Cybersécurité : au cœur de l'industrie des ransomwares

LIVRE BLANC



STORMSHIELD

Les attaques par ransomware se multiplient et menacent l'équilibre économique et la pérennité de nombreuses entreprises et organisations. Pas une semaine ne passe sans qu'une entreprise ou qu'une administration ne fasse l'objet d'une attaque de ce type et ne reçoive la demande de rançon associée.

En 30 ans, nous sommes passés d'un programme malveillant sur disquette réclamant une centaine de dollars, à une industrie criminelle structurée qui extorque plusieurs millions chaque année. Quels sont les modes opératoires actuels des groupes de ransomwares ? Comment les cyber-criminels les déploient-ils dans les organisations ? Perturbation voire arrêt de l'activité, divulgation des données, à quels moyens de pression font-ils appel ? Et surtout, comment s'en protéger ?

Ce livre blanc revient sur l'évolution des ransomwares et des acteurs qui en font une menace de premier plan. Il décrypte le fonctionnement de ces logiciels malveillants et délivre de bonnes pratiques pour ne plus en subir les conséquences. Sans occulter la question centrale qui traverse de nombreuses structures confrontées au problème : payer ou non, faut-il céder ?

01. Du chantage au particulier au Big Game Hunting : le ransomware d'hier à aujourd'hui

08 — Des origines « pré-Internet » (1989 à 2006)
10 — Une diffusion qui surfe sur « la Toile » (2007-2013)
12 — Les premières révolutions technologiques (2013 à 2016)
14 — De premières attaques étatiques mondialisées (2017-2018)
16 — L'ère du Big Game Hunting (2019-2021)
18 — Vers la structuration de la filière cyber-criminelle (2021-2022)

02. Prix et préjudices : quelles sont les conséquences d'une attaque par ransomware ?

22 — À qui profitent les attaques de ransomwares ?
26 — Qui sont les victimes ?
28 — Quels effets sur les structures visées ?
30 — Payer ou non, faut-il céder ?

03. Dans les rouages des ransomwares : des mécaniques fluides

36 — Itinéraire d'un ransomware
38 — Focus sur les accès initiaux

04. Quelles stratégies mettre en œuvre pour faire dérailler ces machines à cash ?

44 — Se protéger avant l'attaque ransomware
44 — Limiter les dégâts pendant une attaque ransomware
44 — Se relever d'une attaque ransomware

05. Quel avenir pour les ransomwares ?

48 — À quoi ressemblera le ransomware de demain ?
50 — Quelles solutions devraient voir le jour ?



01.

Du chantage au particulier au *Big Game Hunting* : le ransomware d'hier à aujourd'hui

Outil le plus médiatisé des cyber-criminels, le ransomware peut perturber n'importe quelle entreprise ou collectivité, quels que soient sa taille et son niveau de sécurisation. Comment cette menace a-t-elle évolué au cours des trente dernières années ? Retour sur un phénomène en perpétuel changement.

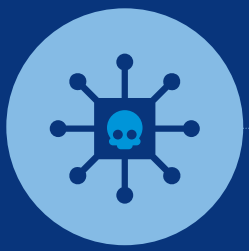
L'évolution des ransomwares à travers le temps



1989-2006

DES ORIGINES "PRÉ-INTERNET"

AIDS TROJAN, PGPCODER



2007-2013

UNE DIFFUSION QUI SURFE SUR "LA TOILE"

WINLOCK



2013-2016

LES PREMIÈRES RÉVOLUTIONS TECHNOLOGIQUES

CRYPTOLOCKER, SYPENG



2019-2021

L'ÈRE DU BIG GAME HUNTING

MAZE



2017-2018

DES PREMIÈRES ATTAQUES ÉTATIQUES MONDIALISÉES

WANNACRY, NOTPETYA.



2021-2022

VERS LA STRUCTURATION DE LA FILIÈRE CYBERCRIMINELLE

RANSOMWARE-AS-A-SERVICE.

1.1
Des origines « pré-Internet » (1989 à 2006)



1989

Les tous premiers ransomwares sont apparus à la fin des années 1980. Une seule mission pour ces logiciels malveillants : bloquer le fonctionnement du poste de travail au sein des entreprises et chez les (rares) particuliers équipés de micro-ordinateurs.

Mais les rançonneurs sont à l'époque relativement faciles à tracer grâce aux informations de paiement. Ce n'est que quinze ans plus tard, avec l'émergence des monnaies numériques, que les ransomwares vont réellement proliférer. Parmi les premiers ransomwares distribués par Internet, PGPCoder, ou « le ransomware à 20 $ », a eu pour but dès 2005 d'infecter des systèmes Windows en ciblant les fichiers aux extensions les plus communes comme .rar, .zip, .jpg, .doc ou .xls. —

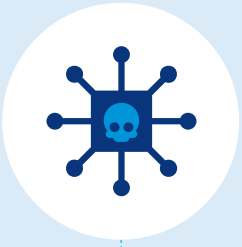
DATE CLÉ

Le tout premier ransomware, « AIDS Trojan » est expédié en 1989 via disquettes. Il chiffre les fichiers des machines qu'il infecte au bout d'un certain nombre de redémarrages et les victimes sont sommées de verser une rançon de 189 $ pour récupérer leurs données.

2007-2013

Une diffusion qui surfe sur "la Toile"

1.2 Une diffusion qui surfe sur « la Toile » (2007-2013)



Scareware

Avec l'adoption des messageries instantanées, des réseaux sociaux, des forums ou encore des réseaux *peer-to-peer*, les ransomwares bénéficient de nouveaux canaux de diffusion. WinLock avait par exemple la particularité de ne pas chiffrer les données sur l'ordinateur infecté. Il bloquait l'accès à la machine en affichant une fenêtre contenant une photo pornographique et une demande de paiement via un service de SMS surtaxé.

Cette première évolution dans le fonctionnement du ransomware est baptisée « locker » pour refléter son objectif : bloquer le démarrage du système d'exploitation.

À la même époque, des variantes usurpant l'image des forces de l'ordre font leur apparition, à l'image du ransomware Reveton en 2012. Distribué sur les plateformes de *peer-to-peer* ou les sites pornographiques, il se fait passer pour le FBI en verrouillant l'ordinateur de ses victimes et en réclamant le paiement d'une « amende » de 200 $.

Par la suite, les demandes de rançons deviendront de plus en plus créatives pour augmenter leurs chances de réussite. —



MOT CLÉ

Scareware : méthode de chantage de type faux antivirus très en vogue dans les années 2010.

2013-2016

Les premières révolutions technologiques

1.3 Les premières révolutions technologiques (2013-2016)



Le ransomware CryptoLocker marque un tournant technologique en 2013 avec son serveur de command & control qui permet de discuter avec la victime et exercer encore plus de pression. C'est également l'un des premiers ransomwares à exiger une rançon en bitcoin.

Car les crypto-monnaies vont marquer une nouvelle étape-clé dans l'évolution des ransomwares. Avec elles – et notamment l'avènement du Bitcoin –, l'anonymisation des destinataires des fonds va rendre la demande de rançon intraçable. En parallèle, des ransomwares comme Sypeng conduisent les premières attaques sur tablettes et mobiles Android en 2014 via de faux messages de mise à jour du logiciel Adobe Flash. En 2016, s'ouvre l'ère des attaques de phishing avec Petya, qui cible les adresses de messagerie professionnelles et se dissimule à l'intérieur d'un document Word ou PDF. —



27 m$

CHIFFRE CLÉ

C'est le montant généré par CryptoLocker au cours des deux premiers mois d'exploitation.

2017-2018

De premières attaques étatiques mondialisées

1.4 De premières attaques étatiques mondialisées (2017-2018)



Suite à la publication de vulnérabilités Zero-day dérobées à une agence gouvernementale américaine, les attaques par ransomware gagnent en capacité technique de propagation : elles se répandent massivement d'une entreprise à une autre dès lors que les réseaux cohabitent.

WannaCry est lancé en 2017 et suscite une grande couverture médiatique. En quelques semaines seulement, il touche 300 000 ordinateurs dans 150 pays en se propageant sur les systèmes d'exploitation Microsoft Windows par l'intermédiaire de la vulnérabilité EternalBlue.

Quelques mois plus tard, certains des éléments fondateurs de WannaCry (exploitation EternalBlue, déplacement latéral) seront réutilisés par le ransomware NotPetya dans le contexte du conflit étatique entre la Russie et l'Ukraine. Véritable arme de destruction numérique, ce ransomware a également camouflé les tentatives de sabotage du métro ukrainien[1], de l'aéroport de Kiev, de la centrale nucléaire de Tchernobyl[2], de la banque centrale ou encore de l'opérateur national d'énergie.

Aujourd'hui encore, des acteurs comme le groupe chinois Bronze Starlight continuent d'utiliser des campagnes de ransomwares pour dissimuler des opérations d'espionnage.

En 2018, le monde de la cybersécurité découvre ensuite le rançongiciel Ryuk qui cible particulièrement les grandes entreprises. Et cela n'augure rien de bon pour la suite… —

« Le ransomware n'était qu'une façade. Le véritable but de NotPetya n'était pas l'extorsion d'argent, mais la destruction de données, et ceci à très grande échelle en ciblant tout un pays. »

PIERRE-OLIVIER KAPLAN — CUSTOMER SECURITY LAB RESEARCHER, STORMSHIELD

1.5 L'ère du Big Game Hunting (2019-2021)



Leakware

Fin 2019, le nombre d'incidents liés à des ransomwares augmente de 365 %. Pour ne pas risquer de se faire repérer par les outils de sécurité, les cyber-criminels délaissent les campagnes à grande échelle (type WannaCry) et **se concentrent sur de grandes sociétés**.

Ce mode opératoire, basé sur la reconnaissance de l'environnement et l'élaboration de scénarios d'attaques avancés, est baptisé big game hunting (chasse au gros gibier). Une stratégie payante puisque le montant moyen des demandes de rançon aurait presque triplé sur cette période, passant de 13 000 à 36 000 $[3].

Le mécanisme de double extorsion apparait également à cette période. Non seulement l'entreprise victime reçoit une demande de rançon, mais elle est menacée de la revente de ses données sur le darknet. Si ce chantage ne suffit pas à convaincre les plus réfractaires au paiement de la rançon, les cyber-criminels divulguent une partie des données critiques dérobées (code source, données clients). Certains gangs vont jusqu'à menacer les clients finaux ou les patients de ces organisations de divulguer leurs données personnelles : c'est la triple extorsion.

Parmi eux, le groupe de cyber-criminels auteur présumé du ransomware Maze. Sa particularité ? Une communication en continu avec ses victimes pour exercer une pression constante.

En 2020, l'attaque par Darkside du géant américain du transport et de la distribution de produits pétroliers, Colonial Pipeline, étoffe le tableau de chasse du *big game hunting*. Le ransomware, qui ressemble techniquement à REvil, extorque une rançon de 5 millions de dollars au passage. —

« Lorsque la pression induite par le chiffrement n'est pas suffisante, les groupes de ransomwares passent à l'extorsion en menaçant de divulguer les données exfiltrées. Et si ça ne suffit pas, ils ont également recours à des attaques type DDoS pour forcer leurs victimes à payer. »

ÉDOUARD SIMPÈRE — RESPONSABLE CYBER THREAT INTELLIGENCE, STORMSHIELD

MOT CLÉ

Module présent dans les ransomwares les plus récents pour voler des données.

À NOTER

Toujours plus de pression. Le groupe ALPHV/BlackCat publie ainsi les données dérobées sur son site .onion mais également sur un site Web classique dont le nom de domaine contient le nom de l'entreprise attaquée. Facilement consultable, il prévoit même une fonctionnalité de recherche pour que les clients de cette dernière puissent vérifier eux-mêmes si leurs informations ont fuité.

2012-2022

Vers la structuration de la filière cyber-criminelle

1.6 Vers la structuration de la filière cyber-criminelle (2021-2022)



Dernière révolution en date du mode opératoire des cyber-criminels : l'apparition des plateformes de Ransomware-as-a-Service (RaaS). Les groupes d'attaquants moins expérimentés y trouvent des ransomwares en marque blanche pour des campagnes clés en main. Contre un pourcentage de la rançon récupérée, ils bénéficient de l'infrastructure complète d'une solution malveillante développée par d'autres groupes de cyber-criminels. Une filière structurée donc, où chacun possède son rôle bien défini.

En 2021, les courtiers en accès initiaux (Initial Acces Brokers ou IAB) font leur apparition. Spécialistes de l'intrusion, ils revendent un accès aux réseaux d'entreprise à d'autres groupes malveillants, qui s'en serviront pour mener ensuite leurs propres attaques.

Cette sophistication croissante de la chaîne des attaques s'explique par l'amélioration du niveau de protection des entreprises. Malheureusement, l'industrialisation des ransomwares conduit également à la réduction des temps de déploiement[5]. Jusqu'au point où certains ne s'embarrassent plus de toutes les étapes : en mars 2022, un groupe de cyber-criminels iraniens[6] a envoyé sa demande de rançon sur l'imprimante locale d'une administration étasunienne sans avoir chiffré les postes au préalable. —

DATE CLÉ

Pendant deux jours, la Maison-Blanche a réuni des dizaines de pays, dont la France ou encore l'Allemagne, pour un sommet visant à trouver des solutions au problème mondial des ransomwares. Suffisant pour prendre enfin le sujet à bras le corps ?

CHIFFRE CLÉ

X2

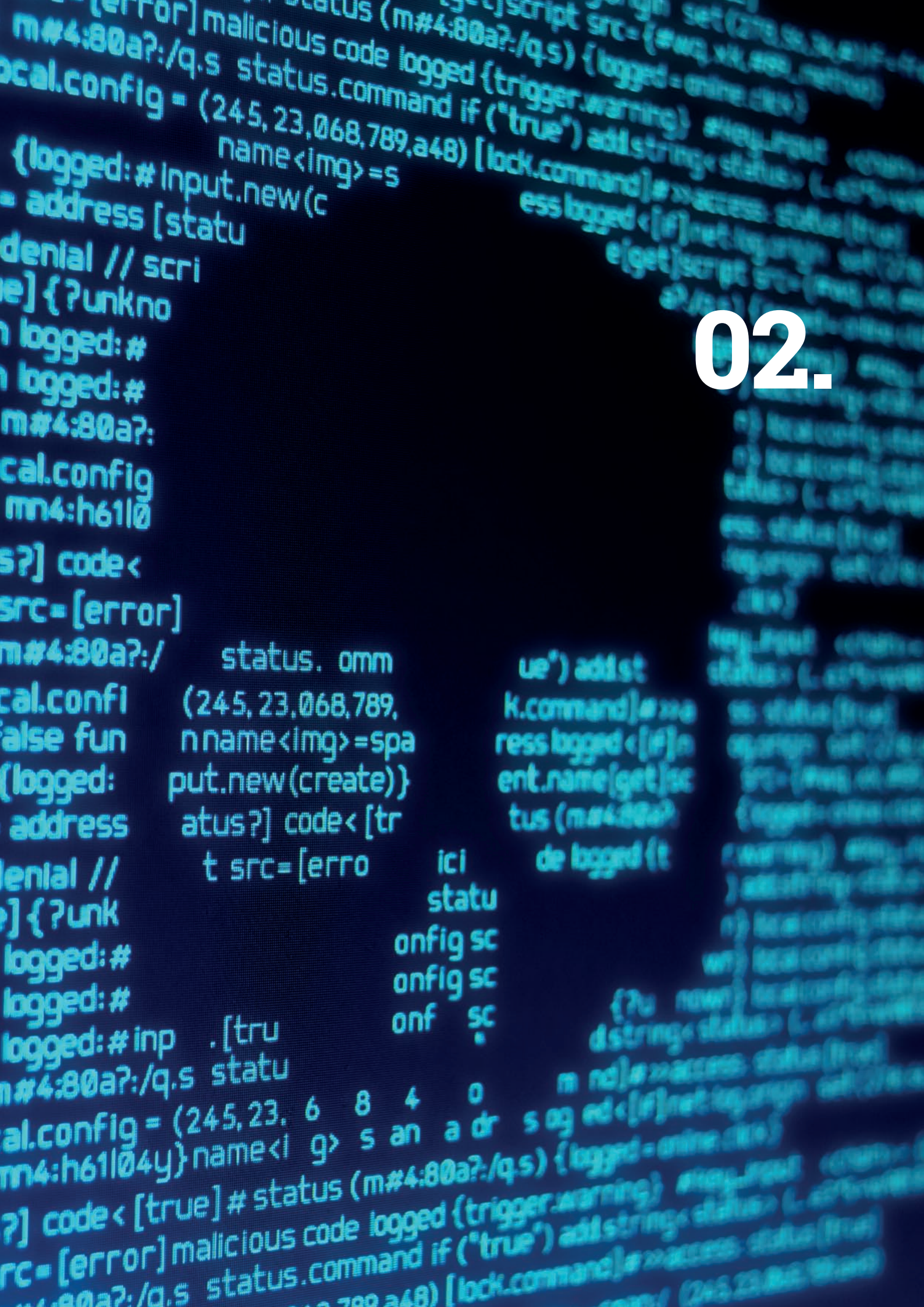
Au niveau mondial, les attaques de ransomwares ont doublé en 2021[4].

POUR ALLER PLUS LOIN

PETITE HISTOIRE DES RANSOMWARES

Retrouvez la « petite » histoire des ransomwares plus en détails dans notre article dédié[7].

Octobre 2022


02.

Prix et préjudices : quelles sont les conséquences d'une attaque par ransomware?

Une attaque par ransomware reste rarement sans conséquence pour les victimes. Au-delà des pertes financières, toute la chaîne de valeur des organisations se retrouve déstabilisée. Plongeons dans les arcanes d'une attaque, ses prix et préjudices.

2.1 À qui profitent les attaques de ransomwares?

Au cours de ces trois dernières décennies, le monde du ransomware s'est structuré. Les gangs de cyber-criminels se font et se défont mais leur montée en compétences n'est plus à démontrer.



Les groupes de ransomwares se répartissent en différentes « familles », réparties à travers le monde. Parmi les 100 familles ou variants repérés par le FBI[8], beaucoup émanent de groupes basés en Asie et en Europe de l'Est. En France, une trentaine de groupes de ransomwares sont actifs, sous des noms tristement connus LockBit, Conti, ALPHV/BlackCat ou encore Hive.

Souvent liés à l'actualité géopolitique, les groupes de cyber-criminels apparaissent et disparaissent à une vitesse effrénée. Après avoir annoncé son soutien à la Russie, le groupe Conti a connu une véritable série de fuites de données : journaux de discussion internes, code source et autres fichiers utilisés par le groupe ont ainsi été divulgué. Il a fermé son site vitrine en 2022[9] ; rapide pour un groupe découvert en 2020… Mais pourrait réapparaitre sous d'autres formes, comme le laissent présager les signes de vie donnés par sa filiale Karakurt en juin[10]. Ce qui rappelle l'exemple du groupe REvil, démantelé en janvier 2022, revenu sur le devant de la scène quelques mois plus tard[11].

En somme, l'industrie du malware se structure, et avec elle, une véritable économie parallèle de la cyber-menace émerge, avec différents métiers. Le développement du marché des cyberattaques est tel que *« nous pouvons aujourd'hui parler d'économie parallèle »* explique Sébastien Viou, Directeur Cybersécurité produits et Cyber-Évangéliste chez Stormshield. —

« Nous avons désormais affaire à une cybercriminalité organisée avec ses forums de vente qui regroupent différents profils : ceux qui trouvent les vulnérabilités, ceux qui s'introduisent dans les systèmes, ceux qui développent le malware, etc. Ces canaux permettent également de recruter des opérateurs pour réaliser l'intrusion. »

NICOLAS CAPRONI — HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

INFO CLÉ

PROFILS JUNIORS

La franchise de rançongiciels Conti forme ainsi des profils « juniors », leur propose un salaire fixe ainsi qu'un intéressement sur résultats.

PANORAMA DES GROUPES DE RANSOMWARES

Le cofondateur de Hackers sans frontières, Clément Domingo, a recensé un peu plus de la moitié des groupes de cybercriminels de la planète.

- → ALPHV
- → Ako
- → Arvin Club
- → Astro Team
- → AtomSilo
- → Avaddon
- → AvosLocker
- → Babuk
- → Babuk Locker
- → Bl4ckt0r
- → Black Shadow
- → BlackByte
- → Bonaci Group
- → CRYP70N1C0D3
- → Clop
- → Conti
- → Cuba
- → DarkLeaks
- → DarkSide
- → DoppelPaymer
- → Dotadmin
- → Egregor
- → Entropy
- → Everest
- → Exorcist
- → Grief
- → HARON
- → Hive
- → LV
- → LockBit
- → LockBit 2.0
- → LockData Auction
- → Lorenz
- → Maze
- → Medusa Locker
- → Midas
- → Mount Locker
- → Nefilim
- → Nemty
- → NetWalker
- → Night Sky
- → Pay2Key
- → payload.bin
- → Prometeus
- → Pysa (Mespinoza)
- → Qlocker
- → Quantum
- → REvil (Sodinokibi)
- → Ragnar Locker
- → Ramp
- → Ransom Cartel
- → RansomEXX
- → Ranzy Locker
- → Rook
- → Sekmet
- → Snatch
- → SunCrypt
- → Suncrypt
- → Vice Society
- → Xing

DE NOUVELLES EXPERTISES… DES DEUX CÔTÉS !

INTERVIEW **FLORENT CURTET**
— ANCIEN HACKER RECONVERTI DANS L'ACCOMPAGNEMENT DE CYBERCRISE, FORMATEUR DES FORCES DE L'ORDRE, CABINETS D'AVOCATS OU ENCORE DE DPO À CE NOUVEL ART DU POURPARLERS



→ Les acteurs du ransomware se spécialisent : développement, mise à jour, échange avec les victimes, blanchiment d'argent virtuel, à chacun son rôle à l'heure du RaaS et de l'affiliation. Côté sécurité aussi, de nouvelles compétences émergent comme l'illustre le parcours atypique de Florent Curtet, dirigeant de NeoCyber et co-fondateur de Hackers sans frontières.

Quelle a été votre plus belle réussite en matière de négociation ?

F.C. — Mes méthodes permettaient de réduire drastiquement le montant de la rançon, en passant de 1 million à 100 000 € par exemple. Il m'est arrivé de convaincre des cyber-criminels de renoncer à leur butin dans le contexte très particulier du médical.

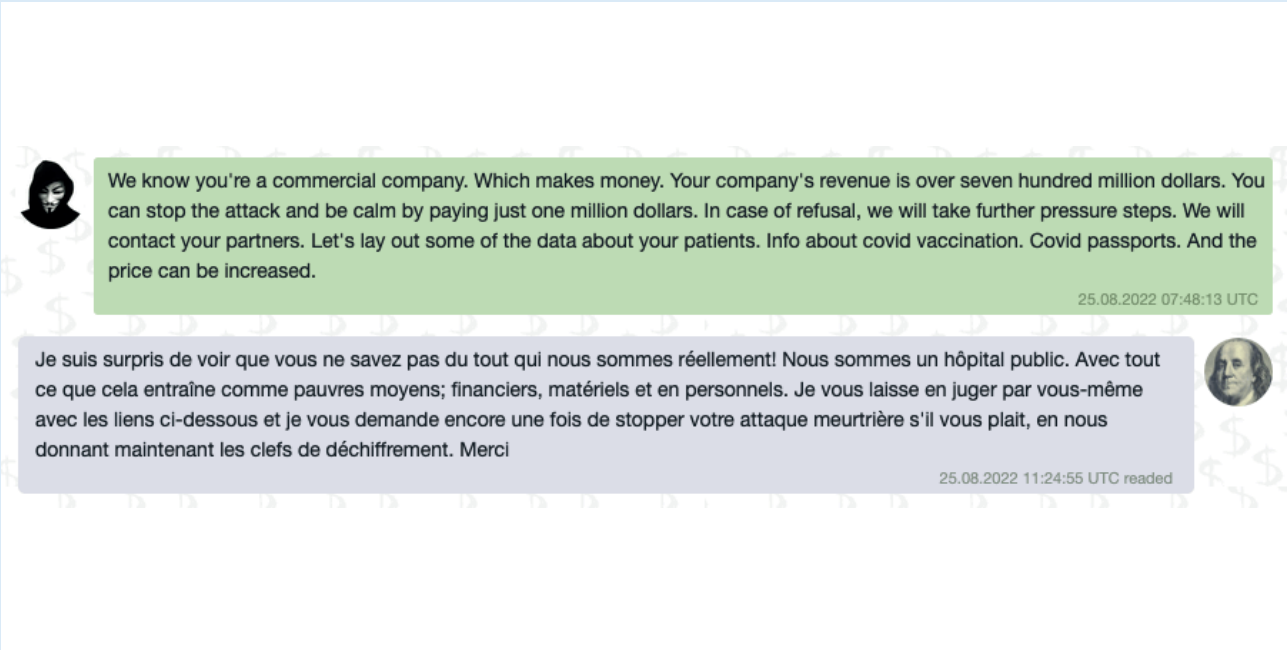
Quelles étaient ces méthodes ?

F.C. — Dans un premier temps, l'enjeu se situe au niveau des outils de communication. En général, les cyber-criminels rentrent en contact avec leur victime par mail. Mon objectif était de déplacer la conversation sur la messagerie en temps réel Tox afin d'établir une relation plus suivie. Cela permet à la fois de les occuper pour gagner du temps, de leur montrer que nous sommes là et de commencer à entrer dans leur cerveau.

Quel est le profil des cyber-criminels avec qui vous négociez ?

F.C. — Même s'ils sont souvent chapeautés par des personnes plus expérimentées, ce sont généralement encore des profils plutôt jeunes et influençables.

« Il me semble qu'il y a avait un besoin de pédagogie des deux côtés. »



LÉGENDE

Dans le cas de l'attaque du CHSF, le cyber-criminel semble persuadé d'avoir affaire à une entreprise commerciale[14].

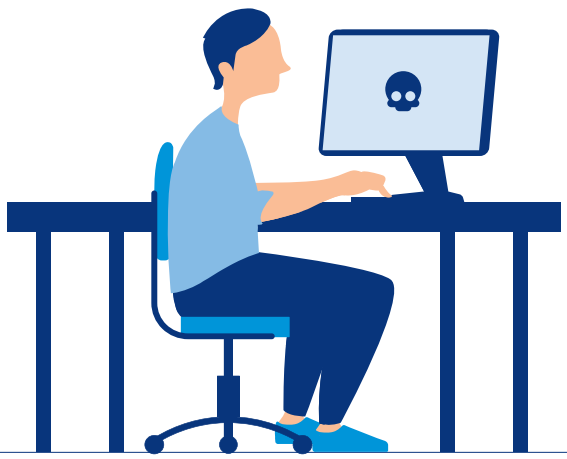
Le rôle de négociateur peut sembler trouble, surtout dans un contexte où l'ANSSI déconseille fortement le paiement de la rançon en cas d'attaque de ransomware. Pourquoi avoir choisi de développer cette expertise ?

F.C. — Il me semble qu'il y avait un besoin de pédagogie des deux côtés. Historiquement, la négociation cyber consistait surtout à expliquer à l'entreprise victime ce qu'était le bitcoin, le réseau Tor, etc. En discutant avec les cyber-criminels, je me retrouvais parfois à expliquer la différence entre chiffre d'affaires et bénéfice ou à resituer l'activité de l'entreprise.
Effectivement, nous pouvons rapidement nous retrouver dans une zone grise, d'où l'importance d'encadrer cette activité pour éviter les dérives. Pour autant, la négociation me semble une réponse pragmatique dans un contexte où certaines petites structures font face à une triple peine : blocage de leurs activités, divulgation de leurs données, voir même amende potentielle de la CNIL en cas de non-respect du RGPD. —

« Nous pouvons rapidement nous retrouver dans une zone grise, d'où l'importance d'encadrer cette activité pour éviter les dérives. »

2.2 Qui sont les victimes ?

Le ransomware a démontré sa capacité à perturber n'importe quelle entreprise et collectivité, quelle que soit sa taille et son niveau de sécurisation. Mais existe-il des profils ou des secteurs particulièrement visés ? Quelques éléments de réponse.



L'ensemble du tissu économique mondial est concerné par la menace ransomware, de la TPE au grand groupe international. En Europe, une entreprise sur deux victimes de ransomwares est une TPE-PME[15]. En France, une PME sur trois a déjà fait les frais d'une attaque de ce type[16]. Mais il ne s'agit là que de la face émergée de l'iceberg : combien de ransomware non-déclarés existe-t-il pour un seul ransomware déclaré ?

Et tous les secteurs sont concernés. Même si les attaques se font moins nombreuses en volume à certaines périodes, celles-ci sont globalement plus ciblées et concentrées sur certains secteurs, notamment le manufacturing, la tech et la finance[17].

Quand elles ne sont pas visées directement, les entreprises peuvent également subir les dommages collatéraux d'attaques par ransomware chez leurs prestataires. —

11 m$[18]

« Personne n'est à l'abri des cyber-criminels qui pratiquent aussi bien le chalutage (des attaques de masse sur des structures peu protégées afin d'interrompre leur activité), que la pêche à la ligne (des actions ciblées pour s'en prendre à l'image de marque ou au savoir-faire industriel d'acteurs mieux protégés) ».

FLORENT CURTET — DIRIGEANT NEOCYBER ET CO-FONDATEUR DE HACKERS SANS FRONTIÈRES

CHIFFRE CLÉ

C'est la somme payée par le géant brésilien de l'agroalimentaire JBS[19], paralysé en 2021 par une attaque de ransomware du groupe REvil.

SECTEURS LES PLUS IMPACTÉS PAR LES RANSOMWARES EN 2022



Source : Mid-2022 Ransomware Threat Landscape, SEKOIA.IO, 2022

2.3 Quels effets sur les structures visées ?

Au-delà des pertes de données, les organisations victimes font face à d'autres conséquences potentiellement durables : arrêt de la production, chute du chiffre d'affaires, risques juridiques, perte de confiance des clients...



2 à 3 milliards €

CHIFFRE CLÉ

C'est le coût estimé de l'attaque de ransomware qui a touché Clestra Hauserman en avril 2022. Le fabricant alsacien de cloisons de bureaux et de « salles blanches », déjà mis en difficulté par la situation économique et géopolitique, a été placé en redressement judiciaire[21] pour une durée de six mois.

Comme son nom l'indique, la suite logique d'une attaque par ransomware est la demande d'une rançon. Mais ce n'est pas l'unique conséquence pour les victimes. Dans la plupart des cas, elles ne pourront que constater la perturbation voire l'arrêt de leur production. Celle-ci entrainera à son tour une perte de chiffre d'affaires voire la fermeture de l'entreprise dans les cas les plus extrêmes.

Et les données ne sont pas épargnées. Elles peuvent être menacées de divulgation, endommagées voire détruites. Dans tous les cas, quand les cyber-criminels accèdent aux données, ils exposent les entreprises victimes à un risque juridique en cas de manque avéré au RGPD. Enfin, la réputation d'une entreprise est bien souvent mise à mal par une attaque de ransomware.

Parmi les conséquences plus indirectes, des chercheurs[20] ont indiqué que la pression qui pèse sur les professionnels de la sécurité informatique du fait de la menace ransomware participe à l'augmentation du turnover au sein de ces équipes. —

+71%

CHIFFRE CLÉ

DES MONTANTS DE RANÇONS QUI GRIMPENT, QUI GRIMPENT…

$500 en 2016, $300 000 en 2020, près de $1 million sur les 5 premiers mois de 2022 (soit +71 % par rapport à 2021).

POUR ALLER PLUS LOIN

EFFETS PSYCHOLOGIQUES

La conséquence de tous les impacts d'une cyberattaque par ransomware est évidemment d'ordre financier. Mais est-elle vraiment la seule ? Ce serait oublier les dimensions sociétales et psychologiques des attaques, (trop) souvent négligées.

2.4 Payer ou non, faut-il céder ?

Payer ou ne pas payer ? Céder ou non à une demande de rançon ? Cette question épineuse a rendu insomniaque un bon nombre de décideurs.
Car cette prise de décision engage la santé financière de la structure, son activité, mais aussi sa réputation et son éthique.



CHIFFRE CLÉ

80%

Environ 80 % des entreprises qui payent la rançon demandée subissent une nouvelle attaque par la suite[23].

Qui sont les entreprises qui payent la rançon demandée ? La réponse s'avère délicate car peu d'entre elles reconnaissent l'opération. Déchiffrer plutôt que de reconstruire, ou même de disparaître : les plus petites structures n'hésiteront pas longtemps puisque leur survie peut en dépendre... Les entreprises de plus grande envergure plieront davantage pour des questions de réputation ou de résultats financiers. Quelle qu'en soit la raison, le paiement d'une rançon reste souvent le dernier recours. Il est d'ailleurs important de rappeler également qu'avoir déjà fait les frais d'un ransomware ne protège en rien d'une nouvelle attaque. Une entreprise britannique[22] a ainsi été contrainte de payer deux fois une rançon à quelques semaines d'intervalle.

En France, le feu vert accordé par le ministère de l'Économie à l'indemnisation des rançons par les assureurs, sous condition de dépôt de plainte, pourrait avoir des effets pervers, en plus de brouiller le message de l'autorité nationale sur le sujet, l'ANSSI[24]. —

« Le texte a le mérite d'exister et faire parler en hauts lieux du sujet, mais il ne changera pas le problème de fond. Un point positif est qu'il devrait mettre un terme aux opérations de paiement de rançon "sous le manteau" pour éviter les potentielles sanctions de la CNIL.[25] »

SÉBASTIEN VIOU — DIRECTEUR CYBERSÉCURITÉ PRODUIT & CYBER-EVANGÉLISTE STORMSHIELD

PODCAST

RANSOMWARES : FAUT-IL S'ASSURER ET PAYER ?

Sur cette question épineuse, quoi de mieux qu'un podcast entre experts ? Des échanges sur le bien-fondé de ce projet législatif avec Valéry Rieß-Marchive, rédacteur en chef du MagIT, Fabrice Epelboin, Damien Douani et Bertrand Lenotre[26].

ACTU

L'INDEMNISATION DES ENTREPRISES VICTIMES DE RANSOMWARES : LE SUJET DÉLICAT DE LA CYBER-ASSURANCE



Tout a commencé en juin 2021. Bruno Le Maire, ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique et la direction générale du Trésor forment un groupe de travail sur le développement d'une offre assurantielle de couverture des risques cyber, associant services de l'État, représentants des entreprises, organismes d'assurance et de réassurance et experts du monde académique.

Un plan d'action se dessine autour de 4 axes :
- → **Clarifier le cadre juridique de l'assurance du risque cyber,**
- → **Mieux appréhender et mesurer le risque cyber,**
- → **Améliorer le partage du risque entre assurés, assureurs, et réassurés,**
- → **Accroître les efforts de sensibilisation.**

Suite à ce rapport, le ministère de l'Economie et des Finances propose en Conseil des ministres, fin 2022 une mesure dédiée aux cyber-rançons au sein du projet de loi d'orientation et de programmation du ministère de l'Intérieur (LOPMI). Seule condition : que l'entreprise victime porte plainte dans les 48h après la découverte de l'attaque informatique. Par la suite, le texte retenu par la Commission des Lois (au sein de l'Assemblée nationale) ne comporte plus le mot rançon mais emploi une terminologie plus large des dommages causés par une cyberattaque.

De nombreuses voix se sont élevées à la publication de ces informations en soulignant plusieurs risques et zones d'incertitudes quant à cette approche. Des incertitudes qui concernent la rançon elle-même : qui va payer ? Est-ce l'entreprise en direct ou un intermédiaire comme un négociateur par exemple ? Quel encadrement de ces derniers ? Quels montants pour le remboursement ? Et les conséquences possibles : est-ce que le montant des rançons va augmenter ? Est-ce que les entreprises françaises vont être davantage ciblées ? S'il est encore trop tôt pour y répondre, ces questions resteront centrales à l'avenir.

Quand d'autres soulignent au contraire un aspect bénéfique au paiement des rançons (comme un meilleur examen des flux financiers, qui peuvent devenir des faisceaux d'indices dans la traque des cyber-criminels), le débat reste plus que jamais ouvert. —

INTERVIEW

RANÇON : PAYER OU NE PAS PAYER, LA QUESTION SE POSE-T-ELLE ENCORE AUJOURD'HUI ?

→ La recommandation officielle de l'ANSSI est sans équivoque : il ne faut pas payer la rançon demandée. Pourtant, en France en 2021, une entreprise attaquée sur cinq a cédé. Pourquoi ?

POURQUOI NE FAUT-IL PAS PAYER LA RANÇON ?

« Beaucoup d'entreprises pensent qu'il s'agit de la meilleure façon de rétablir le service au plus vite. Mais ce n'est pas forcément le cas. Bien souvent, l'outil de déchiffrement conçu par l'attaquant présente des bugs. De plus, le déficit de confiance oblige à passer par une phase d'analyse avant de restaurer les données. Il faut avoir en tête que la restauration des données reste la méthode la plus sûre de retrouver ses données : en moyenne, seules 54 % des structures qui payent retrouvent leurs données. »[28]

ARNAUD PILON —
DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

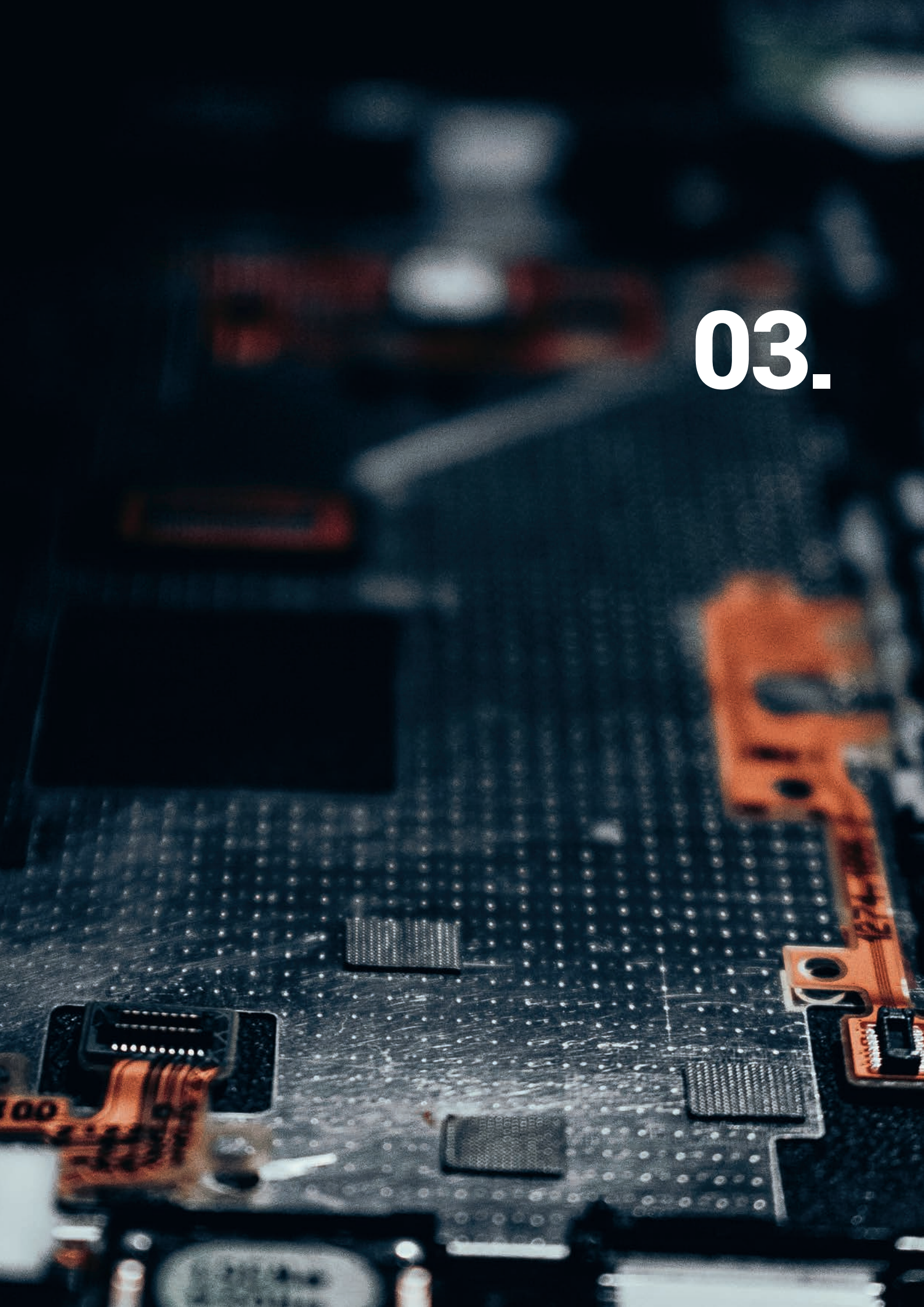
« D'un point de vue éthique, le paiement peut aussi être considéré comme une validation du modèle. C'est d'ailleurs de là que nait la polémique autour du modèle de risques des assureurs. »

NICOLAS CAPRONI —
HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

POURQUOI CERTAINES ENTREPRISES N'ONT-ELLES PAS LE CHOIX ?

« Les victimes sont parfois de toutes jeunes entreprises qui n'ont pas encore pu investir dans la sauvegarde de leurs données. Pour elles, le paiement est une question de survie. Plutôt que de condamner ces structures acculées, les autorités pourraient utiliser le suivi des paiements pour démanteler des gangs de ransomwares. Et réfléchir en parallèle à la mise en place d'une sorte de contrôle technique cyber. Pourquoi ne pas mettre en place un crédit d'impôt permettant d'auditer la sécurité des jeunes entreprises ? »

FLORENT CURTET —
DIRIGEANT DE NEOCYBER ET CO-FONDATEUR
DE HACKERS SANS FRONTIÈRES



03.

Dans les rouages des ransomwares : des mécaniques fluides

Différents terminaux peuvent être ciblés par un ransomware : un poste de travail, un téléphone portable, un automate dans une usine, un vélo connecté dans une salle de sport… Mais que se passe-t-il concrètement lors d'une attaque de ce type ?

3.1 Itinéraire d'un ransomware

Comment se propage le ransomware ? Quels sont ses principaux ressorts ? Accès initiaux et infection, camouflage, recherche de vulnérabilités exploitables… Le processus compte plusieurs phases, stratégiques et bien rodées.



Historiquement, le terme « ransomware » désignait principalement les « blockers » qui bloquaient les accès au système et les « crypto » qui chiffraient les données.

Aujourd'hui, il s'applique à tous les programmes qui permettent l'extorsion. Il s'agit d'un type d'attaque complexe qui repose sur différents mécanismes et différentes temporalités. Néanmoins ces attaques partent toujours d'une infection initiale. Celle-ci peut être réalisée par phishing, téléchargement peer-to-peer, téléchargement furtif (drive by download), l'exploitation d'une vulnérabilité, etc.

Vient ensuite la phase d'attaque à proprement parler durant laquelle le « dropper » crée une porte dérobée sur le système qui permettra d'installer tous les outils nécessaires à l'attaque, en passant les mécanismes de détection, avant que le « loader » ne s'assure de sa bonne exécution.

Après cela, le cyber-criminel entre dans la phase de Defense Evasion pendant laquelle il va chercher à couvrir les traces de son intrusion pour que la porte dérobée survive au redémarrage. La phase suivante, *Credential access*, consiste pour l'attaquant à récupérer des accès en volant des noms de comptes et des mots de passe. S'ouvre alors une phase de quelques heures à quelques mois (*Discovery* ou découverte réseau) durant laquelle les cyber-criminels recherchent des portes d'entrée afin de s'étendre par des mouvements latéraux. Ces portes d'entrée peuvent être autant des mots de passe volés au préalable, des vulnérabilités exploitables ou encore des mauvais paramètres de sécurité. Ils identifient ensuite les fichiers comportant des données de valeur (*Collection*) et procèdent à leur chiffrement, parfois en les exfiltrant au préalable et en effaçant les sauvegardes.

La dernière étape vise à mettre la pression sur la victime via la publication d'éléments de preuve de l'attaque, comme des captures d'écran sur le site Web du gang, le plus souvent sur le réseau Tor. Parfois, les cyber-criminels mènent également une attaque par déni de service en parallèle. Une pression supplémentaire pour inciter la victime à payer plus vite, et pour éviter également que la société ne communique sur son site institutionnel par exemple. —

MOT CLÉ

Le dropper (injecteur en français) est un programme informatique conçu pour installer un logiciel malveillant sur un système. Le loader s'occupe quant à lui d'assurer son exécution.

Dropper

COMMENT EXPLIQUER SIMPLEMENT LE MÉCANISME DU RANSOMWARE ?

INITIAL ACCESS

↓

EXECUTION
COMMAND- LINE INTERFACE

↓

PERSISTENCE

↓

PRIVILEGE ESCALATION

↓

DEFENSE EVASION
COMPILED HTML FILE

↓

CREDENTIAL ACCESS
PRIVATE KEYS

↓

DISCOVERY
PROCESS DISCOVERY

↓

LATERAL MOVEMENT

↓

COLLECTION
DATA FORM LOCAL SYSTEM

↓

COMMAND AND CONTROL

↓

EXFILTRATION
DATA COMPRESSED

↓

IMPACT
DATA ENCRYPTED FOR IMPACT

Source : framework MITRE ATT&CK

3.2 Focus sur les accès initiaux

Une fois l'entreprise victime identifiée, le cyber-criminel commence donc un travail minutieux pour s'introduire dans le système d'information de l'entreprise. En quête d'un précieux sésame : les fameux accès initiaux.





Une fois l'entreprise victime identifiée, le cyber-criminel commence donc un travail minutieux pour s'introduire dans le système d'information de l'entreprise. En quête d'un précieux sésame : les fameux accès initiaux.

Ces accès sont la pierre angulaire des groupes de ransomware, puisqu'ils vont servir à s'introduire dans le système d'information de leurs victimes en devenir. Et nécessitent une longue phase de reconnaissance. « *L'étude des cibles va plus loin que la seule étude technique de la surface d'attaque exposée sur Internet,* détaille Valéry Marchive dans un article[29] publié sur Le Mag IT. *Et il s'agit notamment d'obtenir des coordonnées permettant de contacter chacune des personnes identifiées. Probablement pour faire pression après le déclenchement du rançongiciel.* »

Pour récupérer toutes ces données, plusieurs techniques sont déployées. Plus ou moins élaborés, les **emails de phishing** sont le vecteur classique par excellence. En parallèle, d'autres canaux sont également mobilisés pour mettre en œuvre des techniques d'ingénierie sociale similaires, comme la messagerie LinkedIn par exemple.

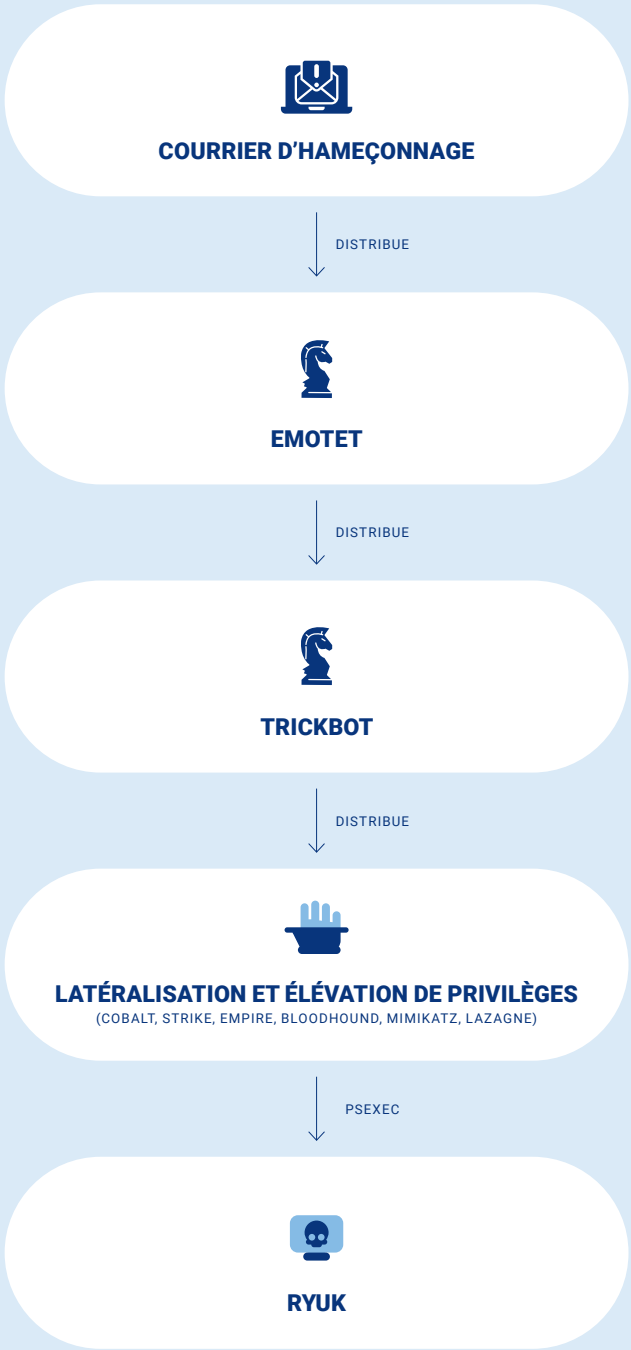
POUR ALLER PLUS LOIN

RANSOMWARE : COMMENT LES CONTI PRÉPARENT LEURS CYBERATTAQUES.

Un article pour comprendre comment le groupe Conti récupère des accès initiaux aux systèmes d'information de nombreuses organisations à travers le monde.

LE RANSOMWARE S'INTÈGRE AUSSI DANS UNE CHAÎNE PLUS COMPLEXE

DÉROULÉ SIMPLIFIÉ DE LA CHAÎNE D'INFECTION EMOTET-TRICKBOT-RYUK



Source : Rapport 'Le rançongiciel Ryuk", ANSSI, 2021

Mais les logiciels utilisés dans les entreprises peuvent également faire partie de leur surface d'attaque quand ceux-ci embarquent, sans le savoir, une vulnérabilité, souvent exploitée lors de la phase de réplication.

« Il n'est pas rare que les cyber-criminels utilisent d'autres malwares comme Emotet, Trickbot ou le loader Bumblebee en amont de leur attaque. »

NICOLAS CAPRONI — HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

« Les technologies sont devenues interfaçables. Ici, Emotet agit comme un cheval de Troie, récupère du code mis à disposition par l'attaquant, puis se propage comme un ver. C'est donc un moyen plutôt qu'une fin. Trickbot, de son côté, est un botnet qui infiltre le client, attend les instructions d'Emotet et les exécute. »

PIERRE-OLIVIER KAPLAN — INGÉNIEUR RECHERCHE & DÉVELOPPEMENT, STORMSHIELD

Autre facteur de complexification des attaques, la prolifération via la supply chain : les cyber-criminels compromettent des chaînes logistiques entières en ciblant les vulnérabilités de logiciels de gestion et/ou de services cloud. Ainsi, en mai 2021, l'éditeur de solution IT Kaseya est victime de REvil. Plus de 1 500 entreprises sont impactées, à travers les réseaux de 60 de ses clients, et la rançon demandée s'élève à 70 millions de $[30]. —

+1500

CHIFFRE CLÉ

Plus de 1 500 entreprises ont été impactées suite à l'infection d'un logiciel de l'éditeur Kaseya


04.
SYSTEM
HACKED

Quelles stratégies mettre en œuvre pour faire dérailler ces machines à cash?

Les ransomwares sont devenus la bête noire des services informatiques, et des entreprises en général. Sont-ils pour autant une fatalité ? Nous avons demandé à Sébastien Viou, Directeur Cybersécurité Produit et Cyber-Évangéliste Stormshield, quelles étaient les mesures à prendre pour faire face.

01

SE PROTÉGER AVANT L'ATTAQUE RANSOMWARE

- **SAUVEGARDER LES DONNÉES… ET PROTÉGER LES SAUVEGARDES[31]**
  « À elle seule cette précaution ne suffit pas, car c'est la première chose que le ransomware va chercher à détruire, avant même le chiffrement. Il faut avoir recours à des sauvegardes sur bande déconnectées et bien travailler la fréquence de ces sauvegardes. Il est également nécessaire de tester les restaurations pour s'assurer que les sauvegardes soient utilisables. ».

- **MAINTENIR À JOUR LES LOGICIELS ET LES SYSTÈMES**
  « Les mises à jour doivent être faites en continu et inclure les PC Windows mais également les systèmes Linux et Mac qui peuvent aussi être des points d'entrée. Tout le parc bureautique est concerné, de Microsoft Exchange à l'Active Directory en passant par l'ensemble des serveurs exposés, même petits. ».

- **CLOISONNER LE SYSTÈME D'INFORMATION**
  « Il est recommandé pour cela d'appliquer des règles strictes de flux autorisés entre différentes zones en fonction de leur criticité. »

- **LIMITER LES DROITS DES UTILISATEURS ET LES AUTORISATIONS DES APPLICATIONS**
  « Sur ce point, c'est la gestion dans le temps qui est déterminante : pour arriver à maintenir la sécurité, il faut prévoir des revues régulières. »

- **METTRE EN ŒUVRE UNE SUPERVISION DES JOURNAUX**
  « La collecte des logs est un impératif. Dans les cas où un très haut niveau de sécurité est requis, il est possible d'y ajouter une composante de détection d'intrusion via un SOC. »

- **SENSIBILISER LES COLLABORATEURS**
  « Avec l'ingénierie sociale, la principale porte d'entrée dans un système d'information d'une entreprise reste ses collaborateurs. Il est donc important de parler des sujets de cybersécurité même si la sensibilisation a ses limites. »

8%

C'est la part de collaborateurs du CERN qui ont été piégés lors d'une fausse campagne de phishing, réalisée après sensibilisation[32]

- **PENSER SA STRATÉGIE DE COMMUNICATION DE CRISE CYBER**
  « Là encore, il est utile d'avoir travaillé ses messages et ses contacts en amont pour communiquer de façon adaptée auprès des différents publics. Des communications qui servent à prévenir d'un arrêt inopiné de la production inopiné par exemple ou encore de fuites de données personnelles, comme prévu par le RGPD. »

- **METTRE EN ŒUVRE UN PLAN DE RÉPONSE AUX CYBERATTAQUES**
  « Ce plan est crucial, car il permet de réagir vite en contactant par exemple au plus tôt les sociétés de CERT préalablement identifiées. Il comporte bien évidemment un volet technique avec la mise en place de solutions de protection comme Stormshield Endpoint Security Evolution et Stormshield Network Security. »

- **ÉVALUER L'INTÉRÊT DE SOUSCRIRE À UNE ASSURANCE CYBER**
  « Certaines assurances cyber intègres des clauses de déploiement de solutions de cybersécurité ; elles sont intéressantes en ce sens, car elles imposent du coup une certaine protection. Pour autant, il ne faut pas voir l'assurance cyber comme une mesure de survie qui suffit seule, et encore moins comme une mesure qui protège. En d'autres termes, une assurance contre les ransomwares ne sera jamais une stratégie de cybersécurité. »

02

LIMITER LES DÉGÂTS PENDANT UNE ATTAQUE RANSOMWARE

- **ADOPTER LES BONS RÉFLEXES**
  « Il faut être capable de repérer rapidement que quelque chose ne va pas, et ne pas hésiter à aller jusqu'à tout débrancher pour mitiger le risque et contenir la propagation au maximum. Au niveau individuel aussi, il faut apprendre à réagir, à dire "j'ai cliqué au mauvais endroit" car chaque minute compte. »
- **PILOTER LA GESTION DE LA CRISE CYBER DEPUIS LE COMITÉ EXÉCUTIF**
- **COMMUNIQUER AU JUSTE NIVEAU**
- **DÉPOSER PLAINTE**

03

SE RELEVER APRÈS UNE ATTAQUE RANSOMWARE

- **RESTAURER LES SYSTÈMES DEPUIS DES SOURCES SAINES**
- **ENQUÊTER SUR LE CHEMIN D'ATTAQUE EMPRUNTÉ**
  « Pour comprendre le déroulé de l'attaque et les faiblesses de son propre système, il faut analyser ce qui s'est passé. Ainsi, on se donne toutes les chances d'éviter que cela ne se reproduise. »
- **ÉLABORER UN PLAN DE CORRECTION**
  « Selon les cas, peut-être faut-il mettre en place une authentification mutlifacteur ou améliorer les solutions de sécurité présentes sur les postes ? »
- **PRÉSENTER LE DOSSIER À L'ASSURANCE**
- **DÉPLOYER LE PLAN DE COMMUNICATION AUPRÈS DES CLIENTS IMPACTÉS, DE VOS INVESTISSEURS, ETC.**
- **GÉRER L'IMPACT PSYCHOLOGIQUE SUR LES COLLABORATEURS**
  « Chômage technique, culpabilité, surcharge de travail équipes IT, les ransomwares ont aussi des conséquences sur les ressources humaines, il faut les prendre en compte. »
- **ENGAGER DES POURSUITES SI CELA N'A PAS DÉJÀ ÉTÉ ENCLENCHÉ**
- **ÉTABLIR UN PLAN DE PRODUCTION POUR RATTRAPER LE RETARD ACCUMULÉ**

QUE PRÉVOIT STORMSHIELD ENDPOINT SECURITY EVOLUTION VIS-À-VIS DES RANSOMWARES ?

→ SES Evolution présente des fonctionnalités particulièrement utiles dans le cadre de la lutte contre la menace ransomware : la détection du chiffrement de fichiers, la protection des sauvegardes automatiques et face aux injections dll, l'analyse comportementale ou encore le blocage en temps réel de processus au comportement anormal. —

POUR EN SAVOIR PLUS, VISIONNEZ CETTE VIDÉO


05.

Quel avenir pour les ransomwares?

Demain, quelles suites pour les ransomwares ? S'en prendront-ils à des portefeuilles cryptomonnaies ? À des véhicules autonomes ? Les cyber-criminels utiliseront ils l'IA pour mener des attaques polymorphes ? Non, vous n'êtes pas dans une dystopie. Juste dans le monde qui vient.

5.1 À quoi ressemblera le ransomware de demain ?

Le portrait type du ransomware de demain n'est pas écrit. Mais une chose est sûre, il se complexifiera et s'adaptera à un environnement davantage sécurisé. Il cherchera aussi des entreprises plus matures et des contextes géopolitiques fragiles.



Si LockBit est actuellement la franchise de ransomwares la plus populaire, la concurrence est rude. Rien qu'au premier semestre 2022, ce sont vingt nouveaux gangs qui ont fait leur apparition.

« Nous pouvons imaginer que ces ransomwares s'en prennent demain à des portefeuilles cryptomonnaies, de NFT, des véhicules autonomes. Les technologies émergentes ne sont pas à l'abri. »

PIERRE-OLIVIER KAPLAN — CUSTOMER SECURITY LAB RESEARCHER, STORMSHIELD

La situation géopolitique et les crises économiques qui se préparent sont en effet un terreau fertile pour les ransomwares. Leurs auteurs redoublent d'investissement en R&D.

« Nos investigations techniques ont également révélé qu'un groupe de double extorsion RaaS peu connu, baptisé Vice Society, utilise des ransomwares différents en fonction des cibles et des systèmes : Zepplin pour Windows, HelloKitty pour Linux.[33] »

NICOLAS CAPRONI — HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

Ces développements restent néanmoins assez chers. Cela oblige les cyber-criminels à cibler de grandes entreprises pour amortir l'opération. —

DES NOUVELLES FAMILLES DE RANSOMWARES AU S1 2022

→ YourCyanide
→ Nokoyawa
→ Vandili
→ Pandora
→ GoodWill
→ Hermetic Ransom
→ Vulcan Ransom Team
→ Mindware
→ Cheerscrypt
→ Yashma
→ NwGen
→ Onyx
→ Axxes
→ Black Basta
→ RTM

Source : Mid-2022 Ransomware Threat Landscape, SEKOIA.IO, 2022

COMMENT TRAQUER UN RANSOMWARE?

AVEC **ARNAUD PILON** — DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

→ « Suivre l'actualité en matière de ransomware n'est pas chose facile. Nous cherchons à trouver les invariants dans les modes opératoires, les techniques, les outils, car il n'est pas rare que les différents groupes se partagent des "astuces", sur les méthodes de propagation par exemple. Nous gardons également un œil sur les campagnes de phishing, qu'il ne faut pas sous-estimer. Enfin, nous essayons d'identifier quelles vulnérabilités sont susceptibles d'être exploitées en masse. » —

5.2 Quelles solutions devraient voir le jour ?

Face à une menace qui évolue sans cesse, les solutions de protection des postes doivent suivre le même rythme. L'amélioration et la multiplication des moyens de détection est une piste à creuser, mais qui ne doit pas faire oublier les nécessaires solutions de protection.



Les ransomwares ont permis de faire parler des menaces sur les SI. Cette communication a éveillé les DSI qui ont augmenté les niveaux de sécurité. En plus de pousser les SI à plus de robustesse, la pression des ransomwares a engendré un renouveau dans l'industrie de la sauvegarde.

Ainsi, le marché des solutions de cybersécurité propose déjà un certain nombre d'outils comme l'EDR ou l'XDR qui augmentent les moyens de détection et de blocage des ransomwares. Il ne faut pas pour autant oublier que ces solutions de détection et de remédiation sont palliatives : à ce stade, la cyberattaque a déjà fait du dégât dans les entreprises. **La première étape indispensable reste bien de mettre en place des mesures de protection**

« L'enjeu de ces prochaines années est d'arriver à réduire le nombre de faux positifs sur les SI de grande taille. Cela peut passer par du machine learning mais ce n'est pas une finalité en soi. En revanche, face à l'accumulation des couches de produits de sécurité, l'amélioration de l'interopérabilité des systèmes sera déterminante. »

ARNAUD PILON — DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

(des données, des postes et des réseaux). L'orchestration des solutions est donc l'une des pistes à étudier pour réduire la fatigue du SOC.

La confiance conférée par les solutions utilisées va quant à elle devenir encore plus stratégique qu'elle ne l'est aujourd'hui. Cela devrait renforcer l'importance du schéma de qualification au niveau européen et/ou français. —

DISPOSERONS-NOUS UN JOUR D'UN « VACCIN » CONTRE LE RANSOMWARE?

ARNAUD PILON — DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), SYNACKTIV

→ ***« Hélas, les menaces s'adaptent rapidement à ce type de solution technique. Tant que ces attaques généreront de l'argent, les cyber-criminels continueront à s'adapter, investir en R&D et donc à progresser. »***

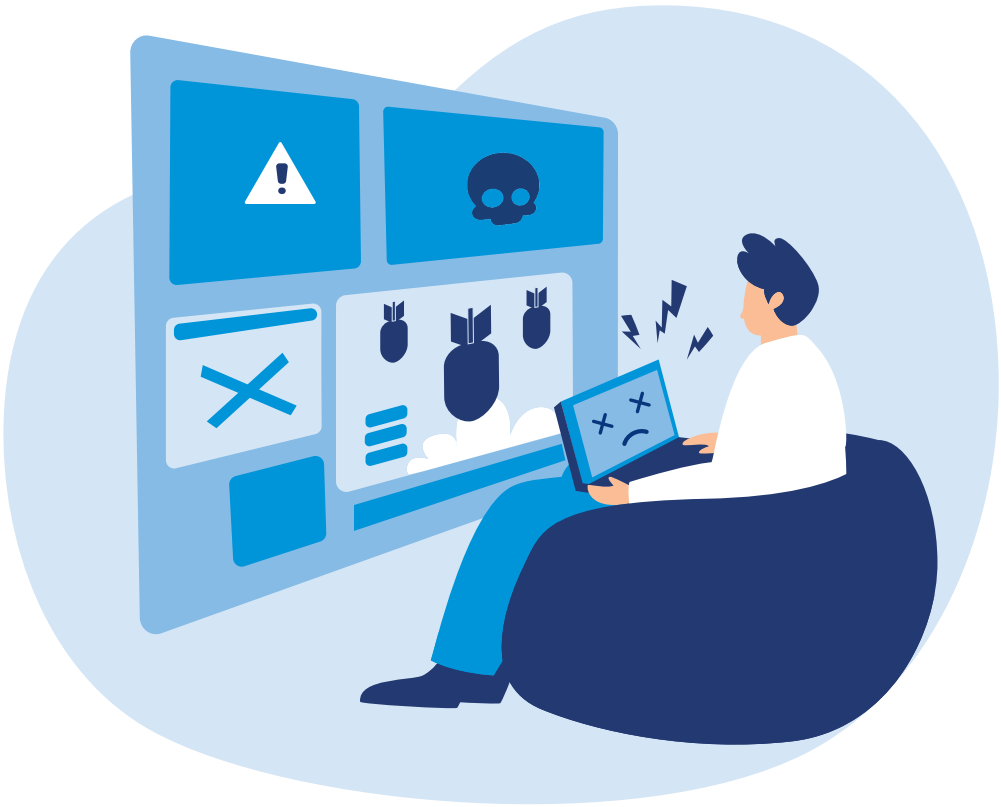
NICOLAS CAPRONI — HEAD OF THREAT & DETECTION RESEARCH (TDR) TEAM, SEKOIA.IO

→ ***« Je ne crois pas au vaccin mais je ne crois pas à la fatalité non plus. La victimologie révèle que la plupart des attaques sont opportunistes. Certes, il y aura toujours quelqu'un pour cliquer sur une pièce jointe compromise mais en alliant connaissance de la menace et outils de détection, il est possible de détecter l'attaque avant le chiffrement et l'extraction de données. »***

FLORENT CURTET — DIRIGEANT DE NEOCYBER ET CO-FONDATEUR DE HACKERS SANS FRONTIÈRES

→ ***« Il n'y a pas de solutions à moyen terme pour enrayer le phénomène, d'autant plus que le business model des rançonneurs continue d'évoluer : certains utilisent des failles très avancées et rémunèrent des "insiders" pour exécuter le virus. »***

En définitive, la veille et la victimologie sont capitales dans la lutte contre les ransomwares, car elles permettent de mieux comprendre les organisations cyber-criminelles et donc de mieux combattre cette menace. Celle-ci n'a fait que se transformer au cours des trois dernières décennies. Il faut donc s'attendre à découvrir encore régulièrement de nouvelles souches et de nouveaux variants, d'autant plus dans le contexte actuel d'émergence de nouvelles technologies et de conflits géopolitiques.



SOURCES ET ANNEXES

[1] https://www.liberation.fr/futurs/2017/06/28/notpetya-le-logiciel-ranconneur-a-propagations-multiples_1580043/
[2] https://www.leparisien.fr/high-tech/cyberattaque-les-centrales-nucleaires-francaises-sont-elles-en-securite-28-06-2017-7094979.php
[3] https://www.insurancebusinessmag.com/asia/news/cyber/ransomware-big-game-hunting-has-major-impact-on-insurers-189773.aspx
[4] https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/
[5] https://cyware.com/news/around-94-reduction-in-average-ransomware-attack-duration-ibm-f6a83827/?web_view=true
[6] https://www.zdnet.com/article/these-ransomware-attackers-sent-their-ransom-note-to-the-victims-printer/
[7] https://www.stormshield.com/fr/actus/petite-histoire-des-ransomwares/
[8] https://www.fbi.gov/news/testimony/america-under-cyber-siege-preventing-and-responding-to-ransomware-attacks
[9] https://www.zdnet.fr/actualites/le-groupe-de-ransomware-conti-ferme-son-site-vitrine-39943928.htm
[10] https://www-lemagit-fr.cdn.ampproject.org/c/s/www.lemagit.fr/actualites/252522126/Cyberattaques-Karakurt-fait-un-retour-en-fanfare?amp=1
[11] https://www.zdnet.fr/actualites/le-site-du-groupe-revil-donne-des-signes-de-vie-39940953.htm
[12] https://www.latribune.fr/technos-medias/informatique/qui-est-lockbit-3-0-le-cyber-ranconneur-de-la-poste-mobile-925065.html
[13] https://www.linkedin.com/posts/clementdomingo_cybersaezcuritaez-ransomwares-ransomgangs-activity-6985605220269441024-ZqLc
[14] https://www.lemagit.fr/actualites/252524255CHSF-lattaquant-ne-semble-pas-comprendre-que-cest-un-hopital-public
[15] https://www.ouest-france.fr/societe/cyberattaque/cyberattaques-voici-combien-les-entreprises-francaises-ont-perdu-depuis-janvier-482ff564-dfe7-11ec-b2a8-056c7579e285
[16] https://www.channelnews.fr/une-pme-francaise-sur-trois-a-deja-ete-victime-dun-ransomware-114729
[17] https://www.zdnet.com/article/ransomware-attacks-have-dropped-and-gangs-are-attacking-each-others-victims/#ftag=RSSbaffb68?&web_view=true
[18] https://www.lemondeinformatique.fr/actualites/lire-ransomware-jbs-debourse-11-m$-pour-recuperer-son-it-83225.html
[19] https://www.zdnet.fr/actualites/le-geant-de-l-agroalimentaire-jbs-vise-par-revil-39923901.htm
[20] https://www.lesechos.fr/pme-regions/grand-est/clestra-hauserman-demande-sa-mise-en-redressement-pour-trois-mois-1778519
https://www.lemoniteur.fr/article/clestra-place-en-redressement-judiciaire.2217432
[21] https://www.zdnet.com/article/the-unrelenting-threat-of-ransomware-is-driving-cybersecurity-workers-to-quit/
[22] https://securite.developpez.com/actu/313967/Victime-d-un-ransomware-une-entreprise-paie-des-millions-aux-cybercriminels-pour-restaurer-ses-fichiers-L-entreprise-se-fait-attaquer-a-nouveau-par-le-meme-ransomware-et-paie-encore/
[23] https://www.zdnet.fr/actualites/ransomware-la-double-peine-pour-les-entreprises-qui-paient-39924567.htm
[24] https://www.usine-digitale.fr/article/ransomwares-rembourser-la-rancon-un-jeu-dangereux-que-les-assureurs-continuent-de-jouer-sous-conditions.N2038932
[25] https://www.linkedin.com/posts/s%C3%A9bastien-viou-b0806861_cybersaezcuritaez-ransomware-activity-6973284015197827073-dAGn?utm_source=share&utm_medium=member_desktop
[26] https://www.zdnet.fr/actualites/ransomware-la-double-peine-pour-les-entreprises-qui-paient-39924567.htm
[27] https://www.clubic.com/antivirus-securite-informatique/actualite-442272-cybersecurite-faut-il-assurer-les-victimes-de-ransomware-le-senat-dit-oui.html
[28] https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2022.pdf
[29] https://www.lemagit.fr/actualites/252501084/Ransomware-ces-rancons-payees-qui-plaident-en-faveur-de-la-cyberassurance
[30] https://www.numerama.com/cyberguerre/738790-apres-deux-mois-dabsence-le-terrible-gang-revil-fait-un-retour-inattendu.html
[31] https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf
[32] https://www.cio-online.com/actualites/lire-experience-de-faux-phishing-au-cern-8%C2%A0-de-compromission-14450.html
[33] https://feedback.sekoia.io/changelog/11222

https://www.lesechos.fr/finance-marches/banque-assurances/
assurance-bercy-donne-son-feu-vert-a-lindemnisation-des-cyber-rancons-1786154
https://www.usine-digitale.fr/article/assurance-un-projet-de-loi-clarifie-le-cadre-
de-l-indemnisation-des-rancons-en-cas-de-cyberattaque.N2041292
https://blog.sekoia.io/vice-society-a-discreet-but-steady-double-extortion-ransomware-group/
https://www.cap-com.org/actualit%C3%A9s/20h02-la-web-serie-des-hopitaux-lyonnais-sur-la-covid-19
https://www.stormshield.com/fr/actus/50-nuances-de-ransomwares/
https://www.stormshield.com/fr/actus/vers-une-nouvelle-economie-de-la-vulnerabilite/
https://www.stormshield.com/fr/zero-ransomware/
https://www.stormshield.com/fr/ressourcescenter/ask-ze-expert-ransomware-ne-payez-pas-les-rancons/
https://www.stormshield.com/wp-content/uploads/SES-FR-Ransomware-Infographics-202204.pdf
https://www.stormshield.com/wp-content/uploads/SES-FR-LockBit2.0-ThreatAdvisory-202203.pdf
https://www.stormshield.com/fr/actus/quel-etat-des-lieux-des-ransomwares-en-2020/
https://www.stormshield.com/fr/actus/alerte-securite-snake-combattre-infection-avec-stormshield-endpoint-security/
https://www.stormshield.com/fr/actus/ransomware-robbinhood-pourquoi-baltimore-se-retrouve-sous-les-projecteurs/
https://www.stormshield.com/fr/actus/tour-dhorizon-des-ransomwares-les-plus-wtf-de-la-planete/
https://www.stormshield.com/fr/actus/les-pirates-seraient-ils-des-juillettistes/
https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/
https://www.idc.com/getdoc.jsp?containerId=US48093721
https://cyware.com/news/around-94-reduction-in-average-ransomware-attack-duration-ibm-f6a83827/?web_view=true
https://www.zdnet.com/article/
ransomware-attacks-have-dropped-and-gangs-are-attacking-each-others-victims/#ftag=RSSbaffb68?&web_view=true
https://www.zdnet.com/article/the-unrelenting-threat-of-ransomware-is-driving-cybersecurity-workers-to-quit/
https://cyware.com/news/ransomware-sprawl-fbi-finds-over-100-variants-to-be-active-88f659f6
https://youtu.be/azdrKZzyWgg
https://www.nomoreransom.org/fr/decryption-tools.html
https://www.stormshield.com/wp-content/uploads/SES-FR-LockBit2.0-ThreatAdvisory-202203.pdf
https://www.vadesecure.com/fr/blog/ransomware-as-a-service-raas-une-activite-illicite-qui-a-desormais-pignon-sur-rue
https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf
https://www.lemondeinformatique.fr/actualites/lire-4-groupes-de-ransomwares-emergents-dangereux-a-surveiller-83944.html
https://www.darktrace.com/fr/blog/les-9-stades-des-ransomwares-comment-l-ia-repond-a-chaque-etape/

LE CHOIX EUROPÉEN DE LA CYBERSÉCURITÉ

WWW.STORMSHIELD.COM

Toute diffusion, reproduction ou représentation, même partielle de ce livre blanc, à d'autres fins qu'une utilisation privative sur un quelconque support, est interdite et pourrait engager la responsabilité civile et pénale de la personne qui ne respecterait pas cette interdiction.
Copyright © 2022 Stormshield

STORMSHIELD