribué par QakBot [31];
- Nemty a été distribué par SmokeBot [32];
- BitPaymer a été distribué par Dridex [33];
- DoppelPaymer est distribué par DoppelDridex [33];
- Defray777 a été distribué par TrickBot [34];
- etc.

Rançongiciel/Loader	QakBot	IcedId	Gozi ISFB	SmokeBot	Dridex	DoppelDridex	TrickBot	BazarLoader
Egregor	x	x	x					
Ryuk							x	x
ProLock	x							
Nemty				x				
BitPaymer					x			
DoppelPaymer						x		
Defray777							x	

La phase de post-exploitation d'une attaque par rançongiciel se déroule généralement de la manière suivante [35] :

- pour élever leurs privilèges au sein du SI, les attaquants peuvent :
  - procéder à des attaques par force brute ;
  - exploiter des vulnérabilités logicielles, par exemple du type ZeroLogon (cas de Ryuk [29]) ou d'autres types de CVE ;
  - utiliser des outils de tests d'intrusion tels que Mimikatz, Mimidogs, Mimikittenz [36], Windows Credentials editor, Rubeus [37] et LaZagne [16], afin de récupérer des identifiants légitimes.
- pour effectuer la cartographie de l'Active Directory (AD), les attaquants utilisent généralement les outils de tests d'intrusion BloodHound, SharpHound ou ADFind [38].
- pour se latéraliser, les attaquants peuvent utiliser les outils de tests d'intrusion Cobalt Strike, Metasploit, Powershell Empire, Koadic ou encore CrackMapExec (cas par exemple de LockBit [39]) mais aussi utiliser abusivement des outils Windows tels que WMI [35], WinRM [16] et PsExec [35].
- pour déployer le rançongiciel, les attaquants utilisent par exemple un *loader*, PsExec [16] ou encore des tâches planifiées déployées par GPO (*Group Policy Objects*).

Enfin, les attaquants emploient des techniques d'assombrissement de code et d'évasion de la défense afin de complexifier leur détection. Ils peuvent notamment utiliser des outils natifs de Windows, qui demandent une surveillance plus poussée du SI pour que leur utilisation malveillante soit détectée.

Par exemple :

- TA505 utilise un code de compression (*packer*) pour rendre ses codes malveillants plus difficiles à analyser. Ce

code, appelé Minedoor, a été utilisé pour compresser le rançongiciel Clop [12];
- comme d'autres rançongiciels peuvent le faire, Netwalker injecte son code en mémoire pour augmenter sa furtivité, aucun binaire du rançongiciel n'étant stocké sur le disque dur de la victime (*fileless ransomware*) [40];
- RagnarLocker a déjà été téléchargé à l'intérieur d'une VM Oracle VirtualBox Windows XP, le but étant d'éviter la détection par le logiciel anti-virus installé sur la machine physique [20].

4.3 Exfiltration de données

De plus en plus de rançongiciels exfiltrent des données de leur victime avant chiffrement. Par exemple, ProLock exfiltre des données *via* l'outil en ligne de commande Rclone sous la forme d'un fichier archive 7ZIP vers des sites de services nuagiques (OneDrive, Google Drive, Mega) [41, 42].

4.4 Chiffrement

Une fois déployé dans le SI, un rançongiciel arrête généralement de nombreux processus, notamment ceux relatifs aux logiciels de sécurité, aux logiciels de gestion informatique à distance, aux outils d'accès à distance ou encore au serveur de base de données. Par exemple, Nephilim arrête plus de 1000 processus [43]. Pour ce faire, les opérateurs de rançongiciel peuvent par exemple utiliser l'API Windows Restart Manager, comme c'est le cas pour Ranzy [11].

En matière de chiffrement, Phobos est capable de chiffrer des fichiers sans accès préalable à une connexion Internet [7] et WastedLocker chiffre aussi bien les fichiers locaux que les fichiers distants et ceux stockés sur des disques externes [14]. Ryuk, quant à lui, dispose d'une fonctionnalité lui permettant d'allumer les postes éteints présents sur le réseau local (*Wake-on-LAN*) afin d'accroître sa surface de chiffrement [44].

Dans le cas d'une attaque de type *Big Game Hunting*, le chiffrement peut être indiscriminé ou adapté à la cible. Par exemple, l'extension des fichiers chiffrés par DarkSide est construite sur la base de l'adresse MAC des victimes [45]. De même, l'extension de fichiers et l'adresse courriel de contact relatives à RansomEXX utilisent le nom de la victime [3].

Enfin, concomitamment au chiffrement des données, les rançongiciels suppriment généralement les copies cachées *via* :

- une commande Powershell comme c'est le cas pour DarkSide [2];
- des commandes vssadmin comme c'est le cas pour par exemple Nemty [32], Netwalker [46], ProLock [41] et Ranzy [11];
- *via* un fichier .bat [6] comme c'est le cas pour Ryuk [47];
- *via* des commandes WMIC [16].

Commentaire : L'outil Raccine disponible sur Github permet d'intercepter le recours à vssadmin et d'empêcher la suppression des copies fantômes voire dans certains cas de bloquer la chaîne d'infection. Raccine est une solution temporaire à mettre en œuvre uniquement en dernier recours face à une menace imminente de chiffrement. Son utilisation ne remplace pas la mise en œuvre de mesures techniques de sécurité et de défense en profondeur.

4.5 Demande de rançon

Généralement, les rançongiciels proposent des options de configuration garantissant que les fichiers systèmes de la machine compromise ne seront pas affectés, permettant ainsi à la victime de prendre connaissance des pertes réelles, de la note de rançon et des modalités de paiement.

6. Extension d'un fichier de commandes MS-DOS permettant de concevoir des scripts, utilisés ici pour des tâches de maintenance telles que la suppression de fichiers.

Une fois le chiffrement terminé, une demande de rançon est accessible à la victime qui peut alors contacter les attaquants soit *via* une adresse courriel de contact qui lui est fournie (cas par exemple de Netwalker [46]), soit *via* le site en .onion associé au rançongiciel, soit *via* un site alternatif ne nécessitant pas l'installation de Tor. LockBit propose par exemple ces deux dernières possibilités [48].

Le paiement peut, quant à lui, être effectué au travers d'un portail de paiement hébergé sur un site en .onion (cas de Darkside par exemple [45]), ou en envoyant les fonds directement aux adresses des portefeuilles de cryptomonnaies fournies par les attaquants dans leur demande de rançon ou après échange avec la victime.

Le montant de la rançon à destination d'une entité victime est variable aussi bien en fonction du rançongiciel que de la victime. Par exemple, le montant d'une rançon DarkSide peut osciller entre 200 000 et 2 millions de dollars [45] tandis qu'une rançon WastedLocker peut être comprise entre 500 000 dollars et 10 millions de dollars [14].

Les opérateurs de rançongiciels, en particulier ceux qui réalisent des attaques de type *Big Game Hunting*, sont souvent ouverts à la négociation du montant de la rançon. Le site de divulgation de données de DarkSide dispose ainsi depuis 2021 d'un accès VIP dédié aux entreprises de négociation leur permettant de bénéficier de réductions du montant des rançons demandées à leurs clients [49]. Certains forcent même à la négociation. C'est par exemple le cas des opérateurs de SunCrypt qui, depuis octobre 2020, menacent ponctuellement leurs victimes de représailles sous forme d'attaques DDoS si elles venaient à cesser les négociations [50]. D'autres opérateurs en viennent même à appeler les victimes, leurs clients et parfois leurs prestataires, ou encore à les menacer d'alerter les journalistes de leur compromission [51].

La grande majorité des rançongiciels demandent à ce que la rançon soit payée en monnaie virtuelle convertible (CVC) [40], et plus particulièrement en Bitcoin. Bien que les transactions en Bitcoin puissent parfois être tracées et permettre aux forces de l'ordre d'en retrouver les bénéficiaires, cette cryptomonnaie est la plus répandue et la plus facile à obtenir pour les victimes. En cas de paiement de la rançon, ces dernières transfèrent les fonds vers une plateforme d'échange de crypto-actifs qui les convertit en Bitcoins. Ces Bitcoins sont ensuite envoyés à l'adresse du portefeuille contrôlé par les attaquants. Une fois la rançon reçue, les attaquants la blanchissent au travers de divers moyens [7] [40].

Certains opérateurs de rançongiciel demandent parfois que la rançon soit payée en cryptomonnaies favorisant l'anonymat (AEC), du type Monero. En effet, les transactions réalisées dans ce type de cryptomonnaies sont réputées moins traçables. Il arrive aussi que des attaquants proposent des réductions sur le montant de la rançon aux victimes qui paieront en AEC [40]. Par exemple, depuis avril 2020, les rançons après un chiffrement par Sodinokibi peuvent être payées en Monero. Si la victime souhaite payer en Bitcoin, le montant de la rançon augmente de 10% [52].

Commentaire : ***Le paiement d'une rançon n'assure pas l'éviction des attaquants du SI compromis, signifiant que des opérations de nettoyage et la mise en place de mesures permettant de faire monter le niveau de sécurité du système d'information seront nécessaires dans tous les cas. De plus, le versement de la rançon n'assure pas à la victime de recevoir la clé de déchiffrement ni que les données potentiellement exfiltrées seront effacées ou ne seront pas utilisées à des fins malveillantes.***

L'évolution de la législation en matière de lutte contre le blanchiment de capitaux pourrait avoir une incidence sur le choix de payer la rançon. En effet, en octobre 2020, le Département du Trésor américain a rappelé que les victimes de rançongiciels qui paieraient la rançon ou les sociétés facilitant ces paiements seraient sanctionnées, en particulier si ces paiements étaient à destination de groupes d'attaquants eux-mêmes sujets à des sanctions américaines. Par exemple, le paiement d'une rançon de 10 millions de dollars par l'entreprise américaine Garmin au groupe cybercriminel Evil Corp dans le cadre d'une attaque par le rançongiciel WastedLocker est à ce titre théoriquement sanctionnable [53, 54]. Au niveau européen, la sixième directive de lutte contre le blanchiment de capitaux et le financement du terrorisme, transposable depuis décembre 2020 par les pays membres de l'Union européenne, inclue quant à elle la cybercriminalité dans la liste des infractions principales constituant le blanchiment. Rendant, en sus des personnes physiques, les personnes morales punissables, elle considère dorénavant complices les facilitateurs de blanchiment de capitaux, tels que les plateformes d'échange de crypto-actifs par exemple [55, 56].

7. Recours à des mixeurs afin de convertir les Bitcoins en d'autres CVCs, répartition des fonds entre de nombreux autres portefeuilles ou encore transfert vers une plateforme d'échange de crypto-actifs située dans un pays aux faibles contrôles en matière de lutte contre le blanchiment d'argent et le financement du terrorisme (LCB-FT).

4.6 Principe de double extorsion

Le principe de double extorsion existe depuis novembre 2019 et aurait été introduit par les opérateurs du rançongiciel Maze. Il consiste à faire pression sur la victime en exfiltrant ses données et en la menaçant de les publier sur un site Internet, généralement en .onion, dans le but qu'elle paye la rançon. Cette menace est limitée dans le temps. Par exemple, les opérateurs d'Egregor laissent aux victimes un délai de 72 heures pour les contacter, sans quoi leurs données sont publiées [1].

Cette menace de divulgation peut être précédée par la révélation de la compromission en mentionnant les adresses IP des machines compromises ainsi qu'un extrait des fichiers récupérés par l'attaquant, ceci ayant pour but d'authentifier l'acte et d'exercer une pression supplémentaire sur la victime. Les fichiers sont parfois protégés à ce stade par un mot de passe.

De plus, afin de faire davantage pression sur les victimes, les opérateurs de rançongiciel peuvent menacer de communiquer une partie des informations dérobées aux médias. C'est par exemple le cas des opérateurs d'Egregor [57]. En outre, le site du rançongiciel DarkSide dispose à cette fin depuis début 2021 d'un accès VIP destiné à la presse [49].

Avant que cette méthode n'émerge, des attaques par rançongiciel pouvaient déjà être accompagnées d'exfiltrations de données. C'est par exemple le cas de DoppelSpider, groupe cybercriminel à l'origine du rançongiciel DoppelPaymer, qui, avant l'introduction de leur site de publication de données en février 2020, exfiltraient déjà les données de leurs victimes à des fins de revente sur le *Dark Web*, dans le but d'augmenter la rentabilité de leurs attaques malgré le non-paiement de la rançon [58].

Les sites de divulgation sont pour la plupart accessibles *via* Tor, bien que certains opérateurs de rançongiciels disposent de deux sites, dont l'un est accessible *via* un navigateur classique. C'est par exemple le cas du rançongiciel Nephilim [18].

Depuis 2020, en sus de la double extorsion, des opérateurs de rançongiciels, tel que ceux de RagnarLocker [59], mettent aux enchères les données exfiltrées aux victimes sur un espace de vente dédié. En mai 2020, la firme d'avocats américains Grubman Shire Meiselas & Sacks a été victime d'une compromission par Sodinokibi. Les opérateurs du rançongiciel ont réussi à exfiltrer des données relatives à certains de ses clients, et ont entrepris de vendre au plus offrant des informations concernant Donald Trump, ainsi que d'autres célébrités comme Madonna. Ils ont ouvert, début juin 2020, un espace dédié aux enchères sur leur site de divulgation, afin de mettre en vente certaines données qu'ils exfiltrent. Tout individu pouvait participer anonymement à la vente aux enchères contre un dépôt de sécurité de 10% du prix de départ. Les enchères se faisaient en Monero [60].

5 Recours à l'écosystème cybercriminel des opérateurs de rançongiciel

5.1 Cybercrime-as-a-service

L'écosystème cybercriminel est constitué de vendeurs et d'acheteurs de biens (codes malveillants, accès compromis, données personnelles volées, etc.) et de services (location d'infrastructures de déni de service, d'anonymisation, etc.). Les opérateurs de rançongiciel peuvent sous-traiter une grande partie des ressources et outils nécessaires à la réalisation de leurs opérations.

Les attaquants peuvent ainsi sous-traiter la compromission du SI de leurs cibles en ayant recours à des services de distribution ou en louant des botnets de pourriels [61]. Par exemple, le botnet Necurs, actif de 2012 à 2020, a distribué des pourriels et diverses charges utiles telles que le rançongiciel Locky [12].

En pratique, ces services de distribution :

- infectent des cibles par des courriels d'hameçonnage d'aspect crédible, envoyés soit depuis l'infrastructure des attaquants en utilisant des adresses courriel expéditrices typosquattées, soit depuis des boîtes courriel compromises. Cette campagne d'hameçonnage peut être réalisée sur commande du client ou avoir été réalisée en amont ;
- distribuent au sein des SI compromis leur code malveillant ;
- ouvrent l'accès au SI compromis à leur client en y distribuant sa charge utile, de type rançongiciel ou de type *loader* (qui distribuera à son tour le rançongiciel). Par exemple, le service de distribution Emotet a distribué de 2018 à 2020 le code malveillant Trickbot, qui a distribué à son tour le rançongiciel Ryuk. De même, en 2020, Emotet a distribué DoppelDridex qui a distribué à son tour le rançongiciel DoppelPaymer [62].

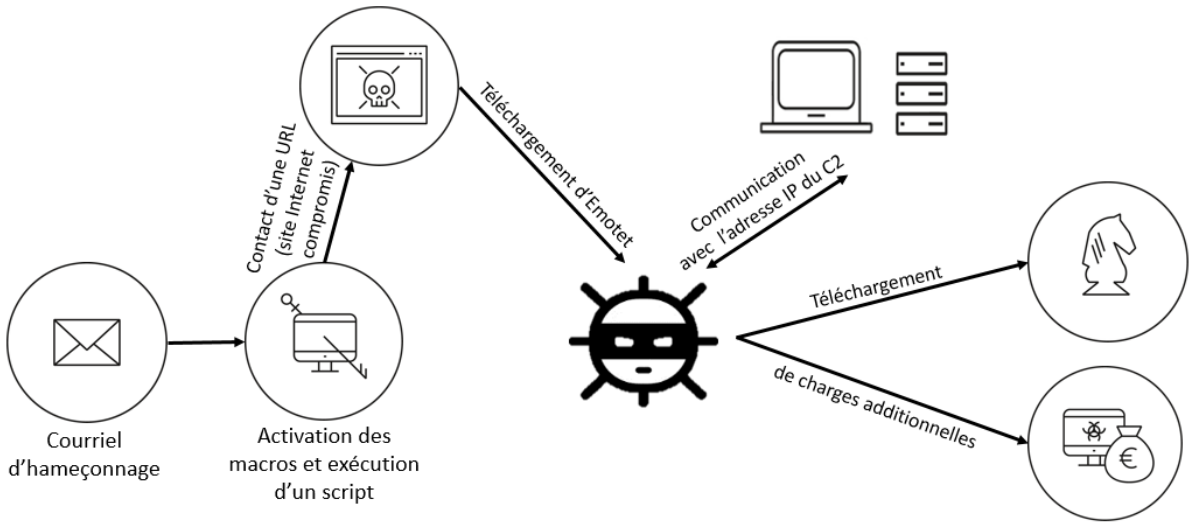

Fig. 5.1 – Distribution de charges malveillantes par Emotet

Les attaquants peuvent également acheter des accès compromis sur des plateformes de commerce actives sur le Dark Web, embaucher un attaquant pour compromettre un ou plusieurs SI pour leur compte, voire solliciter de l'aide sur des forums cybercriminels.

Commentaire : Dans ce cadre, il est fréquent de constater des périodes d'inactivité de plusieurs mois entre la compromission des réseaux des victimes et le dépôt du code de chiffrement sur ces mêmes réseaux, correspondant à la période entre la mise en vente de l'accès compromis et son achat par un autre groupe afin de mener l'attaque.

L'achat de rançongiciel ou de codes intermédiaires est également possible. Par exemple, le rançongiciel Jigsaw, actif depuis 2016, coûte environ 3 000 dollars sur les forums cybercriminels anglophones [61].

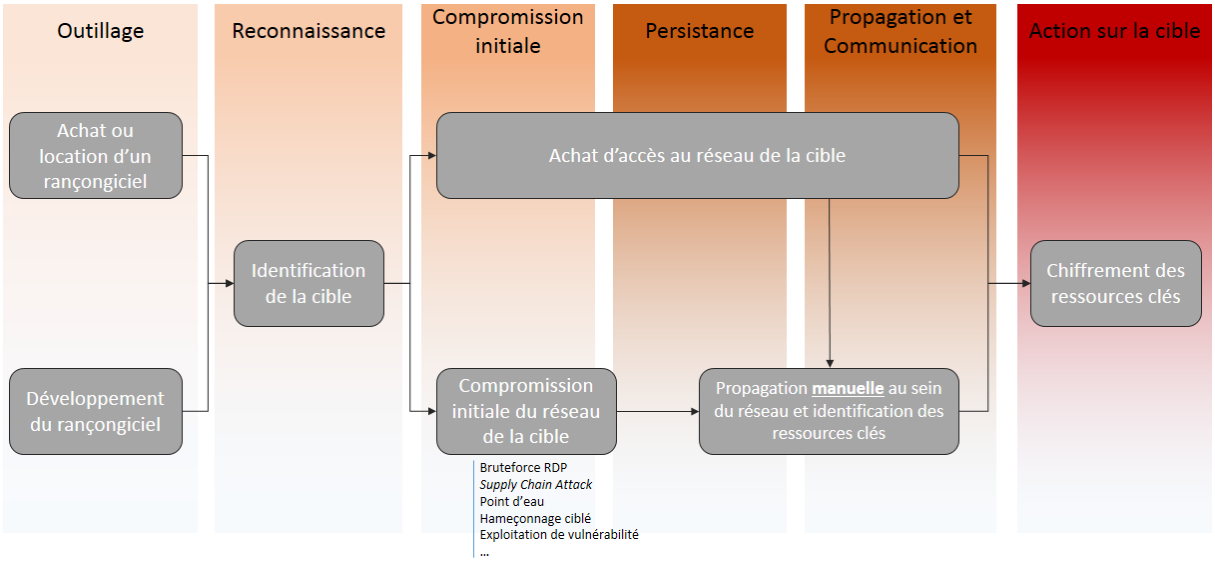

Fig. 5.2 – Recours possible à l'écosystème cybercriminel lors de différentes phases de la *kill chain* d'une attaque par rançongiciel ciblée

Enfin, ces activités malveillantes nécessitent une infrastructure de déploiement robuste et sécurisée susceptible de garantir le meilleur anonymat possible et une certaine pérennité. Cette infrastructure est le plus souvent fournie par des hébergeurs nommés *bulletproof hosters*. Parmi ceux-ci, Yalishanda [63] figure parmi les plus actifs et les plus expérimentés et héberge certains sites associés à des rançongiciels.

Les prestations d'un *bulletproof hoster* comprennent généralement :

- la mise à disposition d'une infrastructure de déploiement pour activité malicieuse protégée contre les DDoS ;
- un support technique de qualité ;
- un contrôle faible sinon inexistant sur l'activité client ;
- un hébergement dans des juridictions hors d'atteinte des traités de coopération judiciaire ;
- des capacités d'enregistrement discret de noms de domaine et certificats SSL ;
- des adresses IP propres tournant régulièrement.

Pour l'enregistrement de leurs noms de domaine, les attaquants ont aussi la possibilité d'utiliser un service du type d'*Emercoin DNS Resolution* [64], qui permet l'enregistrement décentralisé de noms de domaine qui ne peuvent être ni modifiés ni suspendus par une autorité. L'enregistrement est en effet localisé sur une *blockchain*. Ce service est par exemple utilisé par BazarLoader, afin de déployer Ryuk [65].

5.2 Collaboration entre opérateurs de rançongiciels

Plusieurs groupes d'attaquants spécialisés dans les rançongiciels créent des partenariats pour partager des conseils, des informations, des codes ou encore des techniques [40].

Par exemple, des données exfiltrées d'une victime de Maze ont été hébergées sur le site de RagnarLocker, de même que des données exfiltrées d'une victime de RagnarLocker ont été hébergées sur le site de Maze. L'un des groupes affiliés de Maze a également adopté la technique propre à RagnarLocker consistant à distribuer la charge du rançongiciel à l'intérieur d'une machine virtuelle [20].

De plus, certains rançongiciels empruntent du code ou des méthodes à d'autres. Ainsi, DarkSide aurait emprunté

certaines caractéristiques de sa demande de rançon ainsi que sa commande Powershell pour supprimer les copies cachées à Sodinokibi [45].

6 Victimologie des attaques par rançongiciel

6.1 Victimologie géographique

Concernant les attaques non ciblées par rançongiciel, aucun secteur d'activité ni zone géographique n'est épargné. Toute entreprise, institution ou particulier ayant un accès à Internet peut être infecté par un rançongiciel s'il n'a pas mis en œuvre les mesures basiques d'hygiène informatique (sauvegardes à froid, sensibilisation à l'hameçonnage, mises à jour logicielle sur ses machines connectées, antivirus, *etc.*).

Concernant les attaques de type *Big Game Hunting*, les entreprises et institutions dont l'arrêt d'activité peut conduire à des conséquences économiques, industrielles ou sociales importantes sont particulièrement ciblées par les groupes cybercriminels. De plus, ces derniers s'attachent à cibler des entreprises suffisamment rentables pour payer des rançons très importantes.

Néanmoins, il est commun que les rançongiciels ne ciblent pas d'entités situées dans les pays de la Communauté des États indépendants (CEI).

De plus, Checkpoint [66] révèle un ciblage très majoritaire d'entités présentes aux États-Unis. Par exemple, la majorité des cibles de RagnarLocker sont des entités situées aux Etats-Unis [1]. Il en est de même pour celles de WastedLocker [67].

6.2 Victimologie sectorielle

Bien que le ciblage des secteurs soit relativement indifférencié tant que les entités qui le composent sont en mesure de payer une rançon importante, il est intéressant de souligner le ciblage récurrent de secteurs d'activité ou de types d'entité qui n'apparaissent pas naturellement comme des cibles de choix pour les cybercriminels.

6.2.1 Les collectivités locales

Les collectivités locales sont particulièrement ciblées par les opérateurs de rançongiciels. Par exemple, en août 2019, Sodinokibi a compromis une vingtaine de villes au Texas ; d'avril 2019 à mars 2020, Ryuk a compromis au moins cinq villes américaines ; et de mars à octobre 2020, DoppelPaymer a lui aussi compromis au moins cinq villes, dont les mairies françaises de Charleville-Mézières en mars 2020 et de Mitry-Mory en juillet 2020 [68, 17, 69, 70].

Les raisons possibles de ce ciblage de plus en plus fréquent peuvent être :

- Le faible niveau de sécurité des systèmes d'information de ce type d'organisation ;
- Un historique de rançons payées par des villes, rendant ces cibles attractives et rentables pour les attaquants. Par exemple, Riviera Beach, Lake City, Jackson, LaPorte County et Rockville Centre ont à elles cinq payées presque 1,9 millions de dollars de rançon aux opérateurs de Ryuk [16] ;
- La présence de données sensibles pouvant peser en faveur du paiement de la rançon ;
- Le fait que la rupture d'activité soit difficile à supporter pour les mairies compte tenu du rapide impact social et politique.

6.2.2 Le secteur de l'éducation

Le secteur de l'éducation est lui aussi particulièrement victime d'attaques par rançongiciel. Aux Etats-Unis, il serait le deuxième secteur victime le plus convoité par les attaquants après les collectivités locales [27].

Netwalker a ainsi récemment ciblé les université d'Etats du Michigan, de Californie, d'Utah et le Columbia College of Chicago [67].

En France, malgré plusieurs signalements relatifs à des compromissions par rançongiciel remontés à l'ANSSI en 2020, le secteur de l'éducation ne fait pas partie des secteurs les plus ciblés.

6.2.3 Le secteur de la santé

Les hôpitaux et autres entités du secteur de la santé représentent globalement l'une des cibles privilégiées des attaquants [27, 71]. Cette tendance s'est accrue en 2020, notamment dans le contexte de pandémie liée à la Covid-19, l'attaque poussant sans doute plus facilement les hôpitaux à payer la rançon au vu du besoin critique de continuité d'activité [66].

Par exemple, en 2020, Netwalker a attaqué plusieurs hôpitaux espagnols ainsi que des services de santé [72, 73] et Sodinokibi a ciblé le centre hospitalier français de Marmande Tonneins [74].

Certains opérateurs de Ryuk, notamment UNC1878, ciblent particulièrement le secteur, ayant été responsables de près de 75% des attaques par rançongiciel sur le secteur de la santé aux Etats-Unis en octobre 2020 [75].

Néanmoins, certains opérateurs de rançongiciels, à l'instar de ceux opérant Nephilim se sont engagés à ne pas attaquer de structures de santé, d'organisations à but non lucratif, d'écoles et d'entités gouvernementales [18].

6.2.4 Les entreprises de services numériques (ESN)

Le secteur d'activité des entreprises de services numériques (ESN) semble de plus en plus attractif pour les opérateurs de rançongiciels. Une ESN peut être ciblée pour atteindre une ou plusieurs victimes précises parmi ses clients, tout comme elle peut être une victime finale, avec comme impact un chiffrement de ses données et potentiellement, de celles de ses clients. Les conséquences peuvent être particulièrement graves si l'ESN n'a pas correctement cloisonné son SI et ses données clients. Outre leur gravité, ces conséquences peuvent être géographiquement et/ou sectoriellement localisées, en fonction de l'ESN victime.

Par exemple, en janvier 2020, l'ESN française Xefi, spécialisée dans les services dédiés aux PME, a été compromise par un rançongiciel, qui s'est propagé sur les réseaux de ses clients par le biais d'un outil de supervision. 200 entreprises du Centre-Est de la France ont ainsi été affectées à plus ou moins grande échelle.

7 Coûts et revenus des attaques par rançongiciel

7.1 Coûts des attaques par rançongiciel pour les entités victimes

D'après les observations de l'ANSSI, les coûts et dégâts causés aux entités victimes de rançongiciels peuvent comprendre :

- des pertes financières, qui concernent toutes les victimes : extorsion d'argent en cas de paiement de la rançon, coût des investigations numériques et de la remédiation ou restauration du SI par un prestataire. Ces pertes ont été estimées par Sopra Steria, victime de Ryuk en octobre 2020, à environ 50 millions d'euros [76];
- une perte d'exploitation, à durée variable : par exemple, arrêt de la production pour une usine, impossibilité temporaire de fournir les services administratifs habituels pour une mairie ou de livrer un projet pour un cabinet d'architecture. En avril 2019, l'attaque par rançongiciel à l'encontre de Fleury-Michon a ainsi provoqué un arrêt de l'activité pendant trois jours et un fonctionnement en mode dégradé pendant deux semaines [77];
- un risque sur la santé des patients, en ce qui concerne les établissements de soin (type Centre Hospitalier ou Urgences notamment) : impossibilité d'accueillir de nouveaux patients, nécessité de les rediriger vers d'autres établissements, perte du standard téléphonique ;
- l'atteinte à l'image ;
- une perte de clients ;
- une perte de confiance à l'égard de l'organisation victime ;
- des pertes de données : R&D, comptabilité, facturation, projets, données de clients ;
- l'atteinte à l'intégrité des données sensibles ou classifiées ;
- l'impossibilité de verser les salaires des employés au cas où l'application RH fait partie du SI endommagé ;
- un impact psychologique de la résolution de l'incident, dû à un manque de ressources et de compétences, dans le cas notamment de petites structures ;
- des victimes collatérales en cas de déploiement du rançongiciel sur des réseaux interconnectés.

7.2 Revenus des attaquants

L'estimation précise des gains des développeurs et des affiliés d'un rançongiciel est rendue difficile par de nombreuses variables inconnues. Le nombre exact d'attaques effectuées, de victimes payant les rançons et leur montant ne sont pas toujours connus. Par ailleurs, l'ANSSI ne dispose pas d'informations permettant d'estimer les éventuels revenus générés par la vente de données exfiltrées.

Cependant, des estimations sont possibles, par le biais notamment de l'étude des mouvements financiers sur les portefeuilles de cryptomonnaies dont les adresses sont mentionnées dans les demandes de rançon. Le suivi de ces transactions permet d'affirmer que les revenus générés se comptent en millions de dollars. Par exemple, de mars à juillet 2020, Netwalker aurait généré 25 millions de dollars, **tandis que Ryuk aurait accumulé 150 millions de dollars depuis ses débuts en 2018** [78].

La prolifération de groupes d'attaquants développant ce genre d'opérations d'extorsion s'explique donc par une rentabilité bien supérieure au coût de mise en œuvre des attaques.

Cette rentabilité est d'ailleurs favorisée par des assurances cyber souscrites par les victimes, dont la couverture du risque consiste simplement à payer la rançon [40].

Certaines sociétés se sont également spécialisées dans le paiement des rançons en proposant des services de négociation et de médiation entre la victime et l'attaquant. Les opérateurs du rançongiciel DarkSide sont d'ailleurs les premiers à avoir permis à ce type de société de s'enregistrer sur leur site de divulgation de données afin d'obtenir des rabais sur la rançon de leur client, en fonction du nombre de rançons déjà payées pour d'autres clients [79], officialisant une pratique déjà courante.

Commentaire : Il est envisageable, au vu de quelques occurrences d'attaques par rançongiciel à l'encontre du secteur assu-

rantiel sur la période 2019-2020, que les attaques à son encontre se démocratisent, notamment dans l'optique d'identifier les clients ayant souscrit une assurance cyber. A ce titre, il est intéressant de constater que l'entreprise d'ingénierie ST Engineering, cliente de l'assurance Chubb elle-même victime de Maze en mars 2020, a par la suite été la cible des mêmes attaquants, qui en ont publié les données. Chubb a pu constituer un rebond ayant permis aux attaquants d'atteindre au moins l'un de ses clients.

8 Conclusion

Les revenus générés par les attaques par rançongiciel et l'émergence d'assurances et de sociétés de négociation validant leur modèle économique suggère que **le phénomène rançongiciel continuera à croître dans les années à venir.** Plus précisément, la multiplication des campagnes de *Big Game Hunting* est favorisée par les efforts des cybercriminels pour s'assurer du paiement de la rançon (ciblage d'entités financièrement solides, recherche de la rupture d'activité, exfiltration de données, moyens de pression).

L'augmentation du nombre d'attaques par rançongiciel est également liée à l'augmentation du nombre d'attaquants, facilitée par le modèle du RaaS ainsi que par un écosystème cybercriminel fournissant un support à tout moment de la chaîne d'infection.

Les attaques à l'encontre d'ESN illustrent le danger d'un impact systémique des rançongiciels qui, en ciblant des entreprises sous-traitantes ou clés d'un secteur d'activité, pourraient être amenées un jour à déstabiliser plusieurs grands groupes (*supply chain attack*), un pan d'activité économique entier (rupture dans l'approvisionnement de matière première par exemple) ou encore une zone géographique spécifique.

Les attaques à l'encontre d'hôpitaux montrent également qu'une attaque par rançongiciel peut avoir des conséquences dans le monde réel, en mettant en danger la vie des patients. Cette incidence forte dans la sphère physique s'illustre également par la perte d'exploitation, parfois définitive, de nombre d'entreprises victimes, ainsi que par l'exfiltration de données sensibles ou confidentielles pouvant mettre en péril des réputations, des opérations de fusions-acquisitions, des projets en cours voire même la sécurité nationale, dans le cas par exemple d'attaques ciblant des sous-traitants du secteur de la défense.

Les attaques par rançongiciel ne peuvent donc plus être reléguées au rang de simples attaques à visée lucrative, étant donné que leur sophistication, leur intérêt pour les données de la victime ainsi que la perte de continuité d'activité qu'elles engendrent, les rapprochent d'attaques à visée d'espionnage ou de sabotage mises en œuvre par des attaquants de niveau étatique.

Les rançongiciels sont d'ailleurs à la portée d'attaquants de niveau étatique ou de type hacktiviste, afin de monétiser leur intrusion en guise de motivation secondaire, d'effacer leurs traces, ou encore dans une logique déstabilisatrice. Ces attaquants ont aussi la possibilité de louer les services de cybercriminels et de consulter ou d'acheter les données qu'ils exfiltrent.

Afin d'éviter qu'une attaque par rançongiciel atteigne l'organisation ou de réduire les conséquences d'une telle attaque, un guide de sensiblisation "Attaques par rançongiciels, tous concernés - Comment les anticiper et réagir en cas d'incident ?" est disponible sur le site de l'ANSSI [77].

9 Annexes : principaux rançongiciels du moment

9.1 DoppelPaymer

En avril 2019, Evil Corp se serait scindé en deux groupes : Indrik Spider et Doppel Spider (alias Gold Heron). Doppel Spider opérerait une version modifiée de Dridex, nommé DoppelDridex, ainsi qu'une variante du rançongiciel BitPaymer, DoppelPaymer. Il mènerait aussi bien des campagnes de fraudes bancaires *via* DoppelDridex, que des campagnes de rançonnage *via* DoppelPaymer [33].

D'après Avast, DoppelPaymer fonctionnerait sur un modèle d'affiliés [17].

Les vecteurs d'infection impliqués dans la distribution de DoppelPaymer seraient des points d'eau distribuant FakeUpdates, puis Dridex et DoppelPaymer, des courriels d'hameçonnage [17], l'exploitation de vulnérabilités de serveurs Citrix non mis à jour [21] et des accès RDP mal sécurisés [17].

DoppelPaymer pourrait également être distribué par le botnet Dridex [80], le service de distribution Emotet ainsi que par le cheval de Troie bancaire QakBot [81].

En matière de post compromission, les attaquants utiliseraient Powershell Empire, Cobalt Strike ou Koadic [82], élèveraient leurs privilèges *via* Mimikatz [70] et déploieraient manuellement le rançongiciel [83]. L'extension des fichiers chiffrés est .locked ou .doppeled [84].

Doppel Spider a introduit un site de divulgation de données (*Dedicated Leak Site* ou DLS) en février 2020 [85]. Auparavant, les opérateurs de DoppelPaymer avaient déclaré avoir déjà exfiltré les données de leurs victimes à des fins de revente, dans le but d'augmenter la rentabilité de leurs attaques, malgré le non paiement de rançons [58].

Un compte Twitter, @DoppelPaymer [86], lui serait associé.

De février à septembre 2020, les données d'au moins 40 victimes ont été publiées sur le site de *leak* de DopplePaymer [85].

9.2 Egregor

Un mémo sur le rançongiciel Egregor est disponible sur le site du CERT-FR [38].

Egregor [38] fonctionne sous le modèle économique du *Ransomware-as-a-Service* (RaaS). Il est issu de la famille de logiciels malveillants Sekhmet, découverte en mars 2020.

Les organisations ciblées sont victimes de chantage à la divulgation de données : en cas de non-paiement de la rançon sous trois jours, les opérateurs menacent de publier les fichiers dérobés sur un site Internet dédié. Afin de faire pression sur les victimes, les opérateurs peuvent également menacer de communiquer une partie des informations dérobées aux médias.

Egregor serait liée à la fin d'activité du groupe d'attaquants à l'origine du rançongiciel Maze. En conséquence, de nombreux affiliés se seraient mis à utiliser Egregor. De plus, certains opérateurs d'autres logiciels malveillants, tel que ceux du code malveillant Qakbot privilégieraient dorénavant l'utilisation d'Egregor en tant que charge finale, au détriment de Prolock.

De nombreuses victimes d'Egregor sont localisées aux États-Unis et appartiennent aux secteurs des services et de l'industrie manufacturière.

Peu d'éléments sont connus pour le moment à propos du ou des vecteurs d'infection utilisés. Néanmoins, il semblerait que les attaquants utilisent des courriels d'hameçonnage avec une pièce-jointe contenant une macro malveillante ainsi que des accès RDP compromis.

Le cheval de Troie bancaire Qakbot serait actuellement utilisé pour distribuer Egregor ainsi que le rançongiciel Prolock. Dans au moins un cas, les opérateurs d'Egregor auraient utilisé des documents Microsoft Excel imitant les documents chiffrés DocuSign et le détournement d'échanges par courriel (*Email Thread Hijacking*) afin de distribuer Qakbot.

Les chevaux de Troie Ursnif et IcedID auraient également été utilisés par les opérateurs d'Egregor.

Les outils SharpHound ou AdFind auraient été utilisés durant la phase de latéralisation au sein de l'*Active Directory* (AD). Pour se déplacer au sein du réseau, les opérateurs d'Egregor utiliseraient des balises SMB *via* l'outil Cobalt Strike ou des accès administrateurs. Les charges utiles de Cobalt Strike peuvent être déobfusquées à l'aide de l'outil *CyberChef*. Les connexions avec le serveur de commande et de contrôle se font *via* le protocole HTTPS.

Le client de l'outil *RClone* permettrait aux opérateurs d'exfiltrer les données à des fins de chantage et de divulgation.

L'outil en ligne de commande Bitsadmin aurait été utilisé pour télécharger et exécuter la dll malveillante d'Egregor. La charge utile est injectée dans un processus « iexplore.exe » et débute le chiffrement.

Les domaines "egregor-support.com" et "egregorsup.com" permettent d'entrer en contact afin de déchiffrer des fichiers et/ou de négocier avec les opérateurs. Les domaines "newsegregor.com" et "egregoranrmzapcv.onion" sont utilisés pour divulguer les données.

9.3 Netwalker

Apparu en août 2019, le rançongiciel Netwalker (a.ka. Mailto, Mailto2, KoKo, Kokoklock, KazKavKozKiz) [46, 87, 88, 89, 90, 91] fonctionnerait depuis mars 2020 selon le modèle du RaaS (*Ransomware-as-a-Service*). Il est déployé au cours d'attaques ciblées de type *Big Game Hunting*. Depuis mai 2020, un site TOR expose les données exfiltrées par le rançongiciel. Netwalker aurait généré 25 millions de dollars entre mars et juillet 2020.

Netwalker a eu recours à différents vecteurs d'infection par le passé :

- Des courriels d'hameçonnage, exploitant parfois la thématique du Coronavirus. D'autres courriels d'hameçonnage auraient parfois été envoyés à partir du carnet d'adresses de l'utilisateur compromis (T1566);
- Rejeu massif de mots de passe (*password spraying*) (T1110);
- Compromission d'accès RDP (T1586);
- L'exploitation d'une vulnérabilité Telerik CVE-2019-18935, Tomcat ou Weblogic.

Durant la phase d'exécution, des éléments indiquent que les attaquants sont capables de mobiliser les techniques et outils suivants :

- PowerShell scripts (T1027, T1140, T1059);
- psexec (T1105);
- Windows Command Shell (T1059);
- Utilisation des API Windows pour l'injection DLL (T1106).

En matière d'élévation de privilèges, Netwalker a exploité par le passé les vulnérabilités CVE-2020-0796 (SMBv3), CVE-2019-1458 (Win32k), CVE-2017-0213 (Windows COM Marshaler), CVE-2015-1701 (Win32k).

Les opérateurs de Netwalker auraient utilisé différents outils permettant l'évasion de la défense parmi lesquels :

- Fileless loading;
- Eset AV remover;
- Gordon's Eset password recovery;
- Trend Micro's Security Agent Uninstall Tool;
- Microsoft Security Client uninstall.

Netwalker utiliserait l'injection de code en mémoire pour augmenter sa furtivité (*reflective dynamic-link library*

injection) (T1106, T1055, T1082). Ainsi, aucun binaire du rançongiciel n'est stocké sur le disque.

Les jetons d'identification présents sur la machine de la victime sont utilisés pour tenter d'accéder aux autres réseaux afin d'en chiffrer également le contenu. Les opérateurs de Netwalker ont recours aux logiciels Mimikatz, Mimidogz et Mimikittenz. Ils utilisent également : Windows Credentials Editor, pwdump, NLBrute, LaZagne et WinPwn (T1003).

Durant la phase d'exploration du réseau, les attaquants privilégieraient les outils suivants : Soft Perfect Network Scanner, NLBrute et Bloodhound.

Enfin, les outils suivants auraient été utilisés par les attaquants afin de se latéraliser dans le système d'information : psexec, Teamviewer et Anydesk (T1570, T1569).

Netwalker détruit toutes les copies fantômes présentes sur le système *via* des commandes vssadmin (T1490, T1047, T1489) afin d'empêcher l'utilisateur de restaurer son système.

Netwalker termine tous les processus blacklistés ainsi que ceux utilisant des fichiers ciblés par le chiffrement (T1562, T1518). A l'issue du chiffrement, les fichiers chiffrés sont renommés en ajoutant « mailto » à leur nom.

Le rançongiciel supprime ensuite ses fichiers de configuration ainsi que l'entrée RUN éradiquant ainsi les traces de son existence (T1112).

La demande de rançon est personnalisée en fonction de la victime. Des adresses emails de contacts sont fournies dans la demande de rançon, ainsi qu'un lien accessible *via* TOR. Le montant de la rançon est adapté aux revenus de l'entreprise ou de l'individu ciblé (entre 1 000 et 3 000 000 dollars, payable en Bitcoin) et double au bout d'une semaine.

Le 27 janvier 2021, une opération coordonnée des autorités américaines, canadiennes et bulgares a permis la saisie d'un serveur ainsi que l'arrestation et l'inculpation d'un ressortissant canadien, affilié de NetWalker.

9.4 RagnarLocker

Apparu en décembre 2019, RagnarLocker (alias Ragnar) est un rançongiciel développé en C et en C++, déployé dans le cadre d'attaques ciblées de type *Big Game Hunting* [23]. Il est mis à disposition de différents groupes d'attaquants selon le modèle du RaaS.

Depuis ses débuts, RagnarLocker a employé différents vecteurs d'infection :

- exploitation de vulnérabilités liées à des serveurs Citrix [23, 24].;
- déploiement d'une machine virtuelle sur le poste ciblé. Par exemple, RagnarLocker a déjà été téléchargé à l'intérieur d'une machine virtuelle (VM) Oracle VirtualBox Windows XP, le but étant d'éviter la détection par le logiciel anti-virus installé sur la machine physique [20];
- exploitation de vulnérabilités de logiciels de gestion à distance (RMM) généralement utilisés par des prestataires en services informatiques, afin d'infecter l'un de leurs clients [23];
- exploitation d'accès RDP mal sécurisés [20];
- courriels d'hameçonnage [10].

Les opérateurs de RagnarLocker utilisent des outils classiques pour se latéraliser dans le réseau de la victime.

Afin de faire pression sur les victimes, les données exfiltrées par les attaquants sont publiées sur le site de *leak* associé au rançongiciel.

Parmi les victimes françaises de RagnarLocker, se trouvent l'acteur majeur du secteur du transport maritime français CMA-CGM [92] ainsi que Dassault Falcon Jet, filiale de Dassault Aviation [93].

9.5 Ryuk

Un mémo sur le rançongiciel Ryuk est disponible sur le site du CERT-FR [29].

Le rançongiciel Ryuk [29] a été observé pour la première fois en août 2018. C'est une variante du rançongiciel Hermes 2.1, vendu sur le forum souterrain exploit.in à partir de février 2017 par le groupe cybercriminel CryptoTech pour environ 400 dollars.

Ryuk n'a pas la capacité de se latéraliser automatiquement au sein d'un réseau, d'où la nécessité d'un accès *via* une première charge utile ou d'une latéralisation manuelle.

Ryuk se compose d'un *dropper*, déposant sur le poste de la victime l'une des deux versions d'un module de chiffrement de données (32 ou 64 bit). Le *dropper* exécute ensuite la charge utile. Après quelques minutes d'inactivité, Ryuk cherche alors à arrêter plus de 40 processus et 180 services, notamment ceux liés aux logiciels antivirus, aux bases de données et aux sauvegardes. Il assure sa persistance par la création d'une clé de registre.

L'utilisation d'une combinaison de l'algorithme de chiffrement symétrique (AES) et de l'algorithme de chiffrement asymétrique (RSA) permet aussi bien de chiffrer les fichiers que de protéger la clé de chiffrement, rendant les données indéchiffrables par un tiers.

Après analyse récursive des disques et partages réseau dans le système infecté puis injection de sa charge malveillante au sein de processus fiables, Ryuk chiffre tous les fichiers, à l'exception de certains fichiers Windows, Mozilla, Chrome et Ahnlab .

Les navigateurs Internet ainsi que les composants de base du système d'exploitation sont laissés intacts pour permettre aux victimes de lire la demande de rançon, d'acheter des cryptomonnaies et de payer la rançon. Il arrive cependant que Ryuk chiffre des fichiers de base Windows ce qui implique le difficile voire impossible *reboot* des machines compromises.

Ryuk ajoute l'extension .RYK aux fichiers chiffrés et dépose le fichier RyukReadMe.txt dans les répertoires chiffrés.

Depuis octobre 2019, Ryuk dispose d'une fonctionnalité lui permettant d'allumer les postes éteints présents sur le réseau local (*Wake-on-LAN*) afin d'accroître sa surface de chiffrement.

Il détruit ensuite toutes les copies fantômes présentes sur le systèmes *via* des commandes vssadmin ou le lancement d'un fichier .bat [8] afin d'empêcher l'utilisateur de restaurer son système.

Ryuk ne dispose pas de fonctionnalité d'exfiltration de données ni de site Internet dédié à la divulgation des données des victimes, à la différence d'autres rançongiciels.

Ryuk est à l'origine de la compromission de nombreuses entités depuis août 2018, qu'il cible pour leur rentabilité et leur capacité à payer des rançons de montants élevés (*Big Game Hunting*).

Bien qu'aucun ciblage sectoriel spécifique ne puisse être identifié, il apparaît cependant que Ryuk cible particulièrement les États-Unis et le Canada.

En octobre 2020, Ryuk aurait été responsable de 75% des attaques sur le secteur américain de la santé, secteur qu'il attaquerait depuis le premier semestre 2019.

Selon Prevailion, au 3 novembre 2020, environ 1400 entités communiquaient avec des serveurs de commande et contrôle (C2) Cobalt Strike associés à UNC1878, l'un des utilisateurs de Ryuk. Ces entités seraient des hôpitaux américains et des agences gouvernementales, des entreprises pharmaceutiques ainsi que des universités dans le reste du monde.

TrickBot a représenté le *loader* distribuant le plus Ryuk. TrickBot peut être distribué en amont par le *Malware-as-a-Service* Emotet. Les chaînes d'infection Emotet-TrickBot-Ryuk et TrickBot-Ryuk ont ainsi été couramment ren-

8. Extension d'un fichier de commandes MS-DOS permettant de concevoir des scripts, utilisés ici pour des tâches de maintenance telles que la suppression de fichier.

contrées, et perdurent au moins jusqu'à septembre en 2020. Le vecteur d'infection apparaît généralement être un courriel d'hameçonnage délivrant soit Emotet, soit TrickBot.

En mars 2020, les chaînes d'infection impliquant TrickBot auraient été moins nombreuses, voire auraient momentanément cessé. En juillet 2020, la chaîne d'infection Emotet-TrickBot émerge de nouveau, après plusieurs mois d'inactivité d'Emotet. Cette chaîne distribue alors alternativement les rançongiciels Ryuk et Conti. A partir de mi-septembre 2020, la chaîne d'infection BazarLoader-Ryuk semble remplacer les chaînes d'infection impliquant TrickBot.

D'autres chaînes d'infection et groupes d'attaquants associés ont été identifiés impliquant le groupe cybercriminel FIN6, le code malveillant Buer ou encore le code malveillant SilentNight.

9.6 Sodinokibi

Le rançongiciel Sodinokibi (également appelé REvil et Sodin)[94, 95, 96, 5, 97, 98] a été détecté pour la première fois en avril 2019, lors d'une attaque exploitant la vulnérabilité *0-Day* Oracle WebLogic CVE-2019-2725 [99].

Suite aux nombreux articles faisant le lien entre GandCrab et Sodinokibi et aux interrogations d'autres cybercriminels, les attaquants développant et commercialisant Sodinokibi ont déclaré être d'anciens affiliés de GandCrab ayant acheté le code source.

Sodinokibi est vendu en tant que RaaS sur certains forums cybercriminels russophones (notamment exploit.in) en tant que Ransomware-as-a-Service (RaaS) par l'identité numérique « UNKN » depuis mai 2019 [5].

A l'inverse de GandCrab, qui n'imposait pas de condition particulière pour adhérer à son modèle de vente, Sodinokibi a choisi de limiter fortement le nombre d'affiliés, de leur imposer un niveau d'activité élevé, et d'interdire tout affilié anglophone. Le groupe derrière Sodinokibi cherche également des profils d'affiliés particuliers, notamment spécialisés dans la compromission ciblée de réseaux d'entreprises [5].

Le code de chiffrement est, dans la très grande majorité des cas, téléchargé par un script (.bat) déposé sur la machine victime par l'attaquant. Ce script récupère la charge sur le site « `pastebin.com` » et l'éxécute au travers d'un script Powershell [100].

En début d'exécution, Sodinokibi cherche à créer un mutex respectant la structure « Global\[A-Z0-9]8-[A-Z0-9]4-[A-Z0-9]4-[A-Z0-9]4-[A-Z0-9]12 ». Si celui-ci existe déjà, le code cesse de s'exécuter [95]. Ce mutex change pour chaque compilation du code de chiffrement, et chaque compilation est généralement associée à une victime [9]. Ainsi, la création préalable de ce mutex sur une machine d'un réseau dont certaines ont déjà été chiffrées peut empêcher le code de s'exécuter sur celles encore saines.

Comme beaucoup d'autres rançongiciels, Sodinokibi réalise des vérifications afin de ne pas chiffrer des machines situées dans certains pays ou utilisées par des locuteurs de certaines langues. Pour cela, il vérifiera que la valeur de « `GetKeyboardLayoutList` » ne correspond pas à une valeur contenue dans une liste prédéfinie associée à de nombreuses langues de pays d'ex-URSS, ainsi que les langues roumaine, persane ou encore azéri [101].

Sodinokibi assure sa persistance par la création d'une clé de registre dans LocalMachine, sinon CurrentUser : « `[HKLM|HKCU]\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\[code]` » ou [code] est une valeur alphanumérique dépendant des paramètres de compilation [102].

Des données de configuration sont aussi stockées de cette façon (« `[HKLM|HKCU]\SOFTWARE\recfg` »), ce qui peut servir à qualifier si une machine a été compromise par un code Sodinokibi [95].

Sodinokibi exploite la CVE-2018-8453 pour élever ses privilèges sur la machine infectée, si la configuration du code le précise (variable de configuration « `exp` »). Cette vulnérabilité n'affecte que les systèmes Windows non mis à jour depuis 2018. Si « `exp` » a pour valeur False, le code tentera tout de même d'élever ses privilèges en s'exécutant avec la commande « runas » ayant pour effet de déclencher l'UAC [95].

9. L'ANSSI a toutefois constaté la réutilisation d'un même mutex chez deux victimes différentes en juin 2020.

Avant le chiffrement, Sodinokibi cherchera à neutraliser (« kill ») un certain nombre de processus et services associés à des logiciels antiviraux et des applications métiers ou bureautique afin de maximiser ses chances d'exécution et de chiffrement. Il effacera également les copies cachés Windows (VSS) en commande directe [95].

Le site Internet « Happy Blog » associé à Sodinokibi facilite la divulgation des données que les affiliés pourraient avoir exfiltrées. Ce site contient également une partie réservée aux enchères.

A la connaissance de l'ANSSI, des milliers de particuliers et d'entreprises sont victimes chaque mois d'attaques impliquant Sodinokibi. Si la plupart de ces victimes ne sont pas connues, les attaques ayant eu un impact important ou celles assorties de divulgation de données ont été rapportées dans différentes médias. La demande de rançon la plus importante associée à Sodinokibi est établie à 42 millions de dollars, pour la compromission du cabinet d'avocats américain Grubman Shire Meiselas & Sacks en mai 2020.

La France n'est pas épargnée par les affiliés de Sodinokibi et représente, à la connaissance de l'ANSSI, un des pays les plus touchés derrière les États-Unis, la Chine et possiblement la Corée du Sud.

9.7 WastedLocker

Malgré la mise en accusation de M. Yakubets et d'autres membres d'Evil Corp, l'activité du groupe cybercriminel ne semble pas avoir été troublée, au vu de la poursuite des campagnes BitPaymer. Cette continuité des incidents relatifs à BitPaymer s'étend jusqu'en mars 2020. A partir de mai 2020, il apparaît qu'Evil Corp utilise un nouveau rançongiciel, WastedLocker [67, 103, 15, 14, 13].

WastedLocker, en plus de partager quelques similarités avec BitPaymer, tirerait certaines de ses fonctionnalités du code source fuité en 2015 de Gozi ISFB.

A partir de mai et l'apparition de WastedLocker, le vecteur d'infection privilégié d'Evil Corp apparaît être FakeUpdates, bien qu'il est possible qu'au moins un autre vecteur d'infection existe.

La victime visite un site légitime compromis. Une fausse mise à jour de navigateur apparaît sur son poste, et télécharge un fichier ZIP contenant le fichier JavaScript malveillant FakeUpdates. Ce dernier déploie Cobalt Strike. *Via* Cobalt Strike, WMI, PsExec ou encore Mimikatz, les attaquants élèvent alors leurs privilèges, se latéralisent et identifient d'autres systèmes sur lesquels déployer leur rançongiciel. Ces étapes sont réalisées manuellement (pas de scripts ou autres méthodes d'automatisation).

PsExec (ou plus rarement SecTool) est ensuite utilisé pour désactiver Windows Defender, et lance WastedLocker. Les fichiers locaux, distants et stockés sur des disques externes sont chiffrés.

Certaines caractéristiques des attaques impliquant WastedLocker sont :

- Chaque échantillon, demande de rançon, extension de fichier et clé publique RSA de WastedLocker est créé spécifiquement pour chaque victime.
- WastedLocker est protégé par un *custom crypter* et s'autodéchiffre lorsqu'il est propagé par PsEsxec dans le SI de la victime. Ce *custom crypter* est également utilisé par le rançongiciel Netwalker ainsi que par les chevaux de Troie bancaires Gozi ISFB v3, Zloader et Smokeloader.
- WastedLocker ne dispose pas de fonction d'exfiltration de données mais des données pourraient être exfiltrées via Cobalt Strike. Malgré le fait que WastedLocker ne dispose pas de site de *leak* associé, il reste envisageable que des données soient exfiltrées.
- Lorsqu'une version de WastedLocker est détectée sur les réseaux d'une victime, Evil Corp met à jour la version pour la rendre indétectable, puis continue son attaque.
- Dans un cas, Evil Corp a compromis sa cible six mois après avoir échoué à élever ses privilèges dans le SI.
- Les domaines de courriels de contact des attaquants sont protonmail, tutanota, eclipso et airmail.
- Le montant des rançons s'échelonne de 500 000 dollars à 10 millions.

De la même manière que BitPaymer, WastedLocker présente un ciblage privilégié des Etats-Unis. Le rançongiciel a ciblé de grandes entreprises de divers secteurs dont principalement l'industrie, la technologie, les médias et les télécommunications. Dans une moindre mesure, il a affecté les secteurs de l'énergie, du transport, de la finance, de

l'hôtellerie et de la santé. Parmi les victimes, se trouvent onze entreprises cotées dont huit appartenant aux 500 premières entreprises américaines (classement Fortune 500).

Commentaire : La France ayant été ponctuellement ciblée par Evil Corp depuis 2019 par le biais du rançongiciel BitPaymer, il est envisageable que WastedLocker compromette des entités françaises à l'avenir.

10 Bibliographie

[1] Secure List. *Targeted Ransomware : It's Not Just about Encrypting Your Data !* 11 novembre 2020.
URL : https://securelist.com/targeted-ransomware-encrypting-data/99255/.

[2] Digital Shadows. *DarkSide : The New Ransomware Group behind Highly Targeted Attacks*. 22 septembre 2020.
URL : https://www.digitalshadows.com/blog-and-research/darkside-the-new-ransomware-group-behind-highly-targeted-attacks/.

[3] Palo Alto. *When Threat Actors Fly Under the Radar : Vatet, PyXie and Defray777*. 6 novembre 2020.
URL : https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/.

[4] Security Affairs. *Group-IB Hi-Tech Crime Trends 2020/2021 Report*. 25 novembre 2020.
URL : https://securityaffairs.co/wordpress/111434/cyber-crime/hi-tech-crime-trends.html.

[5] McAfee. *Episode 2 The All-Stars - Analyzing Affiliate Structures in Ransomware-as-a-Service Campaigns*. 1er octobre 2019.

[6] Advanced Intel. *Inside "Phobos" Ransomware : "Dharma" Past & Underground*. 24 juillet 2020.
URL : https://www.advanced-intel.com/post/inside-phobos-ransomware-dharma-past-underground.

[7] Malwarebytes Labs. *A Deep Dive into Phobos Ransomware*. 24 juillet 2019.
URL : https://blog.malwarebytes.com/threat-analysis/2019/07/a-deep-dive-into-phobos-ransomware/.

[8] ZDNet. *Linux Version of RansomEXX Ransomware Discovered*. 6 novembre 2020.
URL : https://www.zdnet.com/article/linux-version-of-ransomexx-ransomware-discovered/.

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

[10] Cybersecurity Insiders. *Ransomware Attack Makes CWT Pay $4.5 Million in Bitcoins to Hackers*. 4 août 2020.
URL : https://www.cybersecurity-insiders.com/ransomware-attack-makes-cwt-pay-4-5-million-in-bitcoins-to-hackers/.

[11] Sentinel Labs. *Ranzy Ransomware | Better Encryption Among New Features of ThunderX Derivative*. 18 novembre 2020.
URL : https://labs.sentinelone.com/ranzy-ransomware-better-encryption-among-new-features-of-thunderx-derivative/.

[12] ANSSI. *Le Groupe Cybercriminel TA505*. 22 juin 2020.
REDMINE : https://projets.ops.fr/issues/1032015.

[13] DarkTrace. *Evil Corp Intrusions : WastedLocker Ransomware Detected by Darktrace*. 19 août 2020.
URL : https://www.darktrace.com/en/blog/evil-corp-intrusions-wasted-locker-ransomware-detected-by-darktrace.

[14] Malwarebytes Labs. *WastedLocker, Customized Ransomware*. 10 juillet 2020.
URL : https://blog.malwarebytes.com/threat-spotlight/2020/07/threat-spotlight-wastedlocker-customized-ransomware/.

[15] NCC Group. *WastedLocker : A New Ransomware Variant Developed By The Evil Corp Group*. 23 juin 2020.
URL : https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group/.

[16] Group-IB. *RANSOMWARE UNCOVERED : ATTACKERS' LATEST METHODS*. 27 mai 2020.
URL : https://go.group-ib.com/rs/689-LRE-818/images/Group-IB_Ransomware_Uncovered_whitepaper_eng.pdf?mkt_tok=eyJpIjoiTkdabFl6UmhZVE0xWVdNNSIsInQiOiJiZkFnZWRpM3c2aHpTdEM0bmh3a0Q5UmN
3D.

[17] Avast. *DoppelPaymer Ransomware Resurgence*. 24 août 2020.
URL : https://blog.avast.com/doppelpaymer-ransomware-resurgence-avast.

[18] Sentinel Labs. *Meet NEMTY Successor, Nefilim/Nephilim Ransomware*. 4 mai 2020.
URL : https://labs.sentinelone.com/meet-nemty-successor-nefilim-nephilim-ransomware/.

[19] ZDNet. *Israeli Companies Targeted with New Pay2Key Ransomware*. 6 novembre 2020.
URL : https://www.zdnet.com/article/israeli-companies-targeted-with-new-pay2key-ransomware/.

[20] Sophos. *Ragnar Locker Ransomware Deploys Virtual Machine to Dodge Security*. 21 mai 2020.
URL : https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/.

[21] Bleeping Computer. *DoppelPaymer Hacked Bretagne Télécom Using the Citrix ADC Flaw*. 27 février 2020.
URL : https://www.bleepingcomputer.com/news/security/doppelpaymer-hacked-bretagne-t-l-com-using-the-citrix-adc-flaw/.

[22] Trend Micro. *Investigation into a Nefilim Attack Shows Signs of Lateral Movement, Possible Data Exfiltration*. 3 avril 2020.
URL : https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/investigation-into-a-nefilim-attack-shows-signs-of-lateral-movement-possible-data-exfiltration.

[23] Bleeping Computer. *Ragnar Locker Ransomware Targets MSP Enterprise Support Tools*. 10 février 2020.
URL : https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomware-targets-msp-enterprise-support-tools/.

[24] [TLP:RED] FireEye. *FireEye Blog : Nice Try : 501 (Ransomware) Not Implemented*. 24 janvier 2020.
URL : https://intelligence.fireeye.com/reports/20-00001604.

[25] Bleeping Computer. *LockBit Ransomware Moves Quietly on the Network, Strikes Fast*. 21 octobre 2020.
URL : https://www.bleepingcomputer.com/news/security/lockbit-ransomware-moves-quietly-on-the-network-strikes-fast/.

[26] CERT NZ. *Active Ransomware Campaign Leveraging Remote Access Technologies*. 16 juin 2020.
URL : https://www.cert.govt.nz/it-specialists/advisories/active-ransomware-campaign-leveraging-remote-access-technologies/.

[27] ENISA. *ENISA Threat Landscape 2020 - Ransomware*. 23 octobre 2020.
URL : https://www.enisa.europa.eu/publications/ransomware.

[28] The DFIR report. *Ryuk Speed Run, 2 Hours to Ransom*. 5 novembre 2020.
URL : https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/.

[29] ANSSI. *Mémo Sur Le Rançongiciel Ryuk*. 30 novembre 2020.
redmine : https://projets.ops.fr/issues/1034471.

[30] Group-IB. *The Locking Egregor*. 23 novembre 2020.
URL : https://www.group-ib.com/blog/egregor.

[31] Hornetsecurity. *QakBot Malspam Leading to ProLock : Nothing Personal Just Business*. 16 juin 2020.
URL : https://www.hornetsecurity.com/en/security-information/qakbot-malspam-leading-to-prolock/.

[32] McAfee. *Nemty Ransomware - Learning by Doing*. 2 avril 2020.
URL : /blogs/other-blogs/mcafee-labs/nemty-ransomware-learning-by-doing/.

[33] ANSSI. *Le Code Malveillant Dridex : Origines et Usages*. 28 mai 2020.
redmine : https://projets.ops.fr/issues/1031872.

[34] Dell Secureworks. *GOLD DUPONT*. 27 novembre 2020.
URL : https://www.secureworks.com/research/threat-profiles/gold-dupont.

[35] Microsoft. *Microsoft Digital Defense Report 2020*. 29 septembre 2020.

[36] Sophos. *Netwalker Ransomware Tools Give Insight into Threat Actor*. 27 mai 2020.
URL : https://news.sophos.com/en-us/2020/05/27/netwalker-ransomware-tools-give-insight-into-threat-actor/.

[37] FireEye. *Unhappy Hour Special : KEGTAP and SINGLEMALT With a Ransomware Chaser*. 28 octobre 2020.
URL : https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html.

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

[39] Microsoft Security. *Ransomware Groups Continue to Target Healthcare, Critical Services; Here's How to Reduce Risk*. 28 avril 2020.
URL : https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/.

[40] FinCEN. « FinCEN Advisory, FIN-2020-A006 ». 1er octobre 2020.
URL : https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2020-a006.

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

[42] GROUP-IB. *Lock Like a Pro : Dive in Recent ProLock's Big Game Hunting*. 30 septembre 2020.
URL : https://www.group-ib.com/blog/prolock_evolution.

[43] FIREEYE. *Financially Motivated Actors Are Expanding Access Into OT : Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families*. 15 juillet 2020.
URL : https://www.fireeye.com/blog/threat-research/2020/07/financially-motivated-actors-are-expanding-access-into-ot.html.

[44] CROWDSTRIKE. *WIZARD SPIDER Adds New Features to Ryuk*. 1er novembre 2019.

[45] BLEEPING COMPUTER. *DarkSide : New Targeted Ransomware Demands Million Dollar Ransoms*. 21 août 2020.
URL : https://www.bleepingcomputer.com/news/security/darkside-new-targeted-ransomware-demands-million-dollar-ransoms/.

[46] CARBONBLACK. *MailTo (NetWalker) Ransomware*. 7 février 2020.
URL : https://www.carbonblack.com/2020/02/07/threat-analysis-unit-tau-threat-intelligence-notification-mailto-netwalker-ransomware/.

[47] BANK INFO SECURITY. *Alert : « Ryuk » Ransomware Attacks the Latest Threat*. 7 septembre 2018.
URL : https://www.bankinfosecurity.com/alert-ryuk-ransomware-attacks-latest-threat-a-11475.

[48] KASPERSKY. *LockBit Ransomware —What You Need to Know*. 30 septembre 2020.
URL : https://www.kaspersky.com/resource-center/threats/lockbit-ransomware.

[49] TWITTER. *@malwrhunerteam*. 8 janvier 2021.
URL : https://twitter.com/malwrhunterteam/status/1347458694053822464.

[50] CYWARE. *SunCrypt Ransomware Takes Extortion Threats to Next Level*. 5 octobre 2020.
URL : https://cyware.com/news/suncrypt-ransomware-takes-extortion-threats-to-next-level-47205250.

[51] ZDNET. *Ransomware Gangs Are Now Cold-Calling Victims If They Restore from Backups without Paying*. 8 janvier 2021.
URL : https://www.zdnet.com/article/ransomware-gangs-are-now-cold-calling-victims-if-they-restore-from-backups-without-paying/.

[52] THE NATIONAL LAW REVIEW. *Sodinokibi Hackers Switch Payment Mechanism to Monero*. 16 avril 2020.
URL : https://www.natlawreview.com/article/sodinokibi-hackers-switch-payment-mechanism-to-monero.

[53] US DEPARTMENT OF TREASURY. *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*. 1er octobre 2020.
URL : https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

[54] ZDNET. *Ransomware : le Trésor américain traite les victimes en collaborateurs*. 2 octobre 2020.
URL : https://www.zdnet.fr/actualites/ransomware-le-tresor-americain-traite-les-victimes-en-collaborateurs-39910677.htm.

[55] COMPLYADVANTAGE. *6AMLD : délits préalables dans les médias defavorables*. 1er janvier 2020.
URL : https://complyadvantage.com/fr/base-des-connaissances/couverture-mediatique-negative/6amld-22-delits-prealables-dans-les-medias-defavorables/.

[56] COMPLYADVANTAGE. *La 6ème directive anti-blanchiment (6AMLD) : Ce que vous devez savoir*. 1er janvier 2020.
URL : https://complyadvantage.com/fr/base-des-connaissances/la-6eme-directive-anti-blanchiment-6amld-ce-que-vous-devez-savoir/.

[57] THREATPOST. *Egregor Ransomware Threatens 'Mass-Media' Release of Corporate Data*. 2 octobre 2020.
URL : https://threatpost.com/egregor-ransomware-mass-media-corporate-data/159816/.

[58] BLEEPING COMPUTER. *DoppelPaymer Ransomware Sells Victims' Data on Darknet If Not Paid*. 3 février 2020.
URL : https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-sells-victims-data-on-darknet-if-not-paid/.

[59] ZATAZ. *Ransomware : trois groupes de pirates lancent des enchères aux données volées*. 16 octobre 2020.
URL : https://www.zataz.com/ransomware-trois-groupes-de-pirates-lancent-des-encheres-aux-donnees-volees/.

[60] BLEEPING COMPUTER. *REvil Ransomware Creates eBay-like Auction Site for Stolen Data*. 2 juin 2020.
URL : https://www.bleepingcomputer.com/news/security/revil-ransomware-creates-ebay-like-auction-site-for-stolen-data/.

[61] Trend Micro. « Shifts in Underground Markets : Past, Present, and Future ». 20 mai 2020.

[62] ANSSI. *Le Code Malveillant Emotet : Origines et Usages*. 27 octobre 2020.
redmine : https://projets.ops.fr/issues/1033690.

[63] Hack Fence. *Meet the World's Biggest 'Bulletproof' Hoster*. 17 juillet 2019.
url : https://www.hackfence.com/w/meet-the-worlds-biggest-bulletproof-hoster/.

[64] Medium. *5 Features Making EmerDNS the Only Truly Decentralized DNS*. 20 février 2020.
url : https://medium.com/@emer.tech/5-features-making-emerdns-the-only-truly-decentralized-dns-4c513bb13850.

[65] Health Sector Cybersecurity Coordination Center (HC3). *Recent BazarLoader Use in Ransomware Campaigns*. 2 octobre 2020.
url : https://www.hhs.gov/sites/default/files/bazarloader.pdf.

[66] Checkpoint. *Global Surges in Ransomware Attacks*. 6 octobre 2020.
url : https://blog.checkpoint.com/2020/10/06/study-global-rise-in-ransomware-attacks/.

[67] Symantec. *WastedLocker : Symantec Identifies Wave of Attacks Against U.S. Organizations*. 26 juin 2020.
url : https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wastedlocker-ransomware-us.

[68] ZDNet. *Charleville-Mézières : le groupe DoppelPaymer diffuse les données volées*. 23 juin 2020.
url : https://www.zdnet.fr/actualites/charleville-mezieres-le-groupe-doppelpaymer-diffuse-les-donnees-volees-39905603.htm.

[69] AP News. *Report : Ransomware Disables Georgia County Election Database*. 23 octobre 2020.
url : https://apnews.com/article/virus-outbreak-elections-georgia-voting-2020-voting-c191f128b36d1c0334c9d0b173daa18c.

[70] Bleeping Computer. *Pennsylvania County Pays 500K Ransom to DoppelPaymer Ransomware*. 29 novembre 2020.
url : https://www.bleepingcomputer.com/news/security/pennsylvania-county-pays-500k-ransom-to-doppelpaymer-ransomware/.

[71] Checkpoint. *Attacks against Healthcare Organizations Spike Globally as COVID-19 Cases Rise Again*. 5 janvier 2021.
url : https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/.

[72] Bleeping Computer. *Lorien Health Services Discloses Ransomware Attack Affecting Nearly 50,000*. 20 juillet 2020.
url : https://www.bleepingcomputer.com/news/security/lorien-health-services-discloses-ransomware-attack-affecting-nearly-50-000/.

[73] Data Breaches. *Pennsylvania Health System Hit by NetWalker Ransomware*. 19 juin 2020.
url : https://www.databreaches.net/pennsylvania-health-system-hit-by-netwalker-ransomware/.

[74] SudOuest. *Marmande : l'hôpital attaqué par des cyberpirates*. 7 juillet 2020.
url : https://www.sudouest.fr/2020/07/07/marmande-l-hopital-attaque-par-des-cyberpirates-7636731-3755.php.

[75] Bloomberg. *Hackers Bearing Down on U.S. Hospitals Have More Attacks Planned*. 30 octobre 2020.
url : https://www.bloomberg.com/news/articles/2020-10-30/hackers-bearing-down-on-u-s-hospitals-have-more-attacks-planned.

[76] Bleeping Computer. *Sopra Steria Expects €50 Million Loss after Ryuk Ransomware Attack*. 25 novembre 2020.
url : https://www.bleepingcomputer.com/news/security/sopra-steria-expects-50-million-loss-after-ryuk-ransomware-attack/.

[77] ANSSI. *Attaques Par Rançongiciels, Tous Concernés*. 1er septembre 2020.
url : https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf.

[78] ZDNet. *Ransomware : Ryuk Aurait Empoché plus de 150 Millions de Dollars*. 8 janvier 2021.
url : https://www.zdnet.fr/actualites/ransomware-ryuk-aurait-empoche-plus-de-150-millions-de-dollars-39915797.htm.

[79] @malwrhunterteam. *MalwareHunterTeam sur Twitter*. 8 janvier 2020.
url : https://twitter.com/malwrhunterteam/status/1347458694053822464.

[80] ZDNet. *The Malware That Usually Installs Ransomware and You Need to Remove Right Away*. 20 novembre 2020.
URL : https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/.

[81] Medium. *Qbot/QakBOT Spam Campaigns with a Dangerous Payload*. 17 avril 2020.
URL : https://medium.com/csis-techblog/qbot-qakbot-spam-campaigns-with-a-dangerous-payload-d87ab653cd72.

[82] Financial Cert. *Fake Microsoft Teams updates lead to Cobalt Strike deployment*. 10 novembre 2020.
URL : https://www.financialcert.tn/2020/11/10/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/.

[83] Intel 471. *Ransomware-as-a-Service : The Pandemic within a Pandemic*. 16 novembre 2020.
URL : https://public.intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/.

[84] Proficio. *DoppelPaymer Ransomware during COVID-19 | Proficio Threat Intel*. 7 mai 2020.
URL : https://www.proficio.com/doppelpaymer-ransomware/.

[85] Crowdstrike. *Ransomware + Data Leak Extortion : Origins and Adversaries, Pt. 1*. 24 septembre 2020.
URL : https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/.

[86] Twitter. *@DoppelPaymer*. 2 décembre 2020.
URL : https://twitter.com/DoppelPaymer.

[87] McAfee. *Take a "NetWalk" on the Wild Side*. 3 août 2020.
URL : /blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side/.

[88] INCIBE-CERT. *NetWalker Ransomware : Analysis and Preventative Measures*. 8 avril 2020.
URL : https://www.incibe-cert.es/en/blog/netwalker-ransomware-analysis-and-preventative-measures.

[89] Trustwave. *An In-Depth Look at MailTo Ransomware, Part One of Three*. 31 mars 2020.
URL : https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/an-in-depth-look-at-mailto-ransomware-part-one-of-three/.

[90] Trustwave. *An In-Depth Look at MailTo Ransomware, Part Two of Three*. 8 avril 2020.
URL : https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/an-in-depth-look-at-mailto-ransomware-part-two-of-three/.

[91] Trustwave. *An In-Depth Look at MailTo Ransomware Part Three of Three*. 10 avril 2020.
URL : https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/an-in-depth-look-at-mailto-ransomware-part-three-of-three/.

[92] Le Mag IT. *Ransomware : CMA-CGM victime de la piraterie de Ragnar Locker*. 28 septembre 2020.
URL : https://www.lemagit.fr/actualites/252489714/Ransomware-CMA-CGM-victime-de-la-piraterie-de-Ragnar-Locker.

[93] ZDNet. *Dassault Falcon Jet Aux Prises Avec Le Groupe Ragnar Locker*. 15 décembre 2020.
URL : https://www.zdnet.fr/actualites/dassault-falcon-jet-aux-prises-avec-le-groupe-ragnar-locker-39914955.htm.

[94] Cybereason. *Sodinokibi - The Crown Prince of Ransomware*. 5 août 2019.
URL : https://www.cybereason.com/blog/the-sodinokibi-ransomware-attack.

[95] Dell Secureworks. *REvil/Sodinokibi Ransomware*. 24 septembre 2019.
URL : https://www.secureworks.com/research/revil-sodinokibi-ransomware.

[96] McAfee. *Episode 1 What the Code Tells Us*. 2 octobre 2019.

[97] McAfee. *McAfee ATR Analyzes Sodinokibi Aka REvil Ransomware-as-a-Service - Follow The Money*. 14 octobre 2019.
URL : https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-follow-the-money/.

[98] McAfee. *McAfee ATR Analyzes Sodinokibi Aka REvil Ransomware-as-a-Service - Crescendo*. 20 octobre 2019.
URL : https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-crescendo/.

[99] Cisco Talos. *Sodinokibi Ransomware Exploits WebLogic Server Vulnerability*. 30 avril 2019.
URL : http://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html.

[100] KPN. *Tracking REvil*. 28 janvier 2020.
URL : https://www.kpn.com/security-blogs/tracking-revil.htm.

[101] Acronis. *Taking Deep Dive into Sodinokibi Ransomware*. 3 juillet 2019.
URL : https://www.acronis.com/en-us/articles/sodinokibi-ransomware/.

[102] INCIBE-CERT. *Sodinokibi : Features and Operation*. 6 avril 2020.
URL : https://www.incibe-cert.es/en/blog/sodinokibi-features-and-operation.

[103] Sentinel Labs. *WastedLocker Ransomware : Abusing ADS and NTFS File Attributes*. 23 juillet 2020.
URL : https://labs.sentinelone.com/wastedlocker-ransomware-abusing-ads-and-ntfs-file-attributes/.

4.3 - 2021-09-01

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