TLP:WHITE

ÉTAT DE LA MENACE RANÇONGICIEL

À L'ENCONTRE DES ENTREPRISES ET INSTITUTIONS

3.2

05/02/2020

TLP:WHITE

Sommaire

1 Synthèse

Un rançongiciel est un code malveillant empêchant la victime d'accéder au contenu de ses fichiers afin de lui extorquer de l'argent. Ce document se concentre sur **les rançongiciels s'appuyant sur des capacités de chiffrement de fichiers et opérés à des fins lucratives.** Il en existe des centaines de variantes.

L'année 2018 a vu la multiplication d'attaques par rançongiciel impactant des entreprises et institutions dans le monde entier, et elles dépassent désormais en nombre celles impactant les particuliers. **Ces codes malveillants 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. Sur les très nombreuses attaques de ce type en France, l'ANSSI a traité 69 incidents en 2019 sur son périmètre.

Si la grande majorité des attaques par rançongiciels s'avère être opportunistes et s'appuie essentiellement sur la faible maturité en sécurité numérique de leurs victimes, l'ANSSI et ses partenaires observent depuis 2018 de plus en plus de groupes cybercriminels cibler spécifiquement des entreprises financièrement robustes dans le cadre d'attaques dites **« Big Game Hunting »**, parfois menées en combinaison avec d'autres codes malveillants (cryptomineurs, trojan bancaires). Elles sont réalisées par des groupes d'attaquants aux ressources financières et aux compétences techniques importantes, et présentent **un niveau de sophistication parfois équivalent aux opérations d'espionnages informatiques opérées par des États.** Alors que les montants de rançons habituels s'élèvent à quelques centaines ou milliers de dollars, celles demandées lors des attaques « Big Game Hunting » sont à la mesure de la cible et peuvent **atteindre des dizaines de millions de dollars**. **Depuis fin 2019, l'ANSSI constate également que certains groupes cybercriminels cherchent à faire pression sur leurs victimes en divulguant des données internes préalablement exfiltrées du système d'information infecté.**

Par ailleurs, la campagne d'attaque Wannacry de 2017 a montré que la combinaison d'un rançongiciel et d'un moyen de propagation automatique pouvait occasionner d'immenses dégâts économiques. S'appuyant sur un code sophistiqué mais exploitant une vulnérabilité logicielle connue faisant déjà l'objet d'une mise à jour de sécurité, **l'impact de Wannacry aurait pu être fortement limité par une meilleure politique de mise à jour logicielle des entreprises dans le monde.**

Les groupes d'attaquants opérant ces rançongiciels s'appuient sur un important écosystème cybercriminel générant deux milliards de dollars de bénéfices annuels [1]. Il permet aux attaquants de sous-traiter une grande partie des actions pour mener à bien leurs opérations d'extorsion et d'y acheter les ressources nécessaires (données personnelles, accès légitimes compromis, codes malveillants).

Si les montants des rançons peuvent varier fortement en fonction des rançongiciels employés et des victimes impactées, les bénéfices générés sont estimés entre quelques millions et plus d'une centaine de millions de dollars par groupe d'attaquants. Le coût de mise en oeuvre de ces opérations est plus difficile à estimer, mais ne s'élève pas à plus de quelques dizaines, voire centaines de milliers de dollars sur l'ensemble de la période d'activité malveillantes.

Les rançongiciels représentant un risque non négligeable de rupture d'activité, de nombreuses assurances proposent de le couvrir. Cette couverture consiste souvent en ce que l'assureur paye tout ou partie de la rançon. Des sociétés se sont développées autour de ce paiement des rançons en proposant des services de négociation avec les attaquants. Aujourd'hui, les assurances incitent les victimes à payer la rançon qui s'avère souvent moins élevée que le coût d'un rétablissement de l'activité sans le recours à la clé de déchiffrement. Pour autant cette couverture n'empêche pas les victimes d'être attaquées de nouveau. **Cette incitation à payer valide le modèle économique des cybercriminels et les amène déjà à augmenter les rançons et à multiplier leurs attaques.**

Les attaques contre Altran et NorskHydro montrent le danger d'un impact systémique des rançongiciels sur un secteur d'activité qui, en ciblant des entreprises sous-traitantes ou clés du secteur, pourraient amener un jour à le déstabiliser. Les attaques contre le laboratoire forensique Eurofins et certains départements de police américains montrent également que les cybercriminels peuvent entraver des investigations judiciaires. Si l'objectif restait lucratif, **il est tout à fait envisageable que des groupes cybercriminels (ou le crime organisé en général) s'appuient un jour sur ce moyen pour faire pression sur la justice.**

2 Périmètre d'analyse

Un rançongiciel est un code malveillant empêchant la victime d'accéder au contenu de ses fichiers afin de lui extorquer de l'argent. Historiquement, les attaquants détournaient des fonctionnalités du système d'exploitation afin de bloquer l'utilisateur face à une page de rançon [2]. Désormais, la très grande majorité des rançongiciels ont la capacité de chiffrer des fichiers stockés sur le réseau de la victime.

Ce chiffrement de fichiers, appliqué à l'ensemble d'un réseau informatique, a montré ces dernières années sa capacité à bloquer l'activité de nombreuses entreprises et institutions et à générer des coûts de remédiation très importants. En mai 2019, la ville de Baltimore a vu ses réseaux paralysés par une attaque de ce type et a évalué le préjudice financier à 18 millions de dollars, dont dix pour la remise en état du parc informatique [3].

Ce document se concentre sur l'analyse des attaques par chiffrement à finalité lucrative et leur impact sur les entreprises et institutions. Il ne prend pas en compte les rançongiciels ne s'appuyant pas sur le chiffrement de fichiers, ainsi que les codes de sabotage prenant l'apparence de rançongiciel mais n'étant pas distribués dans une logique lucrative.

3 Typologie des attaques par rançongiciels

Il existe actuellement plusieurs dizaines, voire centaines, de familles de rançongiciels utilisés lors d'attaques informatiques plus ou moins sophistiquées. Certaines n'entrainent que le chiffrement des données d'une seule machine, d'autres sont en mesure de chiffrer l'ensemble des ressources d'un réseau, supprimer les copies cachées, voire atteindre les systèmes de sauvegardes [4].

Les rançongiciels représentent la menace informatique actuelle la plus sérieuse pour les entreprises et institutions, par le nombre d'attaques quotidiennes et leur impact potentiel sur la continuité d'activité. Les rançongiciels représentent également en 2019 le sujet le plus discuté sur les forums d'attaquants informatiques, démontrant l'intérêt de la communauté cybercriminelle pour ce type de code et son retour sur investissement [5].

Du point de vue de l'attaquant, l'impact général des attaques par rançongiciel dépend de plusieurs facteurs :

- l'efficacité ou le nombre de méthodes d'infection employées par les attaquants pour compromettre les réseaux des victimes ;
- l'ampleur des campagnes de distribution du code ;
- la capacité du code à se propager au sein du réseau victime afin de chiffrer un maximum de ressources (fichiers) ;
- la robustesse du chiffrement des fichiers, que ce soit par l'algorithme de chiffrement choisi, la qualité de son implémentation dans le code malveillant ou encore la capacité de l'attaquant à protéger sa clé de déchiffrement des investigations des forces de police[1].

En fonction de ces facteurs, il est possible de catégoriser les attaques par rançongiciels selon trois types : les campagnes d'attaques non ciblées, les campagnes massives automatiques, et enfin les attaques ciblées dites « Big Game Hunting ».

3.1 Vastes campagnes d'attaques non ciblées

L'année 2014 a vu un accroissement important du nombre de rançongiciels possédant des fonctionnalités de chiffrement de fichiers[2]. De vastes campagnes d'infections indiscriminées , disséminées par simple hameçonnage (ou

[1] Par exemple en louant son infrastructure de commande et contrôle (C2) auprès d'un hébergeur dit « *bulletproof* », c'est à dire peu ou pas collaboratif avec les forces de police

[2] Même s'il est possible de trouver des cas bien plus anciens, notamment le célèbre *AIDS Trojan* de 1989.

vulgaire *spam*), ont été menées par des groupes cybercriminels et ont impacté de très nombreuses entreprises et institutions, mais avant tout des particuliers.

Cette méthode d'attaque non ciblée est connue en source ouverte sous les noms *Fire and Forget* ou encore *Spray and Pray*, mettant en exergue leur faible coût de mise en oeuvre ainsi que leur faible sophistication.

Elles reposent essentiellement sur trois éléments pour espérer amener une victime à payer :

- l'ampleur de la campagne d'infection ;
- l'absence de protection numérique des cibles, l'attaque ne reposant généralement pas sur des moyens sophistiqués ;
- la présence **fortuite** de fichiers suffisamment importants sur l'ordinateur de la victime.

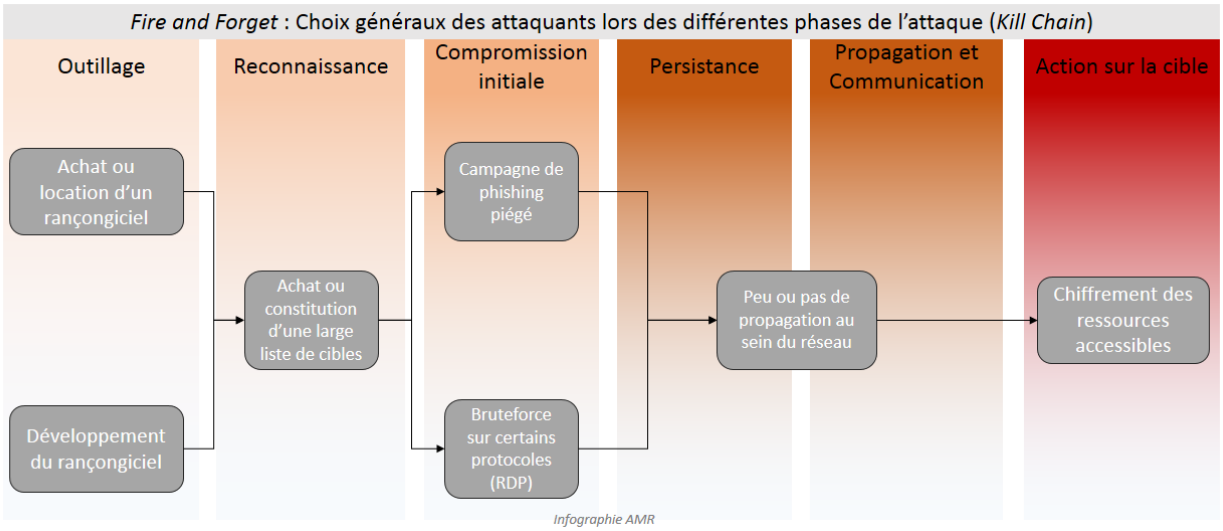

Fig. 3.1 : Les attaques non ciblées mettent rarement en oeuvre des capacités évoluées de propagation au sein des réseaux victimes.

S'il n'existe pas de chiffres fiables sur le taux de victimes payant la rançon lors de ce type d'attaques non ciblées [6], il est généralement admis qu'il est très faible (autour de 1%). Dans tous les cas, les attaquants ont réalisé beaucoup d'efforts ces dernières années pour affiner leurs méthodes d'attaques afin de s'assurer de la présence de ressources importantes sur les machines compromises et de la capacité financière de leurs cibles à payer des rançons de plus en plus élevées (Voir 3.3). **Notamment, ils utilisent désormais des listes d'adresses de messagerie professionnelle en vente sur les marchés noirs afin de diriger leur campagne d'hameçonnage sur des employés et ainsi compromettre des machines susceptibles de contenir des données importantes** [7]. Symantec rapporte ainsi pour le début 2019 une baisse générale de 20% des infections par rançongiciel, mais une hausse de 12% à l'encontre des entreprises [8]. En juillet 2019, des groupes cybercriminels ont également cherché à compromettre directement des systèmes de stockage de données en réseau (NAS) exposés sur Internet ou faiblement protégés [4, 9].

En baisse depuis 2018, ces campagnes *Fire and Forget* représentent encore la majorité des attaques par raçongiciel et constituent donc une menace pour les entreprises et institutions peu ou pas protégées numériquement. En août 2019, l'éditeur MalwareBytes a fourni des données comparatives entre les attaques impactant les particuliers et celles ciblant les entreprises, montrant une forte progression de ces dernières [10]. Certains rapports mentionnent également une augmentation de ce type d'attaque à l'encontre des plateformes mobiles [11].

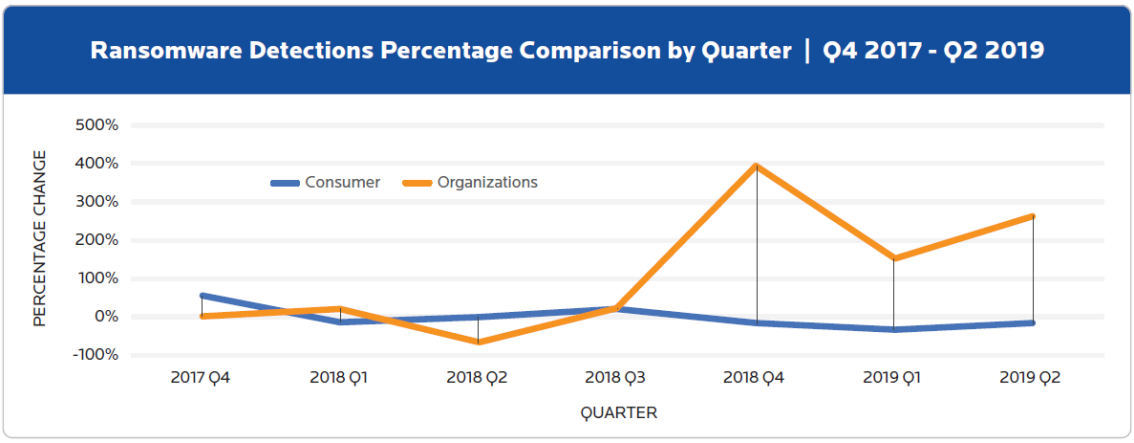

Fig. 3.2 : Comparatif de l'évolution du nombre d'attaques par rançongiciels impactant les particuliers et les entreprises. Source : MalwareBytes

3.2 Les campagnes d'attaques massives à propagation automatique

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. En France, l'attaque obligeait notamment l'entreprise Renault à arrêter par mesure de précaution plusieurs sites de production [12]. Au Royaume-Uni, plusieurs entités du *National Health Service* étaient touchées et des services d'urgences arrêtés. Le coût pour le système de santé anglais sera plus tard évalué à 100 millions d'euros [13].

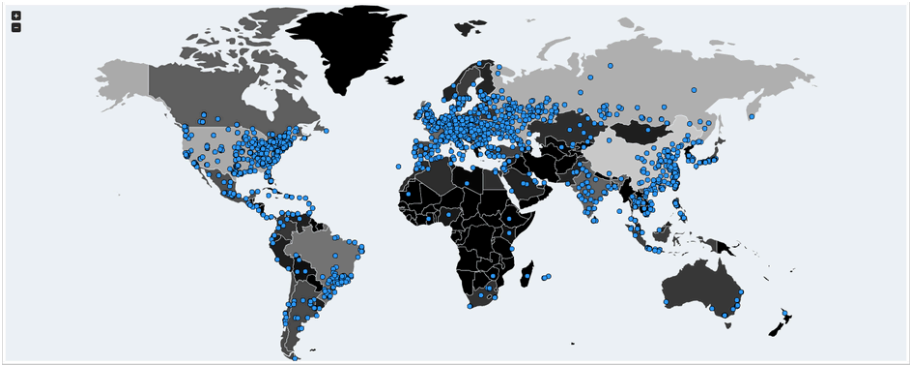

Fig. 3.3 : Compromissions par Wannacry recencées à travers le monde. Source : MalwareTech

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. Une fois une machine d'un réseau d'entreprise ou d'institution compromise, Wannacry pouvait se propager au sein du réseau en exploitant, entre autres, la même vulnérabilité à la façon d'un ver informatique, expliquant l'impact massif de cette campagne d'attaques.

Le code comprenait également une fonctionnalité dite *Killswitch* permettant à l'attaquant d'éviter que le ver, sinon incontrôlable, n'atteigne ses propres systèmes. Cette fonctionnalité a été découverte dès le premier jour de l'attaque et a ainsi permis de stopper sa propagation.

Il est important de retenir plusieurs éléments :

- la vulnérabilité exploitée était connue et Microsoft avait publié un correctif deux mois plus tôt. La propagation massive de Wannacry a été rendue possible par la **non-application du correctif** par de très nombreuses entités ;

- la combinaison d'un code de chiffrement et d'une propagation automatique peut provoquer un impact immense au niveau mondial. Cette combinaison a été réutilisée lors de la campagne de sabotage NotPetya contre l'Ukraine, également en 2017.

À la connaissance de l'ANSSI, il n'existe pas d'autre cas d'attaque à but lucratif de ce type. **Si dans le futur une attaque équivalente survenait, la qualité de la politique de mise à jour logicielle des entités impactées sera un facteur majeur dans la réduction de l'impact de l'attaque.**

3.3 Big Game Hunting : Attaques informatiques ciblées

Depuis 2018, 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. Ces attaques ciblées sont connues en source ouverte sous le nom de « Big Game Hunting ». Elles mettent en oeuvre des méthodes et techniques auparavant réservées à des opérations d'espionnage informatique opérées par des attaquants étatiques (exploitation de vulnérabilité 0-day, propagation manuelle et furtive).

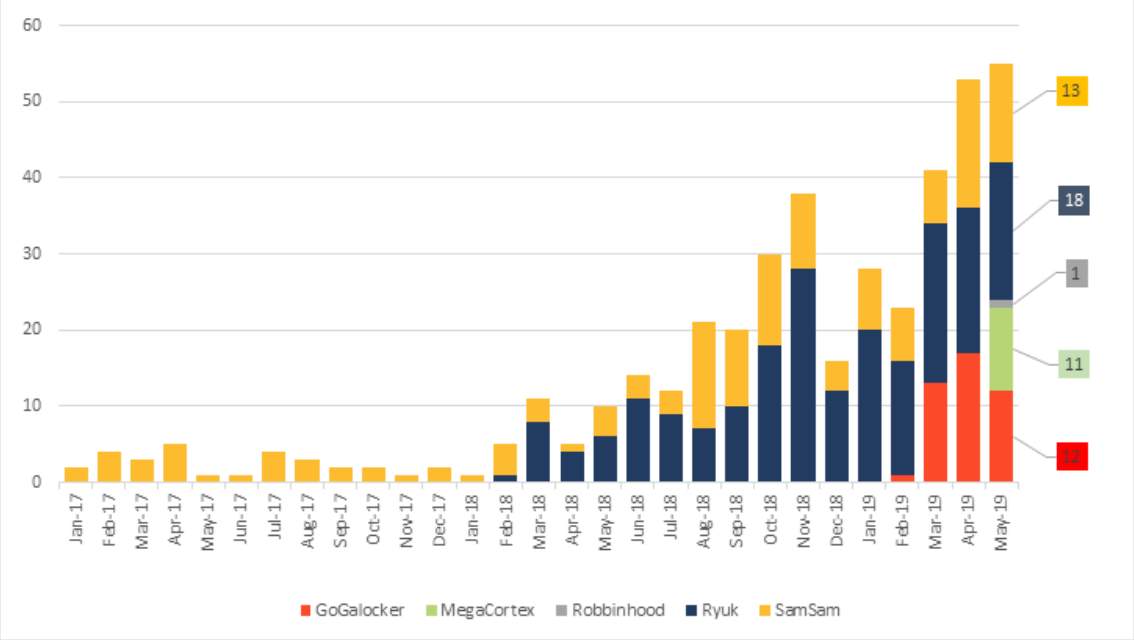

Fig. 3.4 : Multiplication des attaques impliquant certains rançongiciels utilisés pour du Big Game Hunting. Source : Symantec

Afin de s'assurer de revenus substantiels, ces groupes sont désormais en mesure de préparer leurs opérations d'extorsion plusieurs mois à l'avance et ciblent spécifiquement des grandes entreprises ou institutions identifiées comme capables de payer de larges sommes d'argent [14, 15]. Ces attaques ciblées 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 façon furtive ;
- la capacité de l'attaquant à identifier et chiffrer les ressources clés de la cible ;
- la capacité financière de la cible à payer d'importantes rançons.

Afin de compromettre les réseaux ciblés, les cybercriminels peuvent employer de très nombreuses méthodes d'infection (compromission d'accès à distance, hameçonnage ciblé, exploitation de vulnérabilité logicielle, compromission

de sous-traitants, compromission de sites Internet légitime, etc.). Toutefois, la compromission d'accès RDP[3] et l'hameçonnage ciblé restent les méthodes les plus largement employées [16].

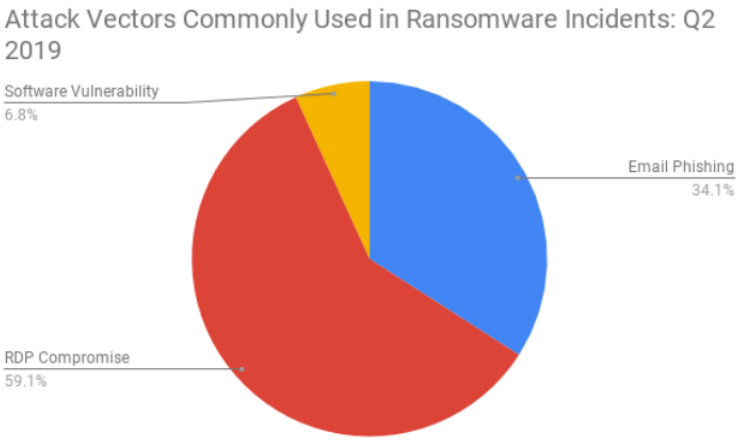

Fig. 3.5 : Vecteurs d'attaques utilisés pour délivrer des rançongiciels au 2ème trimestre 2019. Source : Security Boulevard

Commentaire : Les chiffres présentés ne s'appuient pas sur des données exhaustives et dépendent essentiellement des capacités de détection de la source. L'usage d'accès RDP compromis s'explique par la vente régulière de ce type d'accès sur les marchés noirs à des prix parfois dérisoires (quelques dizaines de dollars). La part importante d'hameçonnage s'explique par la nature des cibles des attaques « Big Game Hunting ». Les entreprises et institutions ont, majoritairement, une meilleure politique de mise à jour logicielle que les particuliers, mais leurs employés ont un usage professionnel des mails qui les poussent à les ouvrir s'ils paraissent suffisamment légitimes.

Dans le cadre de ces attaques ciblées, les attaquants peuvent acheter tout ou partie des ressources nécessaires pour mener leurs attaques, notamment acheter sur les marchés noirs les accès à un réseau préalablement compromis par un autre groupe cybercriminel (Voir Chapitre 5). Ainsi, un code de type Trojan bancaire ayant infecté un réseau peut aussi être utilisé ultérieurement pour distribuer un rançongiciel [17]. Le NCSC-NL, partenaire néerlandais de l'ANSSI, a ainsi constaté 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. Cette inactivité correspond très probablement à la période entre la mise en vente de l'accès compromis et son achat par un autre groupe afin de mener l'attaque.

Commentaire : le développement d'une capacité de suivi des transactions de ce type sur les marchés cybercriminels permettrait grandement d'anticiper de potentielles attaques sur des entreprises et institutions d'intérêt.

De plus, les cybercriminels s'appliquent à se propager manuellement au sein du réseau victime afin de rester discrets et atteindre les ressources identifiées comme clés, et ainsi maximiser l'impact de l'attaque.
Depuis fin 2019, certains groupes d'attaquants s'emploient à exfiltrer de grandes quantités de données présentes sur le système d'information compromis avant d'action de chiffrement[4]. Ils se servent ensuite de la divulgation de ces données afin d'exercer une pression supplémentaire sur les victimes afin de les inciter à payer la rançon. Des victimes des rançongiciels Maze et Sodinokibi ont vu certaines de leurs données divulguées dans ce cadre. Il est désormais important de prendre en compte ce nouveau risque sur la confidentialité des données qui peut notamment amener des implications importantes liées à la réglementation RGPD.

[3] Remote Desktop Protocol : protocole réseau d'administration à distance.
[4] il est intéressant de noter qu'en mai 2019, les opérateurs du rançongiciel RobbinHood avaient divulgué quelques documents appartenant à la ville de Baltimore, alors compromise par ce rançongiciel

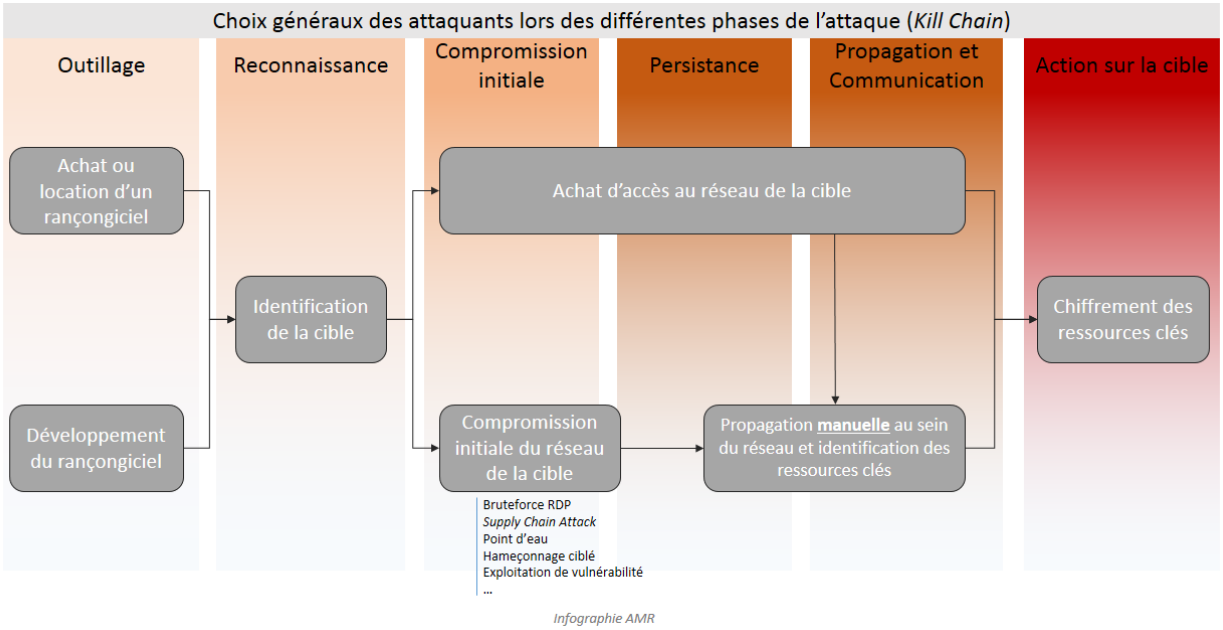

Fig. 3.6 : Les cybercriminels peuvent acheter sur le marché noir certains composants essentiels à une attaque.

Certains rançongiciels sont connus pour être employés exclusivement dans le cadre d'attaques de type « Big Game Hunting ». D'autres, disponibles sur les marchés cybercriminels par un système d'affiliation connu sous le nom de « Ransomware-As-A-Service » (notamment GandCrab, Sodinokibi, Dharma ou encore Maze), 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 (voir Chapitre 5). Toutefois, la majorité des rançongiciels reste utilisée dans le cadre d'attaques non ciblées et peu sophistiquées, plus accessibles à la majorité des groupes cybercriminels en activité.

Rançongiciel	Emploi	Annexes
SamSam	Big Game Hunting (inactif)	8.1
BitPaymer	Big Game Hunting	8.2
Ryuk	Big Game Hunting	8.3
LockerGoga	Big Game Hunting	8.4
Dharma	Mixte	8.5
GandCrab	Mixte (inactif)	8.6
Sodinokibi	Mixte	8.7
MegaCortex	Mixte	8.8
RobinHood	Big Game Hunting	8.9
Maze	Mixte	8.10
Clop	Big Game Hunting	8.11

Principaux Rançongiciels utilisés dans le cadre d'attaques « Big Game Hunting ». Source : ANSSI

4 Victimologie des attaques par rançongiciel

4.1 À l'échelle mondiale

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 oeuvre des mesures de sécurité informatique basique (sauvegardes à froid, sensibilisation à l'hameçonnage, mise à jour logicielle sur ses machines connectées, antivirus).
Concernant les attaques « Big Game Hunting » les entreprises et institutions dont l'arrêt d'activité peut amener 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 ayant suffisamment d'argent pour payer des rançons très importantes. Symantec révèle en ce sens un ciblage très majoritaire d'entités présentes aux États-Unis.

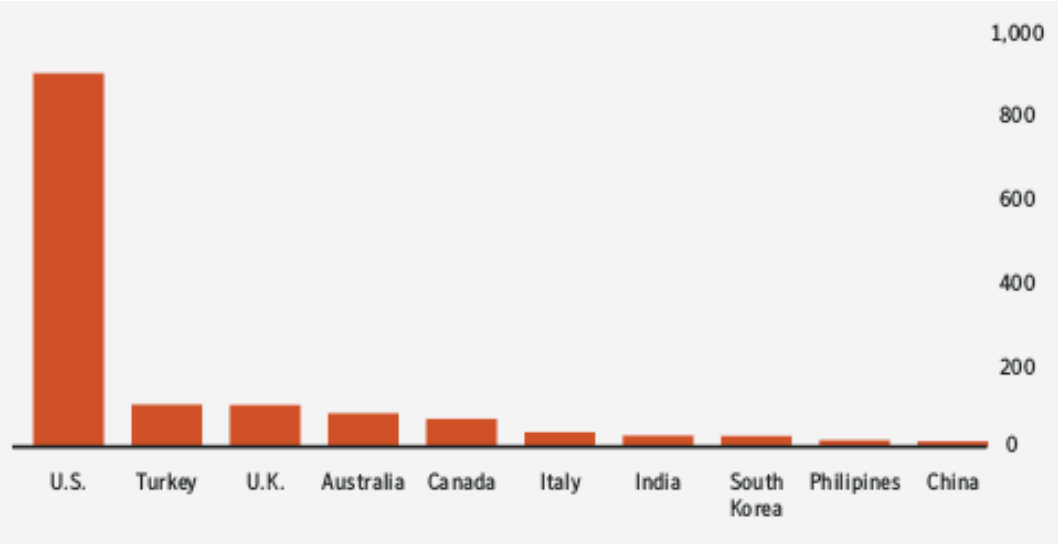

Fig. 4.1 : Répartition par pays des attaques « Big Game Hunting » détectées par Symantec ces dernières années. Source : Symantec

Commentaire : Les chiffres présentés par Symantec sont largement influencés par le positionnement de ses solutions de détection. Le marché de cet éditeur étant majoritairement américain et anglosaxon, il est normal de voir apparaitre les États-Unis comme principale cible. Malgré ce biais important, ces statistiques représentent de manière générale une réalité. Les cybercriminels considèrent les entreprises et institutions américaines comme financièrement robustes et meilleures candidates pour payer des rançons élevées.

Les attaques présentées ci-après sont particulièrement représentatives de la menace posée par les rançongiciels au niveau mondial.

4.1.1 Compromission de Norsk Hydro en mars 2019

Le 19 mars 2019, l'entreprise norvégienne spécialisée dans l'industrie de l'aluminium a été forcée d'arrêter une grande partie de son réseau et réaliser sa production « manuellement » suite à son infection par le rançongiciel LockerGoga (Voir 8.4) [14].

Possédant des sauvegardes de ses données, Norsk Hydro a fait le choix de ne pas payer la rançon [18]. La baisse de productivité due à l'attaque aura couté environ 40 millions de dollars à l'entreprise [19].

4.1.2 Compromission de la municipalité de Baltimore en mai 2019

Le 7 mai 2019, la ville de Baltimore a été victime d'une attaque par le rançongiciel RobinHood (Voir 8.9) provoquant l'indisponibilité de nombreux services, notamment la messagerie professionnelle de la ville, ses lignes téléphoniques et sa plateforme de paiement en ligne. Les cybercriminels demandaient une rançon de 100 000 dollars, soumis à un incrément de 10 000 dollars par jour une fois le délai imposé dépassé [20].

Certains médias ont annoncé que l'attaque contre Baltimore aurait été rendue possible par l'utilisation du code d'exploitation de vulnérabilité *Eternal Blue*, vraisemblablement développé par la NSA et divulgué sur Internet en 2017. Pour autant, aucune trace de ce code n'a été retrouvée lors des analyses du rançongiciel. Il apparait plus probable que les attaquants aient propagé le code de chiffrement manuellement sur le réseau, Robinhood ne possédant pas de moyens de propagation automatique [21].

Ayant refusé de payer la rançon pour le déchiffrement de ses données, la ville de Baltimore peinait encore un mois après l'attaque à rétablir l'ensemble de ses services. L'attaque aura couté 18 millions de dollars à la ville de Baltimore dont dix pour la remédiation et le reste en perte de revenus [22].

4.1.3 Compromission d'Eurofins Scientific en juin 2019

En juin 2019, les laboratoires européens de recherche Eurofins Scientific ont été compromis par un rançongiciel dont l'identité n'est pas précisée en sources ouvertes. . Eurofins Scientific a fait le choix de payer la rançon afin de déchiffrer les données [23].

Un des laboratoires d'Eurofins Scientific est le sous-traitant responsable de la moitié des analyses forensiques effectuées au profit des forces de police anglaises [24] et l'attaque a **provoqué le report de nombreuses procédures judiciaires** [25, 26].

4.1.4 Compromission de la compagnie américaine Southwire en décembre 2019

En décembre 2019, un groupe cybercriminel a annoncé avoir compromis l'entreprise américaine Southwire avec le rançongiciel Maze [27], accompagnant leur annonce de fichiers présentés comme issus de son système d'information.

Devant le silence de Southwire, les attaquants ont rapidement publié quelques documents internes sur un site Internet librement accessible. Southwire a alors intenté une action en justice contre les opérateurs de Maze pour avoir publié des données personnelles tombant sous la réglementation RGPD et le site a été fermé.

En réponse, les opérateurs de Maze ont divulgué en janvier 2020, sur un forum d'attaquants russophones, 14Gb de données issus du système d'information de Southwire [28].

Commentaires : Cette attaque illustre parfaitement une nouvelle tendance dans les attaques par rançongiciel qui sont désormais pour certaines accompagnées de divulgations de données. Surtout, les groupes cybercriminels importants sont maintenant en mesure de réagir, adapter leur mode opératoire en fonction de la situation technique mais aussi informationnelle. Il est probable que de plus en plus d'attaques par rançongiciel soient assorties de divulgations de données. Les rançongiciels Sodinokibi et Nemty ont emboité le pas de Maze en ce sens [29, 30, 31].

4.1.5 Ampleur du phénomène aux États-Unis

Un recensement des attaques par rançongiciel à l'encontre d'entités gouvernementales, médicales et éducatives ayant eu lieu aux États-Unis a été réalisé par l'entreprise de sécurité informatique PCMatic et donne un indice de l'ampleur du phénomène, qui touche par ailleurs les entreprises américaines.

Fig. 4.2 : Recensement des attaques par rançongiciels sur des entités gouvernementales américaines. Source : PCMatic.

Il est à noter également que des rançongiciels ont parfois compromis des départements de police locaux [32, 33].

4.2 En France

69 incidents relatifs à des attaques par rançongiciels ont été traités par l'ANSSI en 2019, en particulier les compromissions des sociétés ALTRAN en janvier 2019 , Fleury Michon en avril 2019 , Ramsay Générale de Santé[5] en août 2019, ou encore du CHU de Rouen en Novembre 2019 [34] .

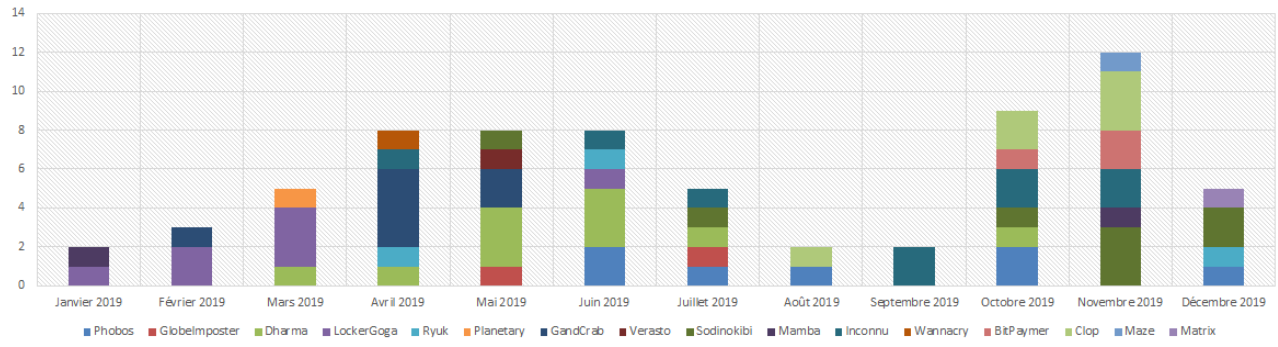

Fig. 4.3 : Incidents traités par l'ANSSI en 2019 concernant des rançongiciels.

[5] Leader de l'hospitalisation privée en France.

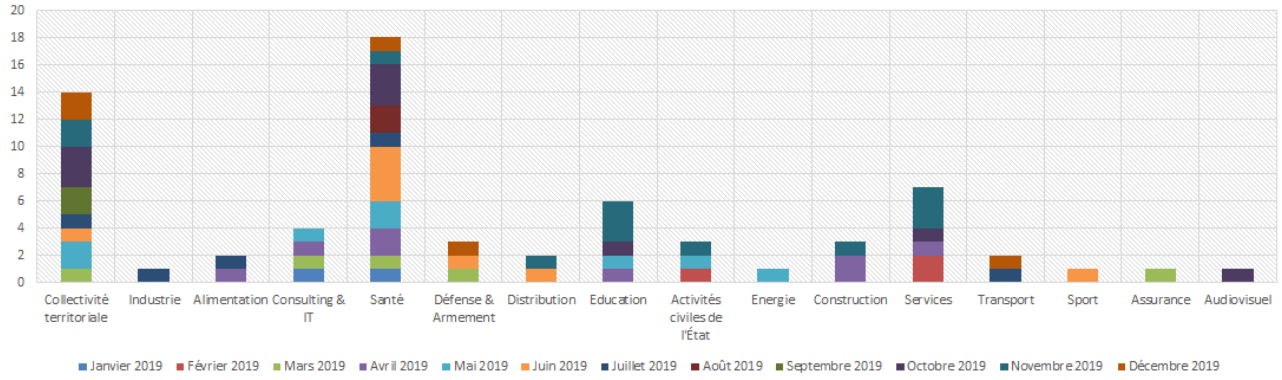

Fig. 4.4 : Secteurs d'activité ciblés par des rançongiciels dans le cadre des incidents traités par l'ANSSI.

Avec un jeu de données aussi limité, l'agence manque de visibilité directe sur l'ampleur du phénomène rançongiciel en France, notamment le nombre de victimes, leur nature ainsi que les rançongiciels ciblant majoritairement le pays. D'un point de vue quantitatif, elles ne peuvent donc pas refléter l'impact réel des rançongiciels en France. Pour autant, elles permettent de tirer deux enseignements :

- une quinzaine de rançongiciels sont concernés par ces incidents, laissant envisager que plusieurs dizaines de rançongiciels différents impactent réellement l'ensemble de l'espace économique français ;
- Les collectivités territoriales et le secteur de la santé sont majoritairement concernés par les incidents relevés. Si cela peut être essentiellement dû à la qualité des signalements d'incidents faits à l'ANSSI, cela peut également montrer l'intérêt des attaquants pour des entités réputées faiblement dotées en sécurité informatique ou dont la rupture d'activité aurait un impact social important.

Les attaques suivantes ont marqué l'année 2019 en France et sont représentatives de la menace des rançongiciels pour les intérêts français.

4.2.1 Compromission d'Altran Technologies en janvier 2019

Le 24 janvier 2019, la société française de conseil en ingénierie Altran Technologies a été victime d'une attaque par le rançongiciel LockerGoga (Voir 8.4), la forçant à déconnecter son réseau d'Internet [15]. Le code de chiffrement, peu sophistiqué et assez mal conçu, ne possédait pas de moyen de propagation en propre.

4.2.2 Compromission du CHU de Rouen en novembre 2019

Le 15 novembre 2019, le CHU de Rouen a été victime du rançongiciel Clop [34]. La compromission a eu lieu par l'ouverture d'un courriel malveillant ayant permis à l'attaquant de déployer des outils de reconnaissance et de propagation manuelle, notamment SDBBot, Metasploit, CobaltStrike ou encore Mimikatz. Ces actions manuelles lui ont permis de prendre le contrôle du domaine et de déployer dans la nuit de vendredi à samedi le code de chiffrement sur la majorité du parc informatique [35].

Les investigations de l'ANSSI ont permis d'associer l'attaque à une large campagne ciblant des universités européennes, opérée par l'important groupe cybercriminel russophone TA505 et ayant notamment touché les universités d'Anvers fin octobre et de Maastricht en décembre.

5 Écosystèmes cybercriminel et légal soutenant ces attaques

Selon une étude commandée par l'entreprise de sécurité informatique Bromium, les activités cybercriminelles correspondraient à une masse financière de plus de 1 500 milliards de dollars en 2018, des bénéfices estimés à deux

milliards de dollars annuels et un salaire pour un groupe cybercriminel moyen d'environ 900 000 dollars par an [1].

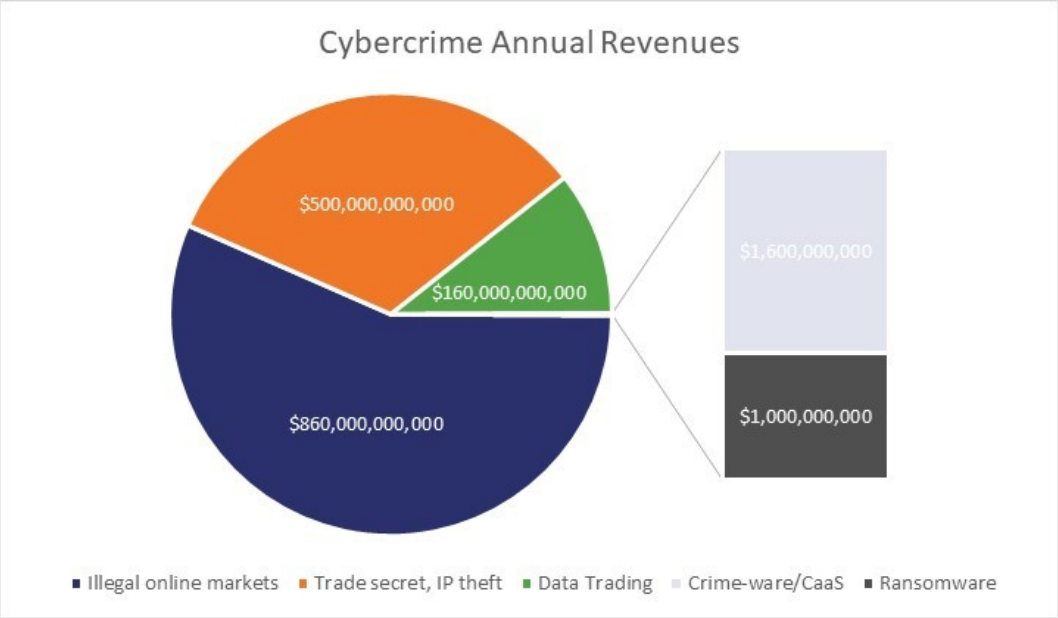

Fig. 5.1 : Masse financière pour certaines catégories d'activités cybercriminelles. Source : Bromium.

Bien que les rançongiciels ne représentent qu'un faible pourcentage de cette économie cybercriminelle, les groupes d'attaquants qui les utilisent profitent de cet écosystème constitué de vendeurs et acheteurs de biens (codes malveillants, accès compromis, données personnelles volées, etc.) et de services (location d'infrastructures de déni de service, d'infrastructures d'anonymisation, etc.).

Les attaques cybercriminelles, y compris celles ayant pour objet le rançonnage, s'organisent autour d'un cycle proche de celui des attaques ciblées réalisées par des États. **Grâce à l'existence de l'écosystème cybercriminel, les attaquants peuvent sous-traiter une grande partie des ressources et outils nécessaires à la réalisation de leurs opérations.**

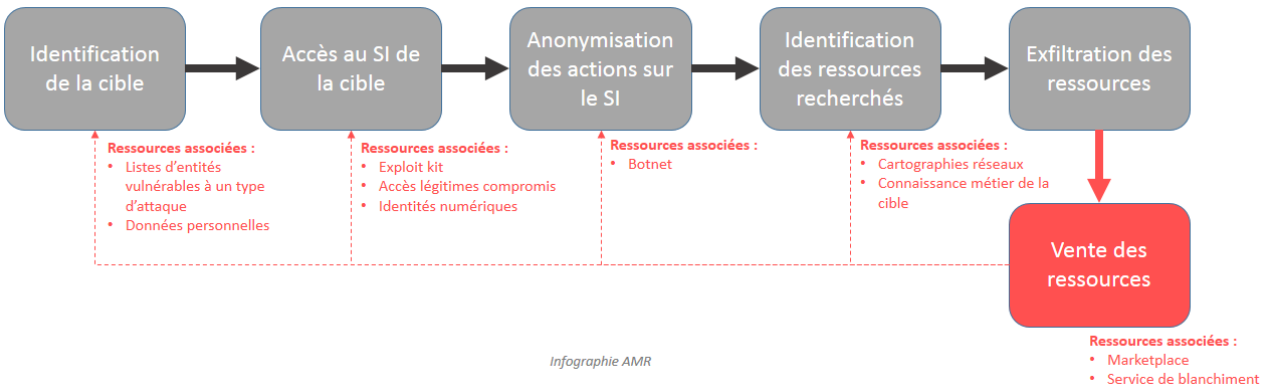

Fig. 5.2 : Différentes phases opérationnelles d'une attaque cybercriminelle.

La maturité actuelle de l'écosystème cybercriminel permet l'existence de plusieurs « offres de service » achetables sur des marchés dédiés, notamment des regroupements de données personnelles voire la reconstitution d'identité numérique, des accès à des systèmes préalablement compromis, et enfin des systèmes d'abonnements pour l'utilisation de codes malveillants [1].

5.1 Vente de données personnelles

La société de sécurité informatique Verint a détecté la circulation de 5 milliards de données (données bancaires, données d'identité, couple login/mot de passe, etc.) en 2018 sur les places de marchés cybercriminelles [36].

Les données personnelles (adresse mail, profession, numéro de sécurité sociale, etc.) servent à mener des opérations de fraudes (usurpation d'identité, fraudes aux aides sociales, etc.), mais les cybercriminels s'en servent également dans leurs manœuvres d'ingénierie sociale. L'hameçonnage ciblé, qui est un des vecteurs d'infection majeurs, s'appuie sur ce genre de données afin de personnaliser le contenu des mails malveillants et inciter les cibles à les ouvrir.

5.2 Vente d'accès compromis

De nombreuses plateformes proposent à la vente des accès compromis à des serveurs légitimes [37]. Si la plupart de ces accès concernent des serveurs de faible intérêt, certains concernent des réseaux gouvernementaux ou d'entreprises et institutions importantes [38]. Pour l'attaquant qui achète ce genre d'accès, ils représentent un moyen simple d'accéder à une cible en s'affranchissant du travail de compromission initiale.

Il est possible que FIN6, un des groupes cybercriminels opérant les rançongiciels Ryuk et LockerGoga, achètent des accès de ce type. Certaines investigations ont en effet démontré des durées d'inactivité importantes de la part de l'attaquant entre le moment de la compromission et le dépôt du code de chiffrement sur le réseau.

5.3 Ransomware-As-A-Service

Certains groupes cybercriminels proposent enfin leurs codes malveillants, notamment des rançongiciels, à la location.

Ainsi, le groupe cybercriminel Gandcrab, vendant le rançongiciel éponyme (Voir 8.6) jusqu'à mai 2019 sur le modèle Ransomware-as-a-service[39], tissait des relations commerciales avec des « affiliés » chargés de trouver et infecter des victimes selon une charte déontologique précise [40]. Pour chaque rançon payée, Gandcrab récupérait un certain pourcentage, dégressif en fonction de la durée du partenariat et du type d'abonnement. Ces partenariats n'empêchaient pas Gandcrab de réaliser lui-même certaines attaques. Le rançongiciel Sodinokibi/Revil (Voir 8.7), apparu en avril 2014, fonctionne sur le même modèle [41, 42].

5.4 Développement d'une économie légale dans le paiement de rançons

Les attaques par rançongiciel, par leur impact sur l'activité des entreprises, représentent un risque économique important et la plupart cherchent un moyen de gérer ce risque. Une façon simple de gérer un risque sur l'activité d'une entreprise est de souscrire une assurance qui le couvre. Des produits d'assurance sur le risque « cyber » se sont ainsi développés et couvrent le risque de chiffrement de données [43]. Dans certains cas, cette couverture consiste entre autres en ce que l'assurance paye la rançon [44] .

Certaines sociétés se sont également développées autour de ce paiement des rançons en proposant des services de négociations et de médiation entre la victime et l'attaquant. C'est le cas notamment de la société Coveware qui procède en toute transparence. Toutefois, certaines sociétés camouflent le fait qu'elles payent la rançon en prestations de déchiffrement des fichiers à l'aide d'expertise technique interne [45]. Pire, certaines de ces sociétés ont également développé des liens parfois étroits avec des groupes cybercriminels, notamment GandCrab, afin d'accéder à des réductions des rançons [46].

Commentaires : cette gestion du risque par le développement d'une économie autour du paiement des rançons est un phénomène inquiétant. Il valide pleinement le modèle économique développé par les attaquants, les assurant d'un plus grand nombre de paiements des rançons. Si à court terme, payer la rançon est le moyen le plus simple et souvent le moins cher de recouvrer ses données, cela ne garantit en rien qu'une attaque de la part du même groupe cybercriminel ou d'un

autre ne surviendra pas un autre jour. L'éditeur de Sophos mentionnait dans un rapport de janvier 2018 que la moitié des victimes de rançongiciels l'étaient plusieurs fois [47].

6 Coûts et revenus des attaques par rançongiciel

Les montants des rançons sont extrêmement variables, allant de quelques centaines à plusieurs millions de dollars. Les rançons à l'encontre des entreprises dans le cadre d'attaques de type « Big Game Hunting » sont toutefois régulièrement au minimum de plusieurs dizaines de milliers de dollars.

Les revenus générés par les rançongiciels peuvent être estimés au travers de l'étude des mouvements financiers sur les portefeuilles de cryptomonnaies dont les adresses sont mentionnées dans les demandes de rançons. 98% des rançons sont demandées en Bitcoin car :

- les cryptomonnaies échappent aux régulations financières habituelles ;
- les cryptomonnaies permettent des échanges anonymisés ;
- la cryptomonnaie Bitcoin est la plus répandue et donc la plus facile d'accès pour les victimes, souvent néophytes en la matière.

Le suivi de ces transactions permet d'affirmer que les revenus générés se comptent en millions de dollars[6]. Le rançongiciel SamSam aurait ainsi rapporté environ 6 millions de dollars à ses créateurs (Voir 8.1). Les créateurs de GandCrab ont annoncé avoir gagné 150 millions de dollars par an au travers de leur modèle économique de Ransomware-As-A-Service (Voir 8.6) [39].

Le tableau suivant présente les profits estimés de plusieurs rançongiciels.

Rançongiciel	Profits connus ou estimés	Période
Cryptolocker	3 millions $	2013
SamSam	6 millions $	2016-2018
Cryptowall	18-320 millions $	2014-2016
Locky	7,8-150 millions $	2016-2018
Cerber	6,9 millions $	2016-2018
GandCrab	150 millions $	2018-2019
Ryuk	7 millions $	2018

Par manque de données disponibles, il est beaucoup plus difficile d'estimer précisément le coût d'une attaque de type Big Game Hunting pour un groupe cybercriminel. Une attaque de ce type nécessite au moins :

- le développement du code malveillant ;
- la mise en place de l'infrastructure de distribution ;
- la mise en place de l'infrastructure de paiement ;
- le développement du vecteur d'infection ;
- les ressources humaines pour réaliser la conduite de l'opération ;
- un moyen de blanchir les revenus.

Certaines ressources nécessaires à ces différentes étapes peuvent être achetées sur le marché noir. Un kit d'exploitation de vulnérabilité peut être acheté pour quelques centaines de dollars. L'affiliation à un modèle Ransomware-as-a-Service coute entre quelques centaines et quelques milliers de dollars [1]. Certains services en ligne, comme Digital Ocean[7], permettent de se constituer une infrastructure d'attaque pour une poignée de dollars. Les méthodes de blanchiment des revenus sont très nombreuses et une estimation de leur coût n'a pu être réalisée pour

[6] Certaines sociétés se sont spécialisées dans le suivi des transactions en cryptomonnaie, notamment ChainAnalysis et Neutrino
[7] Il est important de noter que Digital Ocean est un service légitime de location d'infrastructure Cloud payable à l'heure.

l'heure. Dans tous les cas, il apparait évident que le coût d'une opération « Big Game Hunting » ne dépassera pas en moyenne les dizaines de milliers de dollars sur l'ensemble de la période d'activité malveillante, l'essentiel étant constitué du « salaire » des opérateurs.

Dans tous les cas, il est très peu probable que le coût pour l'attaquant approche ses revenus potentiels.

7 Effets latents

Les revenus générés par ce type d'attaques et l'émergence d'assurances et de sociétés de négociation validant leur modèle économique incitent à penser que **le phénomène rançongiciel prendra de l'ampleur dans les années à venir.** Plus précisément, les efforts des cybercriminels pour s'assurer que la rançon sera payée (ciblage d'entités financièrement solides, recherche de la rupture d'activité, etc.) favoriseront l'émergence de nouvelles campagnes de « Big Game Hunting ».

L'augmentation du nombre d'attaques par rançongiciel pourra également amener à la répétition des infections, les victimes voyant tout ou partie de leur réseau paralysé régulièrement, qu'ils aient payé ou non les extorsions précédentes.

Les attaques à l'encontre d'Altran et de Norsk Hydro montrent le danger d'un impact systémique des rançongiciels qui, en ciblant des entreprises sous-traitantes ou clés d'un secteur d'activité, pourraient amener un jour à déstabiliser plusieurs grands groupes (supply chain attack) ou un pan d'activité économique entier (rupture dans l'approvisionnement de matière première par exemple).

De nombreuses attaques montrent également que certains cybercriminels utilisent simultanément différents types de codes : Trojan bancaire, mineur de cryptomonnaie, rançongiciel. Ces codes sont autant de moyens d'extorsion différents, permettant aux attaquants de générer du profit avec l'ensemble des ressources de la cible (puissance de calcul, données personnelles, bancaires et métier, vente de l'accès au réseau, etc.).

Certaines attaques ont montré qu'il était possible pour les cybercriminels d'entraver certaines investigations judiciaires (cas de la compromission des laboratoires Eurofins Scientific) et des postes de police. Si l'objectif restait lucratif, il est tout à fait envisageable dans le futur que des groupes cybercriminels (ou le crime organisé en général) puissent s'appuyer sur ce moyen afin de faire pression sur la justice.

Enfin, la frontière entre l'utilisation d'un code de chiffrement et un code de sabotage est ténue. NotPetya et GermanWiper [48] sont deux exemples de codes se faisant passer pour des rançongiciels, mais ayant uniquement une finalité de sabotage. Il est tout à fait envisageable que des puissances étrangères utilisent des rançongiciels dans une logique déstabilisatrice.

8 Annexes

8.1 SamSam

Le rançongiciel SamSam est le premier code de ce type à avoir été utilisé, dès 2016, à l'encontre d'entreprises et institutions lors d'attaques ciblées et opérées manuellement par les attaquants, préfigurant la tendance du « Big Game Hunting » [49]. Son activité a pris fin avec l'accusation publique par le FBI de deux ressortissants iraniens fin novembre 2018 [50]. **En France, aucun incident lié à SamSam n'a été remonté à l'ANSSI.**

SamSam n'a jamais été mis en vente sur le DarkWeb et a vraisemblablement été utilisé par un seul groupe d'attaquants. Bien qu'employant des moyens peu sophistiqués, les attaquants ont montré une capacité significative d'adaptation et d'évolution technique, améliorant les méthodes de compromission, le code malveillant et l'infrastructure de paiement afin d'augmenter les chances d'infection et rendre plus complexe la rétro-ingénierie du code. SamSam a également montré, à la fois à la communauté de la cybersécurité et aux cybercriminels qu'il était possible de générer des millions de dollars de revenus avec assez peu de moyens.

S'appuyant initialement sur l'exploitation d'une vulnérabilité applicative pour compromettre les réseaux ciblés[8], les attaquants ont par la suite compromis des accès à distance (bruteforce RDP) profitant des nombreux accès de ce type peu ou pas protégés. Après avoir pris pied sur le réseau de la victime, les attaquants utilisaient des outils d'administration réseau légitimes pour s'y propager. Ils déclenchaient ensuite le chiffrement des fichiers tard dans la nuit afin de limiter au maximum la réactivité de la victime.

Intelligemment, les attaquants opérant SamSam ont ciblé des infrastructures critiques, notamment des hôpitaux et établissements de soin, ainsi que des structures publiques locales (mairies, services publics, universités), majoritairement aux États-Unis. Ce type d'entités, dont le niveau de sécurité informatique est souvent très bas faute de budget, est très sensible aux ruptures d'activité puisqu'elles causent invariablement l'arrêt de services publics parfois essentiels, les incitants ainsi fortement à payer la rançon. L'éditeur Sophos considère toutefois que de nombreuses entreprises privées font également partie des victimes de SamSam [49].

Par ce mode opératoire peu sophistiqué, SamSam aurait rapporté à ses créateurs environ 6 millions de dollars. L'étude menée par Sophos et Neutrino montre également que les attaquants ont adapté à la hausse le montant des rançons demandées au cours des deux années d'activité.

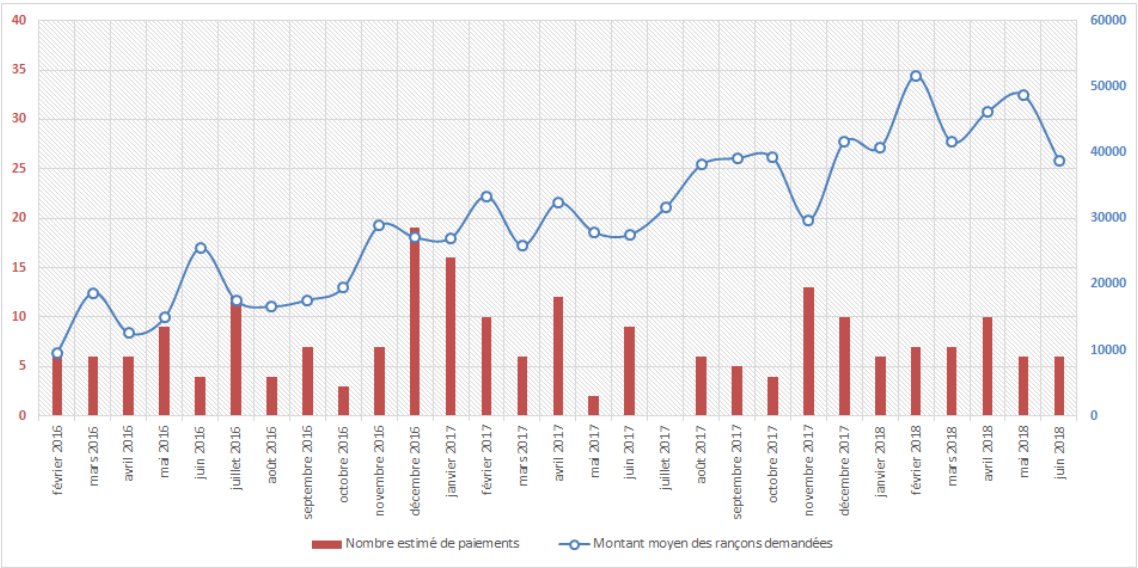

Fig. 8.1 : Montant moyen des rançons ($) demandées par SamSam de février 2016 à juin 2018. Source : Sophos. Infographie : AMR

[8] La vulnérabilité JAVA CVE-2010-0738.

8.2 BitPaymer/FriedEx

Le rançongiciel connu sous les noms BitPaymer, FriedEx ou IEncrypt a été utilisé depuis juillet 2017 à l'encontre d'entreprises et institutions, dans le cadre d'attaques ciblées et opérées manuellement [51]. Bitpaymer/FriedEx était toujours utilisé en juillet 2019 [52].

Les recherches de l'éditeur ESET [53] ont permis de lier le rançongiciel au code Dridex (Trojan bancaire[9] particulièrement sophistiqué apparu en 2014 et connu pour cibler le secteur financier) avec lequel il partage de nombreuses similarités techniques. Le groupe cybercriminel utilisant Dridex aurait ainsi diversifié ses activités lucratives, ayant probablement étudié la réussite des rançongiciels déjà existants.

Bitpaymer/FriedEx est distribué au travers de sites Internet légitimes compromis proposant le téléchargement de mises à jour Flash et Chrome piégées [54]. Les analyses de Crowdstrike indiquent que cette méthode d'infection serait « sous-traitée » à un autre groupe d'attaquants, d'autres codes malveillants ayant été distribué de la même manière et au même moment. Les attaquants ont également compromis des accès RDP peu ou pas protégés [51]. Dernièrement, la compromission des victimes aurait aussi été réalisée au travers de campagnes d'hameçonnage [55]. Afin de se propager au sein du réseau victime, les attaquants utilisent l'outil de test de pénétration Powershell Empire ainsi que l'outil de récupération de mot de passe Mimikatz. Les réseaux victimes sont également compromis avec le Trojan bancaire Dridex. En plus de chiffrer les fichiers accessibles, BitPaymer/FriedEx a également la capacité de supprimer les copies cachées[10].

Commentaire : Il est probable que, durant cette phase de propagation et de reconnaissance au sein du réseau de la victime, les attaquants choisissent quel type d'attaque sera menée (rançongiciel ou vol de données bancaires) sur la base des informations récupérées.

BitPaymer/FriedEx a notamment compromis le 25 août 2017 plusieurs hôpitaux écossais [56] et aurait également ciblé des organisations à but non lucratif, des municipalités américaines, des entités des secteurs de l'éducation, de l'industrie [57] ainsi que de la finance et de l'agriculture [55].

Les rançons demandées sont particulièrement élevées, allant de 20 à 53 Bitcoins (soit l'équivalent de plusieurs centaines de milliers de dollars) en 2018, puis jusqu'à 216 Bitcoins (plusieurs millions de dollars) en 2019 [57].

En juillet 2019, une nouvelle variante du rançongiciel (DoppelPaymer), présentant des différences notables avec Bitpaymer/FriedEx, a été détectée par l'éditeur Crowdstrike [58] lors d'une attaque contre la municipalité d'Edcouch au Texas. Crowdstrike avance l'hypothèse d'une séparation au sein de l'équipe cybercriminelle, Bitpaymer/FriedEx étant toujours utilisé.

Cette nouvelle variante donne des indications intéressantes sur la volonté des cybercriminels d'adapter leurs attaques à leurs cibles, et notamment à leur capacité financière. Ainsi, des attaques impliquant DoppelPaymer ont pu être associées à des rançons de 2, 40 et 100 Bitcoins (soit d'environ 25 000 à 1 200 000 dollars).

En France, le groupe audiovisuel M6 a été victime du rançongiciel Bitpaymer en octobre 2019 [59].

8.3 Ryuk

Le rançongiciel Ryuk est utilisé depuis août 2018 dans le cadre d'attaques de type « Big Game Hunting ». Il est opéré par le groupe cybercriminel russophone FIN6, initialement spécialisé dans la compromission d'entités du secteur financier et de terminaux de points de vente. Début 2019, l'éditeur Crowdstrike avait identifié 52 transactions vers des portefeuilles Bitcoins du groupe pour un total de gain de 705 Bitcoin environ (soit plusieurs millions de dollars) [60].

À la connaissance de l'ANSSI, Ryuk n'est pas en vente sur le marché noir et utilisé uniquement par FIN6 et ses possibles groupes affiliés .

[9] Code malveillant ayant pour objet initial d'exfiltrer des données bancaires, mais capable également de télécharger d'autres codes malveillants.
[10] Copies de données permettant leur recouvrement lors d'incidents affectant la structure de fichiers d'un système d'exploitation

Une particularité de Ryuk est qu'il est distribué dans de nombreuses attaques à la suite d'une compromission par le Trojan bancaire Trickbot, code possiblement développé par le groupe cybercriminel FIN6 [60], lui-même parfois déposé sur le réseau victime par le Trojan bancaire Emotet [61]. FireEye relève également des incidents impliquant l'exploitation de vulnérabilités sur des serveurs connectés à Internet [62].

Commentaire : La distribution d'un rançongiciel sur un réseau victime après son infection par un Trojan bancaire démontre l'importance pour les organisations de prioriser le traitement d'incidents liés à ce type de code. Dans les analyses de risque, celui de certains Trojan bancaires ne doit pas se limiter au vol de données bancaires, mais s'étendre au risque d'escalade vers une attaque par rançongiciel impactant la continuité d'activité.

Ryuk est connu pour avoir ciblé de très nombreuses institutions publiques, notamment les villes américaines de Jackson en Géorgie [63], Lake City en Floride [64], le Conseil de Justice de Géorgie ainsi que la société de sécurité Prosegur [65]. Comme d'autres groupes cybercriminels, les opérateurs de Ryuk font attention à ne pas compromettre de réseau identifié comme russe et ont intégré des vérifications techniques au sein du code Ryuk en ce sens. [66].

Un rapport de l'éditeur chinois Tencent a fait état de compromissions par Ryuk en juillet 2019 à l'encontre d'entreprises et de municipalités chinoises [67].

L'ANSSI a connaissance de trois compromissions d'entreprises françaises (ou de leurs filiales) par Ryuk. En décembre 2018, l'entreprise Travel Technologies Interactive a vu l'ensemble de son réseau sensible chiffré contre une rançon de 170000 euros après l'exploitation triviale d'une vulnérabilité sur l'un de ses sites Internet. Le 11 mars 2019, l'entreprise Fleury Michon a dû interrompre sa production et positionner 3000 employés en chômage technique suite à la compromission de l'ensemble de son réseau logistique par un rançongiciel ayant de forte similarités opératoire avec Ryuk. Enfin, en mai 2019, le réseau d'une filiale canadienne de Bouygues Construction a été compromis par Ryuk, chiffrant ses serveurs Windows. L'ANSSI n'a pas connaissance des montants des rançons demandées pour ces deux dernières victimes. Pour autant, la société Coveware, spécialisée dans la négociation de ce type de rançons, révèle que les opérateurs de Ryuk ont fortement augmenté le montant de leur rançon à partir de janvier 2019.

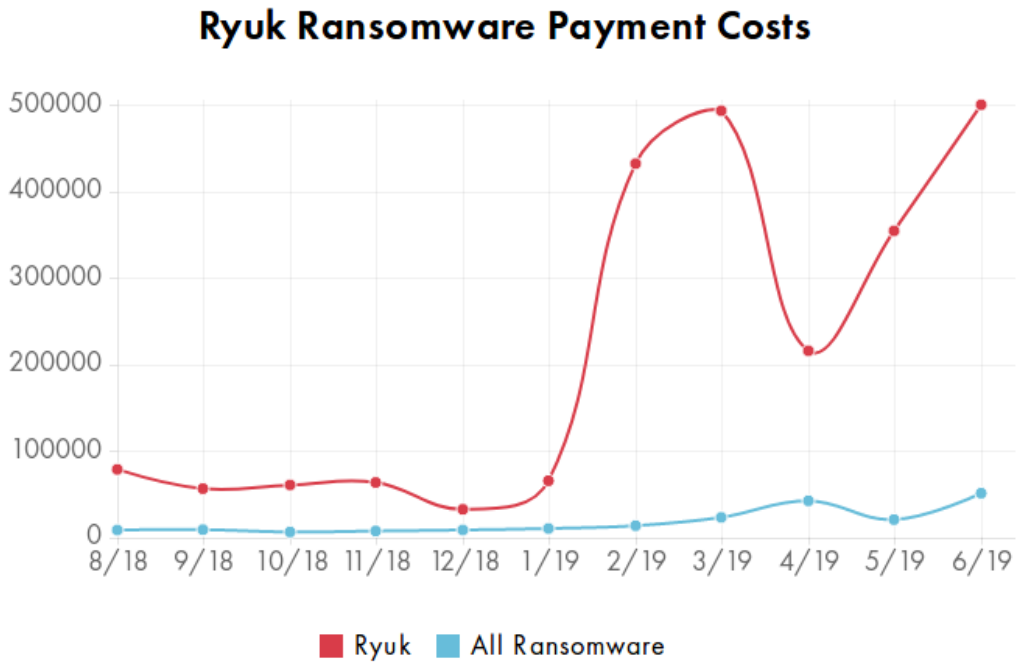

Fig. 8.2 : Évolution du montant des rançons associées aux attaques impliquant Ryuk. Source : Coveware.

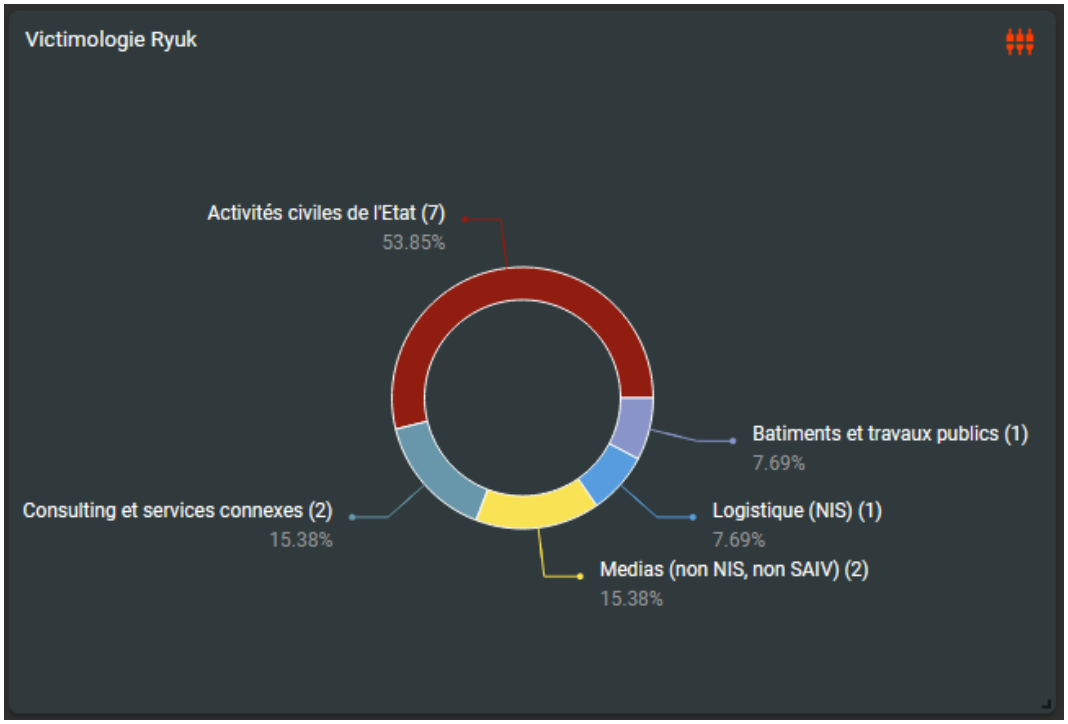

Fig. 8.3 : Répartition par secteur d'activité des victimes de Ryuk connues de l'ANSSI. Source : ANSSI

8.4 LockerGoga

Le rançongiciel LockerGoga est actif depuis le début de l'année 2019 et serait uniquement opéré par le groupe cybercriminel FIN6. À l'instar du code Ryuk, il semble exclusivement utilisé dans le cadre d'attaques « Big Game Hunting », se concentrant sur de grands groupes internationaux.

LockerGoga s'est ainsi fait connaitre par la compromission en janvier 2019 de l'entreprise française d'ingénierie ALTRAN. La participation de l'ANSSI au traitement de l'incident permet de connaitre les techniques, tactiques et procédures employées par les attaquants afin de réaliser leur attaque. Ainsi, les attaquants ont utilisé des accès à distance (RDP) afin d'utiliser l'outil légitime d'administration Psexec pour déployer le code de chiffrement sur un certain nombre de machines. Certains rapports indiquent que la compromission initiale aurait été menée par hameçonnage ciblé contre un employé d'Altran en Roumanie [68]. La compromission a forcé Altran à interrompre ses activités [69].

Le 18 mars 2019, LockerGoga a été utilisé pour chiffrer le réseau de l'entreprise Norsk Hydro spécialisé dans l'aluminium et les énergies renouvelables. Plusieurs sites de production auraient été arrêtés [70]. Norsk Hydro estime dans son rapport financier que l'attaque lui aura couté 75 millions de dollars [71]. Toujours en mars 2019, deux compagnies américaines du secteur de la chimie industrielle, Hexion and Momentive, ont également été compromises par LockerGoga sans que l'ampleur de l'impact ne soit connue [72].

Étrangement, les dernières versions de LockerGoga empêchent les utilisateurs de se connecter aux machines chiffrées, leur laissant peu de chance de trouver le message de demande de rançon [73].

Commentaire : Cette méthode qui rend plus difficile le paiement de la rançon par la victime peut questionner sur la finalité lucrative de LockerGoga. En ciblant des entreprises possédant des réseaux industriels de cette manière, les attaquants pourraient également chercher à mener des actions de sabotage aux conséquences physiques potentiellement graves.

Le rançongiciel LockerGoga n'a pas été détecté depuis juin 2019. Une alerte de FBI avance des liens techniques avec le rançongiciel MegaCortex apparu à la même période et toujours actif. Ce dernier pourrait donc avoir remplacer LockerGoga [74].

8.5 Dharma

Le rançongiciel Dharma est actif depuis 2016. Il est responsable de 9 incidents traités par l'ANSSI depuis 2017, majoritairement dans le secteur de la santé avec en août 2019 la compromission de Ramsay Générale de Santé, leader de l'hospitalisation privée sur le territoire . En fin d'année 2019, Dharma était toujours actif après avoir vu un pic d'activité mi 2019 [75].

Le très grand nombre de variantes du code Dharma présentant des configurations différentes laisse penser que ce rançongiciel est partagé, probablement sous le modèle « Ransomware-as-a-service ». Responsable d'un quart des infections détectées en 2018, Dharma est probablement proposé à bas prix. Certains groupes d'attaquants ont également montré une mauvaise maitrise opérationnelle du code, empêchant les victimes de récupérer leurs fichiers malgré le paiement de la rançon [76].

Cherchant majoritairement à compromettre des entreprises, Dharma est distribué par hameçonnage comprenant soit un lien malveillant, soit une pièce jointe piégée. Cette dernière usurpe parfois l'identité d'un antivirus. Comme beaucoup d'autres rançongiciels, il compromet également ses victimes par l'utilisation d'accès RDP peu ou pas protégés. Cette multiplicité des méthodes d'infection est typique du modèle « Ransomware-as-a-service ». Dharma chiffre ensuite les fichiers présents sur la machine ainsi que sur les partages réseau accessibles. Il supprime également les copies cachées.

Les montants des rançons et les chances de récupérer ses fichiers sont très variables en fonction des variantes de Dharma [76].

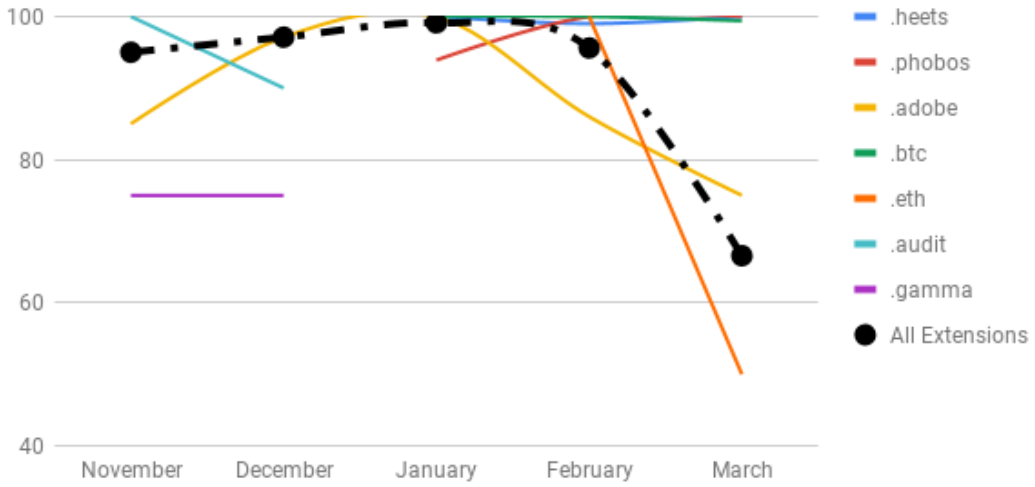

Fig. 8.4 : Taux de récupération des fichiers après paiement de la rançon pour certaines variantes de Dharma. Source : Coveware.

8.6 GandCrab

Le rançongiciel GandCrab est apparu en janvier 2018 et a été vendu sur le marché noir en tant que « Ransomware-as-a-Service » (RaaS), permettant ainsi à des groupes cybercriminels dits « affiliés » de l'utiliser dans leurs propres attaques en échange du versement d'une partie des bénéfices (40% la plupart du temps). Le premier prix d'entrée pour un affilié était de 100$ pour deux mois d'utilisation [40]. Les développeurs de GandCrab sont russophones.

Utilisé par de nombreux groupes cybercriminels ainsi que par les auteurs eux-mêmes, GandCrab a été distribué selon de nombreuses méthodes d'infection, en fonction des capacités de chaque affilié. Il a notamment été distribué au travers de publicités en ligne malveillantes [40], de campagnes d'hameçonnage et de compromissions d'accès à distance (RDP) [77].

Gandcrab, par son système d'affiliation, a ainsi pu être utilisé dans le cadre d'attaques ciblées, mais également non ciblées. GandCrab a notamment compromis en France une entreprise du secteur énergétique qui a vu l'ensemble de son parc informatique chiffré le 11 mai 2019.

L'auteur du code a montré une grande réactivité aux publications d'outils de déchiffrement des éditeurs de sécurité. Il est également à noter que l'auteur de GandCrab interdisait à ses affiliés de cibler des pays de l'ex-URSS ainsi que la Syrie.

Commentaire : Cette restriction de ciblage est à comprendre à la fois comme une « charte éthique » liée à un certain patriotisme des groupes cybercriminels russophones, mais également comme une mesure de protection. En ne ciblant pas cette région du monde, les attaquants espèrent une certaine complaisance, tout du moins un désintérêt, de la part des forces de police des pays en question où se situent très probablement les cybercriminels. Étant donné l'impunité dont jouissent jusqu'à présent ces cybercriminels, cette technique semble fonctionner.

Début juin 2019, l'auteur de GandCrab a annoncé son « départ à la retraite » et la fermeture définitive de son « service », et a également déclaré un revenu total pour l'ensemble des affiliés de 2 milliards de dollars [39]. Au cours du mois suivant, les efforts combinés du FBI, d'Europol, de services de police européens et d'éditeur de solutions de sécurité ont permis la publication de la clé-maître[11] de la dernière version du code GandCrab, permettant ainsi le déchiffrement de l'ensemble des fichiers des victimes.

Commentaire : Il est fort probable que cette clé-maître ait été obtenue par la saisie d'un serveur central de l'infrastructure d'attaque liée à GandCrab.

Selon le FBI, GandCrab aurait causé plus de 300 millions d'euros de perte et infecté plus de 500 000 victimes au niveau mondial [78].

8.7 Sodinokibi/Revil

Sodinokibi est apparu en avril 2019 et présente des similarités de code avec le rançongiciel GandCrab. Il est possible qu'il ait été développé par les mêmes auteurs, invalidant de fait le retrait du groupe des activités cybercriminelles. Il est particulièrement connu pour avoir attaqué de façon coordonnée une vingtaine de villes au Texas en août 2019 en demandant l'équivalent de 2,5 millions de dollars de rançons [42].

Sodinokibi fonctionne sur le même principe d'affiliation que GandCrab et présente aussi les mêmes restrictions de ciblage concernant la Syrie et les pays de l'ex-URSS. **Les créateurs de Sodinokibi refusent également l'affiliation de groupes d'attaquants anglophones.**

[11] Alors que les différents affiliés possèdent les clés de déchiffrement associées à leur utilisation du rançongiciel, son créateur possède parfois une clé-maître permettant de déchiffrer l'ensemble des fichiers chiffrés par les affiliés. Cela lui permet de garder un certain contrôle sur l'usage de son code et notamment du respect de ses règles d'emploi.

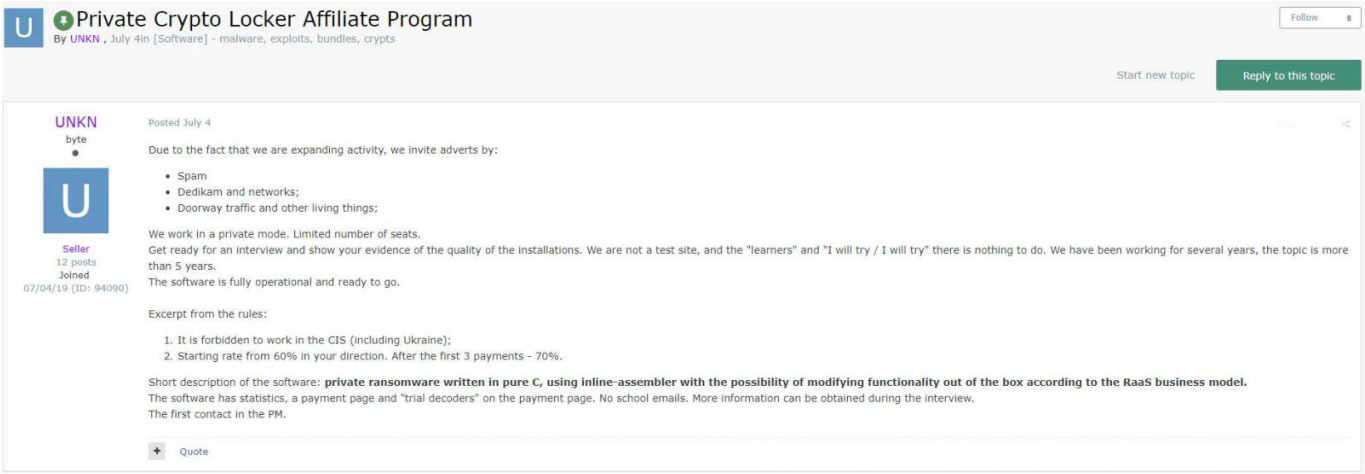

Fig. 8.5 : Message de lancement de Sodinokibi sur un forum d'attaquants. Source : BleepingComputer.

Les rançons associées à Sodinokibi varient de quelques milliers à plusieurs centaines de milliers de dollars en fonction des groupes affiliés l'utilisant et des victimes [42].

Sodinokibi pourrait représenter dans le futur une menace plus importante pour les entreprises et institutions que GandCrab, même si pour l'heure l'ANSSI ne relève que des incidents mineurs sur son périmètre. Les auteurs semblent en effet privilégier des affiliés ayant de fortes compétences techniques. Les méthodes d'infection employées sont ainsi beaucoup plus efficaces :

- Exploitation d'une vulnérabilité 0-day Oracle en avril 2019 [79];
- Campagne d'hameçonnage usurpant l'identité de Booking.com en juin 2019 [80];
- Compromission d'entreprises de services numériques (ESN) pour distribuer le rançongiciel sur les réseaux de leurs clients en juin 2019 [81];
- Utilisation de kit d'exploitation (RIG) associé à une campagne de publicités en ligne malveillantes en juin 2019 [82];
- Dépôt du rançongiciel sur le réseau victime après sa compromission par un Trojan bancaire (Ursnif) en juillet 2019 ;
- Compromission de sites Internet afin de distribuer des logiciels légitimes piégés, comme WinRar, toujours en juin 2019 [83];
- Exploitation de la vulnérabilité Pulse Secure (CVE-2019-11510) fin décembre 2019 [84].

Par ailleurs, en janvier 2019, un groupe cybercriminel utilisant Sodinokibi a divulgué des documents présentés comme issus d'un système d'information compromis de l'entreprise américaine Artech Information Systems. Selon les attaquants, cette divulgation a été effectué suite au refus de l'entreprise à payer la rançon demandée [29].

8.8 MegaCortex

Le rançongiciel MegaCortex a été découvert en mai 2019 et était utilisé initialement dans le cadre d'attaques « Big Game Hunting ». Il ne semblait alors pas être distribué en tant que « Ransomware-As-A-Service » [85]. La société de service nuagique américaine iNSYNQ a été victime du code en juillet 2019, l'attaque paralysant ses services et empêchant ses clients d'accéder à leurs données [86].

MegaCortex est déposé sur les réseaux victimes après leurs compromissions par un Trojan bancaire (Emotet, Trickbot, mais aussi Qbot et Rietspoof). Dans certains cas, les attaquants ont eu accès aux droits d'administration du réseau et se sont servis d'outils d'administration légitimes afin de propager le code de chiffrement sur des serveurs

d'intérêt [87].

Crowdstrike révèle dans un rapport que les opérateurs de MegaCortex utilisent des outils et méthodes similaires à celles identifiées lors d'attaques impliquant LockerGoga N. Il est possible que megaCortex soit désormais utilisé en lieu et place de LockerGoga qui n'est plus détecté.

Alors que la grande majorité des groupes cybercriminels s'adonnant au « Big Game Hunting » cherchent, au travers de la façon dont leurs notes de rançon sont rédigées, à accompagner les victimes dans leur paiement, les opérateurs de MegaCortex emploient un ton extrêmement agressif [88]. Une autre particularité de MegaCortex est qu'il ne pouvait être déposé sur le réseau victime que manuellement et nécessitait l'usage d'un mot de passe par l'attaquant pour être utilisé.

En août 2019, une nouvelle version du code MegaCortex a été détectée et analysée par la société Accenture. Cette version est construite pour être distribuée massivement et s'exécuter automatiquement (la protection par mot de passe ayant été supprimée) [89]. Il est possible que cette version ne soit pas destinée à des attaques « Big Game Hunting ».

8.9 RobinHood

Le rançongiciel RobinHood a été détecté en avril 2019 et est connu pour avoir paralysé les services de la ville de Baltimore pendant plusieurs semaines [20] ainsi que la ville de Greenville [90]. Il a été utilisé dans le cadre d'attaques « Big Game Hunting » à l'encontre de municipalités aux États-Unis [91] et d'entités du secteur de l'énergie en Inde N.

Afin de déposer le code de chiffrement sur le réseau victime, les opérateurs de RobinHood s'appuient sur la compromission préalable du réseau par un Trojan bancaire ou utilisent des accès à distance compromis [92].

Si le code de chiffrement ne présente aucune particularité significative, Crowdstrike relève que la présence de captures d'écran sur un portail de paiement montrant un document sensible présenté comme provenant de la victime **laisse penser que les opérateurs exfiltrent également des données et ne se contentent donc pas de les chiffrer** .

8.10 Maze

Le rançongiciel Maze[12] a été découvert en mai 2019. Il est principalement connu pour être associé à des divulgations sur Internet d'informations présentées comme issues des systèmes d'information compromis. Certains de ses opérateurs ont en effet choisi d'exercer ce moyen de pression supplémentaire à l'encontre des victimes qui ne payent pas rapidement la rançon demandée. Dans ce cadre, les données sont publiées sur le site Internet « mazenews.top ».

En France, la compromission par Maze d'une partie des systèmes d'information de Bouygues Construction a été détecté le 30 janvier 2020 [93], occasionnant le chiffrement de nombreuses données. Les attaquants ont déclaré avoir demandé une rançon équivalente à dix millions de dollars [94], ce qui n'est pas confirmé par Bouygues. Pour l'heure, un fichier d'archive de 1.2Gb protégé par un mot de passe est présent sur le site des attaquants. Il n'est pas confirmé que cette archive corresponde réellement à des données exfiltrées du système d'information de Bouygues Construction.

Chaine de compromission connue

À la connaissance de l'ANSSI, Maze était initialement distribué au travers de sites piégés à l'aide d'exploit kit (Fallout EK, Spelevo EK) et aux couleurs de fausses plateformes d'échange de cryptomonnaie [95]. Le montant de la rançon variait alors en fonction de la nature de la cible (ordinateur de particulier, machine professionnelle, serveur d'entreprise, controleur de domaine, etc.).

[12] Également nommé ChaCha ransomware de par son usage de l'algorithme de chiffrement ChaCha20.

Depuis fin octobre 2019, de nouvelles campagnes de courriels malveillants prétendument issus d'organismes étatiques italiens, allemands ou américains [96] ont servi à délivrer des codes CobaltStrike téléchargeant le rançongiciel Maze [97]. S'en sont suivies de nombreuses compromissions d'envergure associées à des montants de rançon très élevés (plusieurs millions de dollars).

Après le dépôt du code CobaltStrike, les attaquants réaliseraient des actions de propagation (RDP, Powershell, ...), d'élévation de privilège et d'exfiltration de données sur le réseau de la victime pendant quelques semaines avant de déployer le code de chiffrement Maze sur les machines accessibles. L'exfiltration serait réalisée via des scripts Powershell et les données envoyées sur un serveur FTP distant [98]. Comme de nombreux autres rançongiciels, Maze ne se contente pas de chiffrer des fichiers présents sur la machine compromise, et efface également les copies cachées.

Victimologie

Outre Bouygues Construction, de nombreuses victimes de Maze sont connues en sources ouverte. La liste suivante présente quelques exemples de victimes ainsi que les montants de rançon et volume de données divulguées associés. Cette liste ne représente très probablement qu'une faible proportion de l'ensemble des victimes du rançongiciel. Il est toutefois intéressant de noter que, à l'instar de nombreux autres rançongiciels, la région nord américaine est fortement touchée.

Victime	Période	Pays	Montant de rançon	Volume de données divulguées
Andrew Agencies	Octobre 2019	Canada	1.1M$	Inconnu
Allied Universal	Novembre 2019	USA	2.3M$	700Mb
Southwire	Décembre 2019	USA	6M$	14Gb
Pensacola City	Décembre 2019	USA	1M$	2Gb
Fratelli Beretta	Décembre 2019	Italie	Inconnu	3Gb
Bouygues Construction	Janvier 2020	France	10M$	Non confirmé
Stockdale radiology	Janvier 2020	USA	Inconnu	Données personnelles
Lakeland Community College	Janvier 2020	USA	Inconnu	19Gb
Medical Diagnostic Laboratories	Janvier 2020	USA	Inconnu	Données de recherche
Hamilton and Naumes	Janvier 2020	USA	Inconnu	Inconnu
Bird Construction	Janvier 2020	Canada	9M$	60Gb
Busch's Inc	Inconnue	USA	Inconnu	Données personnelles
BST	Inconnue	USA	Inconnu	Données personnelles
Massey Services	Inconnue	USA	Inconnu	Données personnelles

Groupe cybercriminel TA2101

Maze est opéré par au moins un groupe cybercriminel spécialisé dans le Big Game Hunting, probablement le groupe cybercriminel identifié par Proofpoint sous le nom de TA2101 [96]. Ce groupe pourrait notamment être responsable des campagnes d'attaques d'octobre 2019 et ainsi cibler les secteurs de la santé, de la construction et de l'IT [99]. Les attaques de ce groupe sont associées à des rançons de plusieurs millions de dollars.

L'attaque contre l'entreprise américaine Southwire en décembre 2019 a été assortie d'une rançon de 850 BTC, soit environ 6 millions de dollars [27]. Devant le refus de payer de la société, les attaquants ont divulgué 14Gb de données présentées comme internes à la société [28]. La ville américaine de Pensacola, également victime de Maze en décembre 2019, s'est vu demander l'équivalent d'un million de dollars contre le déchiffrement de ses fichiers [100]. Il est intéressant de noter que dans un cas, les attaquants ont déclaré qu'une partie de la rançon permettait d'obtenir l'outil de déchiffrement tandis que l'autre partie permettait d'assurer que les données ne soient pas divulguées[13] [101]. **Au delà de la pression supplémentaire exercée sur la victime par ces divulgations, il semble ainsi qu'il y ait aussi une volonté de monétiser les données exfiltrées.**

[13] 100BTC pour avoir accès à l'outil de déchiffrement, 100BTC pour assurer la non divulgation des données exfiltrées.

Commentaires

Ces forts montants, combinés au risque de divulgation de données internes, en font le rançongiciel ayant le plus fort impact potentiel sur les entreprises et institutions. Celles-ci peuvent effectivement se retrouver à supporter l'impact de la divulgation de données clients, notamment personnelles (RGPD), mais également de données de recherche, commerciales ou encore classifiées.

Enfin, rien n'empêche les attaquants de revendre les données exfiltrées à d'autres groupes cybercriminels.

8.11 Clop

Le rançongiciel Clop a été observé pour la première fois en février 2019. Son code est l'objet de fréquentes modifications mineures, qui semblent principalement avoir pour objectif de complexifier sa détection [102]. Il est une variante de la famille de rançongiciels CryptoMix, elle-même dérivée des familles CryptXXX et CryptoWall.

Il semble être majoritairement distribué au travers de campagnes d'hameçonnage, qui n'apparaissent pas ciblées mais plutôt massives. **Le rançongiciel étant dépourvu de fonctionnalités de propagation automatique**, les attaquants s'attachent en premier lieu à se propager au sein du réseau de la victime à l'aide de plusieurs codes malveillants. Ainsi, l'éditeur Ahnlab et le CERT gouvernemental sud-coréen rapportent l'usage de la porte dérobée FlawedAmmyy[14] et de l'outil d'attaque Cobalt Strike lors de cette phase. L'ANSSI a pu constater également l'utilisation des outils Metasploit et Mimikatz ainsi que de la porte dérobée SDBBot. L'objectif des attaquants est d'acquérir des droits d'administration de domaine « Active Directory » afin de faciliter le déploiement du code de chiffrement sur l'ensemble du système d'information à partir de serveurs centraux.

Des certificats sont utilisés pour signer le code malveillant Clop afin de lui donner une apparence légitime. Les entités suivantes ont été observées à plusieurs reprises dans le champ « Sujet » des certificats associés aux attaques déployant le rançongiciel Clop : "ALISA L LIMITED"[15], "THE COMPANY OF WORDS LTD" et "MISHA LONDON LTD".

Enfin, afin d'entraver les actions des équipes de sécurité informatique de la victime, le rançongiciel est souvent déployé en début ou veille de week-end et comporte une fonction de suppression des copies cachés Windows (*Volume Shadow copies*).

Les attaques impliquant Clop ne se limitent pas à une zone géographique ni à un secteur d'activité particulier. L'éditeur McAfee mentionne ainsi des attaques ayant majoritairement ciblé les États-Unis, mais également une douzaine d'autres pays[16]. Durant le premier semestre 2019, Clop aurait également ciblé des agences gouvernementales en Corée du Sud. En décembre 2019, des universités en Allemagne et au Pays-Bas ont été compromises [103].

En France, 6 incidents ont fait l'objet de traitement par l'ANSSI, dont 5 en Novembre 2019 dans le cadre de la compromission du CHU de Rouen .

Liens entre TA505 et le déploiement du rançongiciel Clop

Outre l'utilisation dans la chaîne de compromission d'outils connus pour être associés au groupe TA505 (en particulier FlawedAmmyy), plusieurs liens techniques rattachent le rançongiciel Clop à ce groupe cybercriminel. Notamment, une souche du rançongiciel a été signée avec le même certificat qu'une souche de FlawedAmmyy.

Un lien similaire a aussi été constaté par le CERT sud-coréen entre une souche du rançongiciel et une souche du code Amadey qui, bien que vendu sur certains forum d'attaquants, est aussi utilisé par TA505.

[14] FlawedAmmyy est un outil d'accès à distance basé sur la fuite du code source du logiciel légitime Ammyy Admin en 2016, et contenant un downloader et une porte dérobée.
[15] Ce nom de certificat se rapproche fortement d'un certificat utilisé pour signer LockerGoga, nommé ALISA LTD.
[16] Suisse, Royaume-Uni, Belgique, Pays-Bas, Croatie, Allemagne, Danemark, République Dominicaine, Porto Rico, Turquie, Russie

Aussi il apparaît intéressant de prendre en compte les informations connues sur TA505, et notamment le fait que ce groupe pratique aussi l'exfiltration de données bancaires et qu'il puisse ainsi réaliser ce type d'action en marge de l'utilisation du rançongiciel Clop.

9 Bibliographie

[1] Bromium. *Into the Web of Profit*. 20 avr. 2018.

[2] Trend Micro. *Compromised Website for Luxury Cakes and Pastries Spreads Ransomware*. 22 fév. 2012. URL : https://blog.trendmicro.com/trendlabs-security-intelligence/compromised-website-for-luxury-cakes-and-pastries-spreads-ransomware/.

[3] Le Parisien. *La cyberattaque de Baltimore a coûté plus de 18 millions de dollars à la ville*. 20 juil. 2019. URL : http://www.leparisien.fr/economie/la-cyberattaque-de-baltimore-a-coute-plus-de-18-millions-de-dollars-a-la-ville-20-07-2019-8120535.php.

[4] BleepingComputer. *New eCh0raix Ransomware Brute-Forces QNAP NAS Devices*. 10 juil. 2019. URL : https://www.bleepingcomputer.com/news/security/new-ech0raix-ransomware-brute-forces-qnap-nas-devices/.

[5] BleepingComputer. *Ransomware - Most Popular Malware in Underground Forums*. 24 juil. 2019. URL : https://www.bleepingcomputer.com/news/security/ransomware-most-popular-malware-in-underground-forums/.

[6] Cyentia Institute. *Measuring Ransomware Payment Rate*. 5 juil. 2017. URL : https://www.cyentia.com/ransomware-p1-payment-rate/.

[7] Kaspersky. *L'évolution du ransomware et les outils pour y faire face*. 19 juin 2018. URL : https://www.kaspersky.fr/blog/evolution-of-ransomware/10610/.

[8] Symantec. *Internet Security Threat Report 2019*. Fév. 2019.

[9] Synology. *Synology Urges All Users to Take Immediate Action to Protect Data from Ransomware Attack*. 23 juil. 2019. URL : https://www.synology.com/en-us/company/news/article/2019JulyRansomware/Synology%C2%AE%20Urges%20All%20Users%20to%20Take%20Immediate%20Action%20to%20Protect%20Data%20from%20Ransomware%20Attack.

[10] Malwarebytes Labs. *Cybercrime Tactics and Techniques : Ransomware Retrospective*. 8 août 2019. URL : https://resources.malwarebytes.com/resource/cybercrime-tactics-and-techniques-ransomware-retrospective/.

[11] ESET. *Android Ransomware Is Back*. 29 juil. 2019. URL : https://www.welivesecurity.com/2019/07/29/android-ransomware-back/.

[12] Les Echos. *Renault, Un Mois et Demi Après WannaCry*. 29 juin 2017. URL : https://www.lesechos.fr/2017/06/renault-un-mois-et-demi-apres-wannacry-156961.

[13] HIPAA Journal. *40% of Healthcare Delivery Organizations Attacked with WannaCry Ransomware in the Past 6 Months*. 31 mai 2019. URL : https://www.hipaajournal.com/40-of-healthcare-delivery-organizations-attacked-with-wannacry-ransomware-in-the-past-6-months/.

[14] Recorded Future. *LockerGoga Ransomware Disrupts Operations at Norwegian Aluminum Company*. 20 mar. 2019. URL : https://www.recordedfuture.com/lockergoga-ransomware-insight/.

[15] BleepingComputer. *New LockerGoga Ransomware Allegedly Used in Altran Attack*. 30 jan. 2019. URL : https://www.bleepingcomputer.com/news/security/new-lockergoga-ransomware-allegedly-used-in-altran-attack/.

[16] Security Boulevard. *Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread*. 16 juil. 2019. URL : https://securityboulevard.com/2019/07/ransomware-amounts-rise-3x-in-q2-as-ryuk-sodinokibi-spread/.

[17] Cybereason. *Triple Threat : Emotet Deploys TrickBot to Steal Data & Spread Ryuk*. 2 avr. 2019. URL : https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware.

[18] Cyware. *Microsoft Helping Norsk Hydro Restore Its IT Systems without Paying the Ransom*. 25 mar. 2019. URL : https://cyware.com/news/microsoft-helping-norsk-hydro-restore-its-it-systems-without-paying-the-ransom-86a32a3c.

[19] Help Net Security. *The Ransomware Attack Cost Norsk Hydro $40 Million so Far*. 27 mar. 2019. URL : https://www.helpnetsecurity.com/2019/03/27/norsk-hydro-ransomware-losses/.

[20] StateScoop. *RobbinHood Ransomware Knocks out City Services in Baltimore*. 7 mai 2019. URL : https://statescoop.com/robinhood-ransomware-knocks-out-city-services-in-baltimore/.

[21] KrebsOnSecurity. *No 'Eternal Blue' Exploit Found in Baltimore City Ransomware*. 3 juin 2019. URL : https://krebsonsecurity.com/2019/06/report-no-eternal-blue-exploit-found-in-baltimore-city-ransomware/.

[22] BankingInfoSecurity. *Baltimore Ransomware Attack Costing City $18 Million*. 7 juin 2019. URL : https://www.bankinfosecurity.eu/baltimore-ransomware-attack-costing-city-18-million-a-12584.

[23] GBHackers On Security. *UK's Biggest Forensic Firm Paid Ransom After Their Systems Lock Down*. 7 juil. 2019. URL : https://gbhackers.com/uks-forensic-firm-ransom/.

[24] Help Net Security. *Eurofins Ransomware Attack Affected UK Police Work*. 24 juin 2019. URL : https://www.helpnetsecurity.com/2019/06/24/eurofins-ransomware-attack/.

[25] BBC. "Forensic Firm Paid Ransom after Cyber-Attack". 5 juil. 2019. In : (5 juil. 2019).

[26] Cybersecurity Insiders. *Ransomware Attack on Eurofins Delays 20K Forensic Sample Research of UK Police*. 16 août 2019. URL : https://www.cybersecurity-insiders.com/ransomware-attack-on-eurofins-delays-20k-forensic-sample-research-of-uk-police/.

[27] BleepingComputer. *Maze Ransomware Demands $6 Million Ransom From Southwire*. 13 déc. 2019. URL : https://www.bleepingcomputer.com/news/security/maze-ransomware-demands-6-million-ransom-from-southwire/.

[28] BleepingComputer. *Maze Ransomware Publishes 14GB of Stolen Southwire Files*. 10 jan. 2020. URL : https://www.bleepingcomputer.com/news/security/maze-ransomware-publishes-14gb-of-stolen-southwire-files/.

[29] BleepingComputer. *Sodinokibi Ransomware Publishes Stolen Data for the First Time*. 11 jan. 2020. URL : https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-publishes-stolen-data-for-the-first-time/.

[30] 01net. *A Marseille, l'hôpital Clairval Bloqué Par Un Ransomware*. 14 août 2019. URL : https://www.01net.com/actualites/a-marseille-l-hopital-clairval-bloque-par-un-ransomware-1748901.html.

[31] BleepingComputer. *Nemty Ransomware to Start Leaking Non-Paying Victim's Data*. 13 jan. 2020. URL : https://www.bleepingcomputer.com/news/security/nemty-ransomware-to-start-leaking-non-paying-victims-data/.

[32] ZDNet. *Ransomware Infection Takes Some Police Car Laptops Offline in Georgia*. 29 juil. 2019. URL : https://www.zdnet.com/article/ransomware-infection-takes-some-police-car-laptops-offline-in-georgia/.

[33] NBC News. *Ransomware Hackers Hold U.S. Police Departments Hostage*. 26 avr. 2016. URL : https://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746.

[34] LeMonde. "Attaque informatique au CHU de Rouen : une enquête ouverte". 18 nov. 2019. In : (18 nov. 2019).

[35] [TLP:AMBER] ANSSI. *Informations Concernant Le Rançongiciel Clop - MaJ Du 29/11/2019*. 29 nov. 2019.

[36] Verint. *The Data Breach Epidemic Report*. 17 juin 2019.

[37] Eurojust. *Cybercrime : xDedic Illegal Online Marketplace Dismantled*. 28 jan. 2019. URL : http://www.eurojust.europa.eu/press/PressReleases/Pages/2019/2019-01-28.aspx.

[38] Dark Reading. *Dark Web Becomes a Haven for Targeted Hits*. 7 juin 2019. URL : https://www.darkreading.com/vulnerabilities---threats/dark-web-becomes-a-haven-for-targeted-hits/d/d-id/1334914.

[39] Sophos. *Le ransomware GandCrab tire sa révérence !* 5 juin 2019. URL : https://news.sophos.com/fr-fr/2019/06/05/ransomware-gandcrab-tire-sa-reverence/.

[40] Sophos. *GandCrab 101 : All about the Most Widely Distributed Ransomware of the Moment*. 5 mar. 2019. URL : https://news.sophos.com/en-us/2019/03/05/gandcrab-101-all-about-the-most-widely-distributed-ransomware-of-the-moment/.

[41] KrebsOnSecurity. *Is 'REvil' the New GandCrab Ransomware? —Krebs on Security*. 15 juil. 2019. URL : https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/.

[42] BleepingComputer. *A Look Inside the Highly Profitable Sodinokibi Ransomware Business*. 30 août 2019. URL : https://www.bleepingcomputer.com/news/security/a-look-inside-the-highly-profitable-sodinokibi-ransomware-business/.

[43] Help Net Security. *Weighing the Options : The Role of Cyber Insurance in Ransomware Attacks*. 27 mar. 2019. URL : https://www.helpnetsecurity.com/2019/03/27/role-of-cyber-insurance-in-ransomware-attacks/.

[44] ESET. *Two US Cities Opt to Pay $1m to Ransomware Operators*. 26 juin 2019. URL : https://www.welivesecurity.com/2019/06/26/cities-pay-ransom-ransomware-operators/.

[45] ProPublica. *The Trade Secret - Firms That Promised High-Tech Ransomware Solutions Almost Always Just Pay the Hackers*. 15 mai 2019. URL : https://features.propublica.org/ransomware/ransomware-attack-data-recovery-firms-paying-hackers/.

[46] BleepingComputer. *GandCrab Ransomware Helps Shady Data Recovery Firms Hide Ransom Costs*. 6 fév. 2019. URL : https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-helps-shady-data-recovery-firms-hide-ransom-costs/.

[47] Sophos. *Businesses Impacted by Repeated Ransomware Attacks and Failing to Close the Gap on Exploits, According to Sophos Global Survey*. 30 jan. 2018. URL : https://www.sophos.com/en-us/press-office/press-releases/2018/01/businesses-impacted-by-repeated-ransomware-attacks-according-to-sophos-global-survey.aspx.

[48] Carbon Black. *GermanWiper Ransomware*. 21 août 2019. URL : https://www.carbonblack.com/2019/08/20/cb-tau-threat-intelligence-notification-germanwiper-ransomware/.

[49] Sophos. *SamSam The Almost Six Million Dollar Ransomware*. 1er août 2018.

[50] US District Court of New Jersey. *Indictment : Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri*. 26 nov. 2018. URL : https://www.justice.gov/opa/press-release/file/1114741/download.

[51] NJCCIC. *Bit Paymer*. 29 août 2017. URL : https://www.cyber.nj.gov/threat-profiles/ransomware-variants/bitpaymer.

[52] Dark Reading. *BitPaymer Ransomware Operators Wage Custom, Targeted Attacks*. 18 juil. 2019. URL : https://www.darkreading.com/attacks-breaches/bitpaymer-ransomware-operators-wage-custom-targeted-attacks/d/d-id/1335298.

[53] ESET. *Dridex Authors Return with a New Chapter in Their Malware Story*. 26 jan. 2018. URL : https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/.

[54] CrowdStrike et Bex Hartley. *Big Game Hunting : The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware*. 14 nov. 2018. URL : https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/.

[55] Morphisec. *BitPaymer Ransomware Leveraging New Custom Packer Framework Against Targets Across the U.S.* 19 juil. 2019. URL : http://blog.morphisec.com/bitpaymer-ransomware-with-new-custom-packer-framework.

[56] BleepingComputer. *Bit Paymer Ransomware Hits Scottish Hospitals*. 29 août 2017. URL : https://www.bleepingcomputer.com/news/security/bit-paymer-ransomware-hits-scottish-hospitals/.

[57] CrowdStrike. *CSA-19255 INDRIK SPIDER Demands Highest BitPaymer Ransom to Date Changes to Ransomware Observed*. 22 fév. 2019.

[58] Crowdstrike. *CrowdStrike Discovers New DoppelPaymer Ransomware & Dridex Variant*. 12 juil. 2019. URL : https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/.

[59] ZDNet. *M6, One of France's Biggest TV Channels, Hit by Ransomware*. 14 oct. 2019. URL : https://www.zdnet.com/article/m6-one-of-frances-biggest-tv-channels-hit-by-ransomware/.

[60] CrowdStrike. *Big Game Hunting with Ryuk : Another Lucrative Targeted Ransomware*. 10 jan. 2019. URL : https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/.

[61] LeMagIT. *Emotet, Trickbot : des vecteurs de diffusion du ransomware Ryuk à prendre très au sérieux*. 12 mar. 2019. URL : https://www.lemagit.fr/actualites/252459312/Emotet-Trickbot-des-vecteurs-de-diffusion-du-ransomware-Ryuk-a-prendre-tres-au-serieux.

[62] FireEye. *Pick-Six : Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware*. 5 avr. 2019. URL : https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html.

[63] BleepingComputer. *Ransomware Attack on Jackson County Gets Cybercriminals $400,000*. 9 mar. 2019. URL : https://www.bleepingcomputer.com/news/security/ransomware-attack-on-jackson-county-gets-cybercriminals-400-000/.

[64] Cyware. *'Triple Threat' Ransomware Attack Cripples Email Systems and Services of Lake City*. 11 juin 2019. URL : https://cyware.com/news/triple-threat-ransomware-attack-cripples-email-systems-and-services-of-lake-city-729e1f23.

[65] BleepingComputer. *Ryuk Ransomware Forces Prosegur Security Firm to Shut Down Network*. 27 nov. 2019. URL : https://www.bleepingcomputer.com/news/security/ryuk-ransomware-forces-prosegur-security-firm-to-shut-down-network/.

[66] BleepingComputer. *Ryuk Ransomware Adds IP and Computer Name Blacklisting*. 19 juin 2019. URL : https://www.bleepingcomputer.com/news/security/ryuk-ransomware-adds-ip-and-computer-name-blacklisting/.

[67] Tencent. 腾讯御见威胁情报中心. 16 juil. 2019. URL : https://mp.weixin.qq.com/s/IzwnUft0GpDJQ-sV-3f9eQ.

[68] CrowdStrike. *French Engineering Company Suffers Ransomware Attack*. 28 jan. 2019. URL : https://falcon.crowdstrike.com/intelligence/reports/csa-19130-french-engineering-company-suffers-ransomware-attack.

[69] ALTRAN TECHNOLOGIES. *Information on a Cyber Attack*. 28 jan. 2019.

[70] CrowdStrike. *CSA-19383 Norwegian Aluminum and Energy Company Experiences Ransomware Infection | Reports | Intelligence | Falcon*. 19 mar. 2019. URL : https://falcon.crowdstrike.com/intelligence/reports/csa-19383-norwegian-aluminum-and-energy-company-experiences-ransomware-infection.

[71] ComputerWeekly. *Norsk Hydro Cyber Attack Could Cost up to $75m*. 23 juil. 2019. URL : https://www.computerweekly.com/news/252467199/Norsk-Hydro-cyber-attack-could-cost-up-to-75m.

[72] Motherboard. *Ransomware Forces Two Chemical Companies to Order 'Hundreds of New Computers'*. 23 mar. 2019. URL : https://motherboard.vice.com/en_us/article/8xyj7g/ransomware-forces-two-chemical-companies-to-order-hundreds-of-new-computers.

[73] Wired. *Meet LockerGoga, the Ransomware Crippling Industrial Firms*. 25 mar. 2019. URL : https://aka.cool/meet-lockergoga-the-ransomware-crippling-industrial-firms/.

[74] BleepingComputer. *FBI Issues Alert For LockerGoga and MegaCortex Ransomware*. 23 déc. 2019. URL : https://www.bleepingcomputer.com/news/security/fbi-issues-alert-for-lockergoga-and-megacortex-ransomware/.

[75] Malwarebytes Labs. *CrySIS, Aka Dharma Ransomware, Causing a Crisis for Businesses*. 15 mai 2019. URL : https://blog.malwarebytes.com/threat-analysis/2019/05/threat-spotlight-crysis-aka-dharma-ransomware-causing-a-crisis-for-businesses/.

[76] Coveware. *Dharma Ransomware Recovery Rates Fall as Ransom Demands Skyrocket*. 21 mar. 2019. URL : https://www.coveware.com/blog/dharma-ransomware-datarecovery-rates-are-decreasing-as-ransom-demands-increase.

[77] Sophos. *Inside a GandCrab Targeted Ransomware Attack on a Hospital*. 14 fév. 2019. URL : https://nakedsecurity.sophos.com/2019/02/14/inside-a-gandcrab-targeted-ransomware-attack-on-a-hospital/.

[78] FBI. *GandCrab Master Decryption Keys FLASH*. 15 juil. 2019. URL : https://assets.documentcloud.org/documents/6199678/GandCrab-Master-Decryption-Keys-FLASH.pdf.

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

[80] Heimdal Security. *Security Alert : Booking.Com Fake Emails Infect Computers with Sodinokibi Ransomware*. 18 juin 2019. URL : https://heimdalsecurity.com/blog/booking-com-fake-emails-sodinokibi-ransomware/.

[81] Dark Reading. *Attackers Exploit MSP's Tools to Distribute Ransomware*. 20 juin 2019. URL : https://www.darkreading.com/attacks-breaches/attackers-exploit-msps-tools-to-distribute-ransomware/d/d-id/1335025.

[82] BleepingComputer. *Sodinokibi Ransomware Now Pushed by Exploit Kits and Malvertising*. 24 juin 2019. URL : https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-now-pushed-by-exploit-kits-and-malvertising/.

[83] BleepingComputer. *Sodinokibi Ransomware Spreads Wide via Hacked MSPs, Sites, and Spam*. 21 juin 2019. URL : https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-spreads-wide-via-hacked-msps-sites-and-spam/.

[84] Tenable. *CVE-2019-11510 - Critical Pulse Connect Secure Vulnerability Used in Sodinokibi Ransomware Attacks*. 7 jan. 2020. URL : https://fr.tenable.com/blog/cve-2019-11510-critical-pulse-connect-secure-vulnerability-used-in-sodinokibi-ransomware.

[85] Malwarebytes Labs. *MegaCortex Continues Trend of Targeted Ransomware Attacks*. 12 juin 2019. URL : https://blog.malwarebytes.com/threat-spotlight/2019/06/megacortex-continues-trend-of-targeted-ransomware-attacks/.

[86] SC Media. *iNSYNQ Shut down by MegaCortex Ransomware*. 22 juil. 2019. URL : https://www.scmagazine.com/home/security-news/ransomware/cloud-hosting-firm-insynq-shut-down-by-megacortex-ransomware/.

[87] Sophos. "*MegaCortex*" *Ransomware Wants to Be The One*. 3 mai 2019. URL : https://news.sophos.com/en-us/2019/05/03/megacortex-ransomware-wants-to-be-the-one/.

[88] BleepingComputer. *Elusive MegaCortex Ransomware Found - Here Is What We Know*. 19 juil. 2019. URL : https://www.bleepingcomputer.com/news/security/elusive-megacortex-ransomware-found-here-is-what-we-know/.

[89] Accenture. *Technical Analysis of MegaCortex Version 2*. 5 août 2019. URL : https://www.accenture.com/_acnmedia/pdf-106/accenture-technical-analysis-megacortex.pdf.

[90] SentinelOne. *Robinhood Ransomware "CoolMaker" Functions Not So Cool*. 9 mai 2019. URL : https://www.sentinelone.com/blog/robinhood-ransomware-coolmaker-function-not-cool/.

[91] FBI. *FLASH-MC-000104-MW-Robinhood*. 5 juin 2019.

[92] BleepingComputer. *A Closer Look at the RobbinHood Ransomware*. 26 avr. 2019. URL : https://www.bleepingcomputer.com/news/security/a-closer-look-at-the-robbinhood-ransomware/.

[93] Bouygues Construction. *Information sur une cyberattaque*. 31 jan. 2020. URL : https://mediaroom.bouygues-construction.com/information-sur-une-cyberattaque/.

[94] Zataz. *Cyber attaque à l'encontre des serveurs de Bouygues Construction*. 30 jan. 2020. URL : https://www.zataz.com/cyber-attaque-a-lencontre-des-serveurs-de-bouygues-construction/.

[95] BleepingComputer. *Maze Ransomware Says Computer Type Determines Ransom Amount*. 31 mai 2019. URL : https://www.bleepingcomputer.com/news/security/maze-ransomware-says-computer-type-determines-ransom-amount/.

[96] Proofpoint. *TA2101 Plays Government Imposter to Distribute Malware to German, Italian, and US Organizations*. 14 nov. 2019. URL : https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us.

[97] SentinelLabs. *Maze Ransomware Update : Extorting and Exposing Victims*. 19 déc. 2019. URL : https://labs.sentinelone.com/maze-ransomware-update-extorting-and-exposing-victims/.

[98] Talos. *Incident Response Lessons from Recent Maze Ransomware Attacks*. 17 déc. 2019. URL : http://blog.talosintelligence.com/2019/12/IR-Lessons-Maze.html.

[99] NJCCIC. *Maze*. 27 nov. 2019. URL : https://www.cyber.nj.gov/threat-profiles/ransomware-variants/maze.

[100] BleepingComputer. *Maze Ransomware Behind Pensacola Cyberattack, $1M Ransom Demand*. 11 déc. 2019. URL : https://www.bleepingcomputer.com/news/security/maze-ransomware-behind-pensacola-cyberattack-1m-ransom-demand/.

[101] BleepingComputer. *Maze Ransomware Not Getting Paid, Leaks Data Left and Right*. 23 jan. 2020. URL : https://www.bleepingcomputer.com/news/security/maze-ransomware-not-getting-paid-leaks-data-left-and-right/.

[102] McAfee Blogs. *Clop Ransomware*. 1er août 2019. URL : https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/clop-ransomware/.

[103] BleepingComputer. *Ransomware Hits Maastricht University, All Systems Taken Down*. 27 déc. 2019. URL : https://www.bleepingcomputer.com/news/security/ransomware-hits-maastricht-university-all-systems-taken-down/.

3.2 - 05/02/2020

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