2023

White paper series
Édition 10

Défis et stratégies:

Considérations sur les attaques de logiciels rançonneurs dans les Amériques

OEA | Plus de droits pour plus de personnes

aws

Crédits

Luis Almagro
Secrétaire général de l'Organisation des États Américains (OEA)

Équipe technique de l'OEA
Luis Fernando Lima Oliveira
Alison August Treppel
Kerry-Ann Barrett
Mariana Jaramillo

Équipe technique de AWS
Abby Daniell
Melanie Kaplan
Camilo Gonzalez
Arturo Cabañas
Jordana Siegel

Rédaction
Jeimy Cano

Table des matières

Définitions

Charge utile
Partie d'un logiciel malveillant (code malveillant) qui exécute l'action adverse ou nuisible sur le système cible après une intrusion réussie.

Copie de sauvegarde
Copie des fichiers et des programmes effectuée pour faciliter la récupération, si nécessaire[1].

Cryptage de données
Toute procédure utilisée en cryptographie pour convertir un texte clair en texte chiffré afin d'empêcher toute personne autre que le destinataire prévu de lire ces données[2].

Cyber-hygiène
Adoption d'un état d'esprit axé sur la sécurité et d'habitudes quotidiennes permettant aux individus et aux organisations de limiter les potentielles infractions en ligne[3].

DDos (attaque par déni de service distribué)
Technique de déni de service utilisant de nombreux hôtes pour effectuer l'attaque[4].

Doxing
Action ou processus consistant à rechercher et à publier des informations privées ou identifiables sur une personne spécifique sur internet, généralement avec l'intention de nuire[5].

Exfiltration d'informations ou fuite d'informations
La copie, le transfert ou l'extraction illicites de données ou d'informations d'un serveur pour arriver entre les mains d'un tiers non autorisé.

Lien malveillant
Lien vers un site frauduleux. Il s'agit généralement d'un lien qui semble mener à un site web légitime, mais qui est en fait un faux site web[6].

Logiciel malveillant
Programme inséré dans un système, généralement de manière dissimulée, dans le but de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des applications ou du système d'exploitation de la victime, ou de la perturber d'une autre manière[7].

Logiciel rançonneur
Type de logiciel malveillant qui détourne et crypte généralement des fichiers sur un système de stockage, puis demande une rançon, habituellement par le biais de paiements en crypto-monnaies, sans garantie que tous les fichiers puissent être décryptés ou qu'ils soient restitués dans le même état.

Réseau zombie
Réseau d'ordinateurs infectés (par un code malveillant) contrôlés à distance et pouvant être contraints d'envoyer des spams, de diffuser des logiciels malveillants ou de mener une attaque DDoS, sans le consentement du propriétaire de la machine[8].

1 https://csrc.nist.gov/glossary/term/backup
2 https://csrc.nist.gov/glossary/term/encryption
3 https://www.kaspersky.es/resource-center/preemptive-safety/cyber-hygiene-habits
4 https://csrc.nist.gov/glossary/term/ddos
5 Tavella, F. (2021). Ransomware Conti: principales características y cómo operan sus afiliados. ESET. https://www.welivesecurity.com/la-es/2021/11/29/ransomware-conti-principales-caracteristicas/
6 https://www.mundopc.es/links-maliciosos-como-detectar-una-url-fraudulenta-484.html
7 https://csrc.nist.gov/glossary/term/malware
8 https://www.avast.com/es-es/c-botnet

Introduction

Selon des informations récentes publiées dans différents rapports, produits à la fois par des fournisseurs de technologies de sécurité de l'information et des autorités chargées de l'application de la loi, le **logiciel rançonneur**[4] est devenu l'un des risques les plus importants pour la sécurité mondiale, non seulement en raison de sa versatilité et de sa capacité d'action, mais aussi de son expansion et de son impact financier et réputationnel pour les entreprises (Interpol, 2020). Dans ce contexte, il est judicieux que les secteurs privé comme public se penchent sur cette menace numérique connue sous le nom de « logiciel rançonneur ».

Lorsqu'une entité est touchée par un logiciel rançonneur, la principale question qui se pose est: ***"comment répondre à un événement de sécurité lié à un logiciel rançonneur et en limiter les effets?".***[5] Cette question génère, tant dans le secteur public que dans le secteur privé, des tensions d'ampleur variable et des implications concernant la responsabilité au sein de la structure. Viennent s'ajouter d'autres implications, notamment pour les détracteurs de l'investissement dans la cybersécurité, ainsi qu'une myriade de dommages collatéraux qui servent généralement l'objectif de l'adversaire, à savoir semer la confusion et créer la division, ce qui lui donnent plus de temps pour agir et se positionner pour demander un paiement comme objectif final. Pour ces raisons, les secteurs public et privé cherchent à limiter les effets que peut avoir un logiciel rançonneur sur leurs données et leur réputation, ce qui peut susciter des incertitudes quant à la manière de gérer le logiciel rançonneur et de savoir s'il convient d'y répondre.

Lorsque la hiérarchie d'une organisation est informée de la présence d'un *logiciel rançonneur*, elle cherche généralement à comprendre quel type d'information est compromis en premier lieu, puis demande des explications techniques sur l'impact de cet événement sur les opérations et les implications juridiques potentielles qui en découlent, notamment si l'information fait l'objet d'une protection juridique particulière. Avec ces données, les organisations tentent généralement d'établir, avec toutes les personnes concernées en interne, une vue d'ensemble de ce qui s'est passé et de définir une position lui permettant d'agir de manière adéquate face le logiciel rançonneur.

Dans certains cas ces incidents de cybersécurité peuvent sérieusement porter atteinte aux organisations. Par exemple, l'extorsion au moyen de données est une forme de cybercriminalité qui repose sur la tromperie et la distraction et est liée à un modèle de comportement basé sur les besoins et les attentes des individus. En ce sens, en identifiant ce qui peut intéresser l'utilisateur cible (par exemple, l'attente d'une promotion, le versement d'une prime, le paiement d'une amende, un appel d'une institution policière, entre autres) et en établissant un lien avec le contexte actuel de la personne, les acteurs malveillants parviennent à imiter leurs actions dans un tissu social spécifique afin d'approcher leurs victimes potentielles sans qu'elles s'en aperçoivent.

4 Définition page 1

5 Les bonnes pratiques internationales développées à ce jour suggèrent de ne pas payer. Voir « Landscape for ransomware attacks », Agence européenne pour la cybersécurité (ENISA): https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

Le manque de compréhension des contrôles de sécurité par les services techniques contribue au succès de ces utilisateurs non autorisés. Si on ajoute à cela un manque d'hygiène informatique (communément appelé *cyber-hygiène*) des personnes dans le monde numérique, la confiance naïve dans les technologies disponibles, ainsi que l'augmentation des produits et services numériques déployés avec des mesures de sécurité et de contrôle limitées, les attaquants ont le scénario idéal pour se mobiliser et réaliser leurs actions et leurs plans avec peu de marge de réaction.

La présente publication vise à fournir des recommandations et des réflexions basées sur les meilleures pratiques internationales pour les décideurs des organisations des secteurs public et privé concernant une attaque de *logiciel rançonneur* et de ses implications. Il s'agit également d'illustrer le processus qui se déroule au cours de ces incidents et à fournir des pistes pour examiner comment relever ce défi, quelle marge d'action peut être dégagée et comment trouver des modèles alertant de l'avancée de ce type de menace dans une organisation.

Détournement de données: Que se passe-t-il pour l'organisation?

Le détournement de données prive les individus ou les organisations de l'un de leurs actifs les plus importants, leurs données et informations, et représente une atteinte directe qui met en péril les droits et les prérogatives des organisations et des êtres humains dans leur liberté d'action dans de la dynamique sociale. Le détournement de données et l'extorsion qui s'en suit par des tiers constituent un agissement criminel qui devra éventuellement être traité par différentes juridictions et procédures législatives afin d'être intégrée dans les systèmes juridiques nationaux et internationaux (Grimes, 2022).

Lorsqu'une organisation est touchée par un logiciel rançonneur, des dilemmes se posent et il n'y a généralement que peu de démarches juridiques qui peuvent être activées pour tenter de contenir les effets négatifs possibles (Leo et al., 2022).

D'une part, une organisation peut utiliser des politiques de cybersécurité qui, en fonction de leur portée et de leurs exclusions, peuvent l'aider à relever ce défi. D'autre part, elle peut négocier avec l'attaquant qui a capturé les données, en sachant que même si elle a les moyens de restaurer les informations, il est probable qu'elle ne pourra pas le faire. Toutefois, il est important de souligner que les meilleures pratiques et recommandations internationales ne recommandent pas de négocier avec l'auteur de l'infraction.[6] L'alternative consistant à payer n'est pas une option recommandée par les meilleures pratiques dans la lutte contre les logiciels rançonneurs (et est manifestement illégale dans un certain nombre de juridictions nationales et internationales). Toutes les mesures conventionnelles prises rendront l'organisation plus résistante face à la l'intrusion d'un logiciel rançonneur, même si cela n'empêchera pas un acteur malveillant de parvenir à ses fins de temps à autre. En outre, ces actions doivent sont conformes à la loi (à l'exception des paiements d'extorsion), ce qui permettra aux dirigeants d'avoir l'esprit tranquille en ce qui concerne la conformité et le signalement aux entités compétente.

Enfin, informer et impliquer les autorités compétentes[7] dans le cadre d'une enquête peut aider à obtenir des informations sur l'acteur de la menace afin d'utiliser différentes stratégies pour trouver l'agresseur, désactiver le mécanisme de cryptage, utiliser les canaux diplomatiques,[8] le cas échéant, et ainsi se conformer aux dispositions constitutionnelles et légales – autant de moyens à disposition pour faire face à un détournement de données.

6 https://www.nomoreransom.org/en/ransomware-qa.html
7 Les superviseurs d'un secteur particulier, la police ou les forces de l'ordre.
8 Lorsque les données compromises se trouvent dans d'autres pays ou juridictions ou y sont transférées, et qu'il devient nécessaire d'utiliser les voies diplomatiques pour coordonner l'action des services répressifs et judiciaires afin de prendre des mesures pour récupérer ou supprimer les informations.

Les *logiciels rançonneurs* forcent les professionnels de la sécurité de l'information, les avocat des entreprises et les décideurs de leur zone de confort, car si les informations ou les données compromises sont soumises à des conditions particulières de protection et de diligence, ils devront établir clairement comment répondre à la situation selon les différentes parties prenantes concernées. En conséquence, l'organisation concernée se trouvera dans une situation délicate où elle sera évaluée en fonction de ses pratiques en matière de sécurité, de respect de la vie privée et de contrôle, ainsi que par rapport à la manière dont ces pratiques ont été élaborées et mises en œuvre, sous oublier les tensions juridiques et les sanctions (généralement financières), lesquelles peuvent avoir un impact sur la réputation de l'organisation dans son secteur d'activité.

Traiter une attaque de logiciel rançonneur est un enjeu qui va au-delà du phénomène technologique en soi. Il s'agit de réaliser un examen systémique d'une problématique qui concerne les pratiques en matière de sécurité, les relations institutionnelles, les cadres juridiques, les assureurs, les vulnérabilités technologiques et, surtout, les comportements humains (Sittig & Singh, 2016).

Les *logiciels rançonneurs* obligent les professionnels de la sécurité de l'information, les juristes institutionnels et les décideurs à sortir de leur zone de confort. Pour être résiliente, il est important que chaque organisation dispose d'un plan proactif pour répondre à la situation, par exemple en suivant le processus de préparation du NIST.[9]

9 Ransomware | NIST

Intrusion de logiciel rançonneur: les deux parties de l'équation

Les actions entreprises après un détournement de données ont une certaine motivation (pas toujours économique) et conduisent à un contact direct ou indirect avec les groupes d'intérêt de la victime, afin d'initier un jeu de pressions et de tensions qui cherche à faire céder la partie visée. À cette fin, les preuves de survie, les appels menaçants et les manifestations visuelles qui génèrent de l'incertitude (photos, symboles ou biens) sont des éléments fondamentaux pour déclencher les actions nécessaires conduisant à la réalisation de l'objectif de l'agresseur.

Dans le monde numérique, les *logiciels rançonneurs* sévissent actuellement sous au moins deux formes. Le prélèvement d'informations ou de données (généralement sensibles) pour lesquelles une rançon doit être payée (en menaçant de les détruire ou les faire disparaitre en cas de non-paiement), ou l'accès à des informations sensibles ou compromettantes qui peuvent être exposées (avec une éventuelle atteinte à la réputation) en l'absence de paiement (Baykara & Sekin, 2018). Dans les deux cas, les criminels chercheront à donner à leurs victimes des preuves que la menace de l'une ou l'autre de ces actions est réelle et sérieuse, en ayant recours à l'intimidation et aux pressions et, y compris au moyen de comptes à rebours visibles, des messages vocaux modifiés pour intimider des organisations ou des individus, et des coordonnées basées sur comptes de messagerie anonymes ou jetables. Lorsqu'on analyse un incident de *logiciel rançonneur,* il convient d'évaluer les deux parties de l'équation: l'organisation (ou l'individu) ainsi que l'attaquant.

Du côté de l'individu ou de l'organisation, l'analyse de l'incident et de l'étendue possibles des dommages causés par un logiciel rançonneur peut porter sur les aspects suivants:

- Niveau d'assurance fourni par les pratiques de sécurité et de contrôle
- Niveau d'affinement et d'utilisation des technologies de sécurité et de contrôle disponibles
- Tests et enseignements tirés de l'évaluation et du suivi des plans de continuité et de reprise des activités
- Analyse du comportement de navigation et de l'utilisation d'internet
- Degré de développement de la culture de la sécurité de l'information (y compris la cyber-hygiène personnelle)
- Analyse prospective des risques latents et émergents liés au secteur d'activité de l'organisation dans le contexte de ses opérations et de ses stratégies
- Définition de l'appétit pour le risque[10] de l'entreprise (ou de la personne) (Herrera Silva, Barona López, Valdivieso Caraguay & Hernández-Álvarez, 2019)

10 Le degré de risque qu'une organisation est prête à accepter et à supporter dans la poursuite de sa mission/vision. Source: Quinn et al: Quinn et al. (2021). Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management. *NIST*. NISTIR 8286A. https://doi.org/10.6028/NIST.IR.8286A

Toute déficience ou tout résultat qui ne correspond pas à ce qui est attendu dans chacun des éléments susmentionnés sera associé à une capacité de gestion des risques limitée de l'organisation et de l'individu en ce qui concerne les précautions à prendre pour protéger les informations ou les données dont ils ont la charge ou la propriété, et pourrait être considéré comme une négligence qui pourrait être prouvée par des exercices d'audit ou des vérifications indépendantes.

Du point de vue de l'attaquant, l'analyse des capacités et du soutien disponibles pour atteindre ses objectifs peut comprendre, entre autres, les aspects suivants:

- Niveau de spécialisation et capacité à développer des renseignements
- Motivations spécifiques de l'action
- Utilisation d'outils connus ou spécialisés
- Liens avec d'autres groupes criminels
- Paiements basés en crypto-monnaies, ou monétisation par d'autres moyens.
- Schémas de comportement antérieurs
- Antécédents disponibles au niveau national ou international (Cano, 2020)

Toute information prise en compte, sur la base de la liste ci-dessus, fournira des indications et des indices permettant de suivre la trace de l'agresseur. Chacune d'entre elles contribuera à construire le puzzle consistant à relier les différentes actions de l'agresseur, afin de trouver des schémas cohérents qui permettent de reconstituer son action criminelle et donc, dans le meilleur des cas, de le localiser et de le capturer. Cet objectif n'est pas toujours atteint et, par conséquent, plus les informations obtenues sont fiables et pertinentes, plus il sera possible de dessiner des pistes face à l'incertitude générée par l'attaquant. (El-Kosairy & Azer, 2018).

Dans le monde numérique, les *logiciels rançonneurs* sévissent actuellement sous au moins deux formes. Le *prélèvement d'informations ou de données* (généralement sensibles) pour lesquelles une rançon doit être payée (en menaçant de les détruire ou les faire disparaitre en cas de non-paiement), ou *l'accès à des informations sensibles ou compromettantes* qui peuvent être exposées (avec une éventuelle atteinte à la réputation) en cas de non-paiement.

Recommandations et bonnes pratiques face à une attaque de logiciel rançonneur: *approches conventionnelles*

Lorsqu'une organisation subit une intrusion d'un *logiciel rançonneur*, elle doit considérer les deux côtés de l'équation, et non seulement se concentrer sur les dommages que cela génère en interne avec les conséquences naturelles que cela entraîne du point de vue des responsabilités individuelles et collectives, mais aussi considérer l'impact possible sur les individus au sein de l'organisation.

Un certain nombre d'agences fournissent des informations afin de mieux équiper les organisations pour faire face à ces incidents. À cet égard, il existe des mesures conventionnelles que les organisations ou les particuliers peuvent prendre en cas de détournement et d'extorsion de données. Par exemple, aux États-Unis, le Federal Bureau of Investigation (FBI) encourage les organisations à signaler les incidents liés aux logiciels rançonneurs aux services de police. L'Internet Crime Complaint Center (IC3) accepte les signalements de délits en ligne, qu'ils proviennent de la victime elle-même ou d'un tiers, et travaille avec cette dernière pour déterminer la meilleure marche à suivre à l'avenir. Dans ce cas, les informations suivantes sont essentielles pour poursuivre lancer la procédure:

1. Toute information pertinente jugée nécessaire pour étayer la plainte
2. En-tête(s) de courrier électronique
3. Informations sur les transactions financières (informations relatives au compte, à la date et au montant de la transaction, coordonnées du destinataire)
4. Nom, adresse, numéro de téléphone, adresse éléctronique, site web et adresse IP de la victime
5. Détails spécifiques sur la façon dont la victime a été affectée
6. Nom, adresse, numéro de téléphone et adresse électronique de la victime

Les recommandations suivantes sont basées sur les meilleures pratiques internationales disponibles à ce jour[11]:

• Engager ou solliciter des services spécialisés pour restaurer les données qui ont été compromises. Ces services sont coûteux et impliquent l'utilisation d'outils particuliers visant à détecter des schémas et à établir d'autres moyens d'accéder aux données, ce qui ne réussit pas toujours.

• Contacter les fournisseurs d'outils de sécurité et de contrôle, ou leurs contacts, afin d'établir des alternatives pour trouver des moyens de récupérer l'information ou une partie de celle-ci. Cette action débouche généralement sur des succès discrets et des centres de recherche peuvent y contribuer.

• Utiliser les sauvegardes d'informations existantes de l'organisation ou de l'individu, ce qui ne correspondent généralement pas à une pratique systématique et validée. Cette stratégie ne fonctionne souvent que partiellement, car la mise à jour des informations sauvegardées définit la portée et la marge de manœuvre que l'organisation ou l'individu peut avoir. L'utilisation de ces informations comme manière de recouvrer les données peut entraîner des lacunes et des différences, selon la fiabilité des supports de stockage utilisés, de la technologie utilisées pour effectuer les sauvegardes et la stratégie utilisée (sauvegarde quotidienne, incrémentale ou totale, ou utilisation d'un stockage en nuage).

• Élaborer et mettre à jour un plan de continuité des activités, qui prend en compte les informations soumises à une protection juridique (en priorité, par exemple, les bases de données contenant des informations personnelles) afin de maintenir la diligence nécessaire et la conformité réglementaire avec les autorités de surveillance de votre secteur aux niveaux national et international.

• Conserver les données cryptées (cryptées en transit et lorsqu'elles ne sont pas utilisées) sur le support de stockage établi par l'organisation/la personne (pour les cas de double extorsion : exfiltration et cryptage).

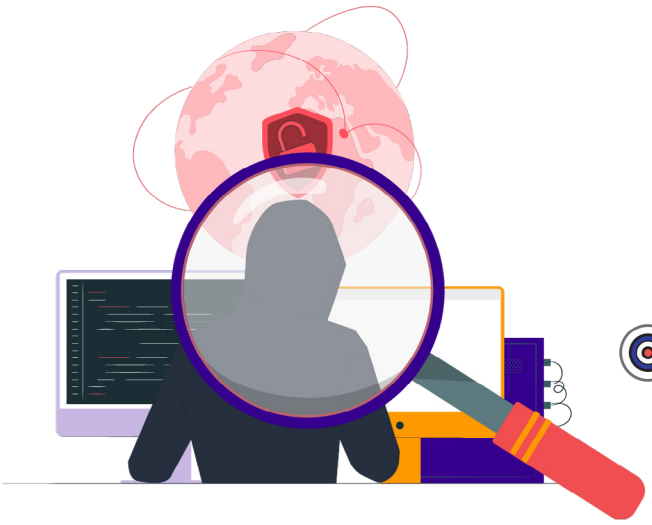
• Appliquer les correctifs (patches) ou les ajustements critiques, publiés par les fournisseurs, aux logiciels ou aux systèmes d'exploitation dont dispose l'organisation ou la personne.

• Organiser une formation et des exercices de simulation réguliers sur les stratégies utilisées par les attaquants pour tromper les individus et lancer des actions visant à l'intrusion d'un logiciel rançonneur.

• Encourager les gens à signaler tout comportement suspect sur les appareils qu'ils utilisent (désactivation de services, redémarrage, alertes antivirus, etc.).

11 Agence américaine de cybersécurité et de sécurité des infrastructures: https://www.cisa.gov/stopransomware/ransomware-guide
Agence européenne pour la cybersécurité (ENISA) : Paysage des attaques de logiciel rançonneur - https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
Centre de cybersécurité australien (ACSC) : Ransomware Attacks Emergency Response Guide - https://www.cyber.gov.au/sites/default/files/2021-07/11515_ACSC_Emergency-Response-Guide_Accessible_08.12.20.pdf

Étude de cas – Guacamaya et Conti: *Menaces présente dans la région*



Compte tenu des analyses précédentes sur les *logiciels rançonneurs*, il est important de reconnaître et d'analyser les potentiels auteurs qui peuvent se cacher derrière ces actions. Dans cette optique, nous décrivons brièvement deux études de cas leur impact pour la région.

GUACAMAYA

Selon Vicens (2022), Guacamaya est un groupe d'activistes d'Amérique centrale dont l'objectif principal est d'infiltrer les compagnies minières et pétrolières, la police et diverses agences de régulation latino-américaines afin de dénoncer les injustices de manière générale, les délits criminels contre la population, les territorialités locales et la planète. Cet acteur critique ouvertement « l'impérialisme nord-américain » et son agression contre les peuples d'Amérique.

Ce groupe d'hacktivistes cible les gouvernements, les entités étatiques, militaires et minières afin de demander une plus grande transparence de l'information sur les initiatives des États ou des institutions susmentionnées et de donner ainsi au public des détails qui ne sont pas directement divulgués.

Le mode de fonctionnement de ce groupe consiste à identifier des vulnérabilités communes ou typiques dans les infrastructures des institutions cibles, telles que des défaillances dans les mises à jour ou dans la configuration du système d'exploitation ou d'applications spécifiques, qui sont exploitées pour obtenir un accès privilégié aux informations résidant sur les appareils technologiques, puis à divulguer les informations et à les publier dans différents médias accessibles au public. En outre, ils disposent d'un portail[12] où ils conservent une trace de leurs actions et de leurs déclarations.

Parmi ses actions les plus marquantes, citons les attaques contre le secteur public au Chili, au Mexique, au Pérou, à El Salvador et en Colombie, où cette attaque par logiciel rançonneur a révélé des informations sensibles sur les gouvernements, les institutions militaires et les entreprises du secteur minier.

12 https://enlacehacktivista.org

CONTI

Contrairement au groupe Guacamaya, CONTI est une organisation criminelle transnationale qui serait originaire de Russie. Ce groupe a été détecté pour la première fois en 2020 et serait le successeur du groupe de logiciels rançonneurs Ryuk. Selon Chainalysis (2022), ce groupe de logiciels rançonneurs était le plus lucratif en 2021, avec des revenus estimés à au moins 180 millions de dollars.

Selon Tavella (2021), CONTI a souvent recours à la double extorsion, également connue sous le nom de *doxing*, qui consiste à exfiltrer des informations confidentielles de ses victimes avant le cryptage, puis à les extorquer en les menaçant de publier les informations exfiltrées si elles ne versent pas la somme d'argent demandée. Ils augmentent ainsi la pression, car il ne s'agit pas seulement de récupérer les fichiers cryptés, mais aussi d'empêcher une éventuelle fuite de données qui pourrait nuire à la victime de diverses manières.

Le mode opératoire de CONTI repose sur les activités suivantes:

- Hameçonnage des entreprises avec des pièces jointes malveillantes;
- Ciblage du collaborateurs internes à l'entreprise concernée afin de concrétiser et d'étendre leurs activités illicites;
- Exploitation de vulnérabilités connues sur des équipements exposés à internet;
- Attaques contre des ordinateurs équipés du service Remote Desktop Protocol (RDP)[13].

Le groupe criminel CONTI fonctionne comme n'importe quelle autre entreprise dans le monde. Il dispose de plusieurs départements, des ressources humaines aux administrateurs en passant par les programmeurs et les investigateurs. Il a des politiques sur la façon dont ses hackers doivent utiliser leur code et, en contrepartie, des meilleures pratiques pour cacher les membres du groupe aux forces de l'ordre (Burguess, 2022).

CONTI a été impliqué dans de nombreuses attaques très médiatisées, notamment contre la ville de Tulsa, les écoles publiques du comté de Broward et Advantech aux États-Unis. Toutefois, ce n'est qu'après avoir attaqué Health Service Executive (HSE) et le Département de la santé en Irlande, mettant hors service les systèmes informatiques du pays pendant des semaines, qu'il a gagné en notoriété (Abrams, 2022).

Récemment, CONTI a été actif en Amérique latine où son action la plus récente, révélée par les médias internationaux, a été l'attaque du 12 avril 2022 contre les bases de données du ministère des finances du Costa Rica et d'autres institutions publiques du pays, qui a conduit à la déclaration d'un « état d'urgence national dans l'ensemble du secteur public de l'État costaricien" conformément aux dispositions du décret n° 43542-MP-MICITT du 8 mai 2022.

Comme on peut le constater, Guacamaya et CONTI font peser des menaces concrètes sur la stabilité de la région, étant donné que leurs stratégies et méthodes, bien que différentes pour atteindre leurs objectifs, profitent d'une application limitée des bonnes pratiques et des normes en matière de cybersécurité au niveau des entreprises et des États, d'où la nécessité de développer et de créer des capacités conjointes pour renforcer la vigilance, permettant non seulement de répondre à ces adversaires, mais aussi de les dissuader, de les retarder ou de les déconcerter.

13 Protocole qui permet à un utilisateur à distance d'avoir un accès complet à votre appareil, de sorte qu'il peut déplacer la souris et utiliser le clavier comme s'il était devant l'ordinateur.

Un résumé des caractéristiques de ces deux groupes est présenté ci-dessous:

Caractéristiques	Guacamaya	Conti
Type d'activité	« Hacktiviste »	Criminalité organisée
Provenance	Apparemment Amérique centrale	Apparemment Russie
Techniques utilisées	Exploitation des vulnérabilités des équipements : failles concernant les mises jour ou la configuration des systèmes d'exploitation ou d'applications spécifiques.	Hameçonnage au moyen de pièces jointes malveillantes, exploitation de vulnérabilités connues, attaques de machines dotées d'un Protocole de bureau à distance (*RDP*), déchiffrage de mots de passe.
Domaine cible	Renseignement militaire, entités étatiques, sécurité nationale, compagnies minières.	Entités étatiques ou sociétés clés pour la population et le fonctionnement du pays.
Organisation	Groupe organisé et centralisé autour d'une cause commune : prétendument le bien-être social et les intérêts nationaux.	Groupe décentralisé avec des opérations au niveau mondial à des fins économiques et d'extorsion.
But	Une meilleure transparence de l'information des gouvernements et des entreprises minières.	Semer l'incertitude, l'instabilité et le chaos pour un profit économique.
Philosophie	Le piratage comme forme de résistance.	Le piratage comme moyen de déstabilisation politique et de profit.
Résultat visé	Exfiltrer des informations sensibles.	Saisir, exfiltrer et chiffrer des données pour exiger un paiement.

Tableau 1. Caractéristiques de Guacamaya et CONTI

Conclusions

Les logiciels rançonneurs représentent une forme de criminalité organisée qui résulte de la transformation numérique de la criminalité depuis plus de 10 ou 15 ans, lorsqu'elle a commencé avec les réseaux zombies (voir la section définitions). La possibilité de prendre le contrôle d'un ordinateur à l'insu de la victime est l'une des motivations des attaquants pour mener à bien des actions criminelles, en raison de l'anonymat ou de l'absence de traçabilité qui peuvent en résulter (Kardile, 2017).

Les caractéristiques actuelles de la criminalité numérique sont les suivantes: i) un anonymat maximal avec un minimum de preuves, ii) une ambiguïté juridique maximale avec un minimum de connaissances technologiques disponibles et iii) une efficacité maximale de ses actions avec un minimum d'efforts. Tout cela donne lieu à une économie de la cybercriminalité qui permet le développement de capacités techniques, sociales et de renseignement suffisamment sophistiquées pour augmenter le niveau d'incertitude pour les individus, les organisations et les pays, et ainsi lancer des actions illégales lucratives qui peuvent passer sous le radar des autorités officielles (Interpol, 2020).

Avant qu'une personne ou une organisation ne tombe victime d'un *logiciel rançonneur,* elle doit réfléchir à ses stratégies d'action afin d'établir avec clarté et recul la réponse la plus appropriée à donner pour limiter les effets négatifs d'un incident. À cette fin, il est nécessaire d'appliquer de bonnes pratiques et de réaliser régulièrement des exercices et simulations afin de générer une «mémoire procédurale et pratique» permettant d'agir de manière coordonnée en contrecarrant les objectifs de l'adversaire, à savoir générer de la confusion, de l'instabilité et de l'incertitude chez la victime.

Annexe

Liste des ressources en ligne disponibles pour lutter contre les logiciels rançonneurs

Compte tenu de l'évolution accélérée des logiciels rançonneurs au niveau international, voici un ensemble de ressources disponibles en ligne qui peuvent servir de support et d'orientation et peuvent être consultées et examinées par les décideurs afin d'agir de manière coordonnée et ciblée en dépit des tensions produites par l'incident.

- Allianz Global Corporate & Specialty (AGCS) (2021). Ransomware trends : Risks and Resilience - https://www.agcs.allianz.com/news-and-insights/reports/cyber-risk-trends-2021.html

- Cybereason (2022). Ransomware. The True Cost to Business 2022. A Global Study on Ransomware Business Impact - https://www.cybereason.com/ransomware-the-true-cost-to-business-2022

- Institute for Security and Technology (2022). Blueprint for Ransomware. Defense. An Action Plan for Ransomware Mitigation, Response, and Recovery for Small- and Medium-sized Enterprises - https://securityandtechnology.org/wp-content/uploads/2022/08/IST-Blueprint-for-Ransomware-Defense.pdf

- ThreatPost (2021). 2021: The Evolution of Ransomware - https://media.threatpost.com/wp-content/uploads/sites/103/2021/04/19080601/0354039421fd7c82eb4e1b4a7c90f98e.pdf

- NIST (2020). Data Integrity: Recovering from Ransomware and Other Destructive Events. NIST Special Publication 1800-11 - https://www.nist.gov/news-events/news/2020/09/data-integrity-recovering-ransomware-and-other-destructive-events-nist

Statistiques mondiales sur les logiciels rançonneurs

De nombreux rapports internationaux démontrent les défis et les implications de l'extorsion au moyen de données, indiquant la nécessité d'avancer et de spécifier des stratégies qui permettent d'identifier ces incidents et de les traiter de la manière la plus appropriée pour limiter les dommages. Dans ce sens, Gartner,[14] dans son rapport sur les risques émergents pour 2022 (Cohn, 2022), établit en premier lieu l'apparition de nouveaux modèles de *logiciels rançonneurs* comme la tendance que doivent surveiller les entreprises, étant donné que l'évolution permanente et la capacité des attaquants à changer leurs pratiques d'extorsion sont le signe que des alternatives et adaptations innovantes sont trouvées.

D'autre part, le site web *Cybersecurity Ventures* (2021), dans son rapport le plus récent sur l'extorsion au moyen de données, présente des statistiques indiquant qu'un logiciel rançonneur s'attaquera à une entreprise, un consommateur ou un appareil toutes les deux secondes d'ici à 2031, ce qui implique une intensification par rapport aux 11 secondes calculées en 2021. Ces données impliquent un exercice permanent d'alerte et de vigilance qui, en corrélation avec ce que Gartner a établi, nécessite un traitement différentiel et particulier étant donné la forte probabilité de succès que cette menace peut avoir.

14 Société de recherche et de conseil en technologies de l'information basée à Stamford, Connecticut, États-Unis.

D'autres rapports récents (Coverware, 2022) font état de vecteurs d'attaque utilisés par les cybercriminels, tels que l'hameçonnage, les vulnérabilités logicielles (certaines connues ou non corrigées, comme celle associée à *WannaCry*[15]) et l'utilisation du *Remote Desktop Protocol* (RDP), qui constituent la stratégie de base pour obtenir l'accès non autorisé nécessaire pour implanter le code malveillant et procéder à son exécution. Ces éléments constituent la stratégie de base pour obtenir l'accès non autorisé nécessaire pour implanter le code malveillant et procéder à son exécution. Il est important de noter que l'attaquant a besoin de l'action de la victime pour lancer le processus, de sorte que plus cette dernière résiste, plus l'adversaire devra consacrer de temps pour parvenir à ses fins.

Lorsqu'une organisation a été victime d'un logiciel rançonneur, les dommages directs sont peuvent être divisés dans au moins cinq thèmes : (SpyCloud, 2022)

- Exposition de données exclusives ou sensibles
- Atteinte à la réputation
- Effort important de récupération et de rétablissement des opérations
- Perte de clients ou de la satisfaction des clients en raison de défaillances opérationnelles
- Perturbation des services/des infrastructures critiques

Quel que soit l'impact, les organisations sont exposées et affectées en termes de confiance des clients, créant une spirale de perte de crédibilité et de contrôle qui finira par affecter la dynamique de l'entité et ses opérations numériques à moyen et long terme.

Récemment, en Amérique latine et dans les Caraïbes, des rapports ont fait état d'une importante activité d'exfiltration[16] et d'extorsion[17] au moyen de données dans la région par deux groupes particuliers appelés «Guacamaya» et «CONTI» qui, bien qu'ils aient des intentions et des méthodes différentes, ont tous deux créé de l'instabilité et des pertes financières dans de nombreux pays de la région. Leurs actions dirigées contre des entités gouvernementales, des entités de défense nationale, des infrastructures critiques et des entreprises du secteur de l'énergie et de l'exploitation minière reflètent une volonté de nuire, avec pour but non seulement d'attirer l'attention, mais aussi de mener des opérations d'extorsion lucratives afin d'accroître leurs capacités et leurs gains économiques.

> Selon les estimations, d'ici à 2031, un logiciel rançonneur s'attaquera à une entreprise, un consommateur ou un appareil toutes les deux secondes, contre 11 secondes en 2021.

15 Une vulnérabilité dans l'implémentation du protocole Server Message Block (SMB) de Microsoft est exploitée. Server Message Block (SMB) est un protocole réseau qui permet le partage de fichiers, d'imprimantes, etc., entre les terminaux d'un réseau d'ordinateurs utilisant le système d'exploitation Microsoft Windows. Source: https://www.avast.com/es-es/c-eternalblue

16 Voir la section des définitions.

17 Détournement de données ou d'informations pour lequel une rançon est demandée, généralement payée en crypto-monnaie.

Anatomie d'un logiciel rançonneur: degré d'exploitabilité et étapes clés

D'un point de vue pratique, l'extorsion au moyen de données nécessite de comprendre le niveau d'exploitabilité de l'organisation cible face à cette menace. Il s'agit de connaître et d'identifier les éléments suivants: (Stallings, 2019)

- **Vecteur d'attaque:** proximité de l'attaquant avec le composant vulnérable
- **Complexité de l'attaque:** le niveau de difficulté requis par un attaquant pour exploiter une vulnérabilité une fois l'élément cible identifié.
- **Privilèges requis:** accès nécessaire à un attaquant pour exploiter une vulnérabilité.
- **Interaction avec l'utilisateur:** indique si un utilisateur autre que l'attaquant doit être impliqué pour que l'attaque réussisse.

En ce sens, pour que l'extorsion au moyen de données réussisse, il est nécessaire que la personne participe directement, c'est-à-dire qu'elle effectue une action concrète sur son ordinateur ou son appareil, par exemple en cliquant sur un lien malveillant (voir la section des définitions), afin de disposer d'une base pivot pour lancer les trois étapes clés de la matérialisation de la menace (figure n° 1).

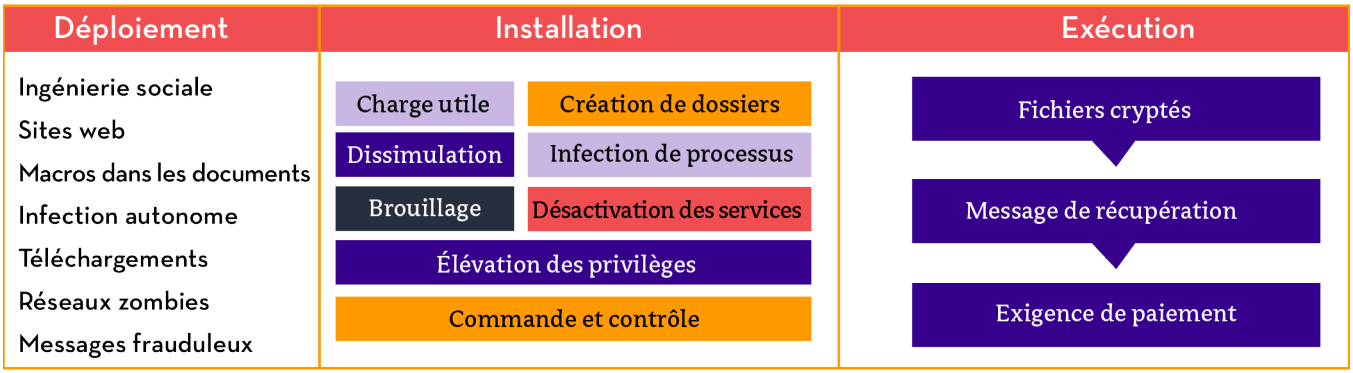


Figure 1 : Anatomie d'un logiciel rançonneur (élaboration personnelle à partir d'idées d'Osorio et al., 2020).

Le premier stade est le *déploiement*. Ce processus a lieu grâce à l'effort planifié de l'attaquant, qui commence obtenir des informations sur les individus ou de la communauté cible afin d'identifier les intérêts et sujets pertinents dans la dynamique sociale des victimes potentielles. Vient ensuite la tromperie crédible par laquelle les individus accèdent à un site web, téléchargent des documents et consultent à des messages frauduleux sans se faire remarquer. Enfin arrive la distraction, qui consiste à exploiter la perte d'attention des personnes pour effectuer l'action qui déclenche le téléchargement ou l'accès du code malveillant au mobile, à l'ordinateur portable ou à l'ordinateur de bureau.

Une fois le téléchargement du logiciel malveillant terminé, *l'installation du logiciel rançonneur* commence. La *charge utile* est activée et déclenche une série d'événements cachés sur l'appareil, tels que la création de dossiers, la dissimulation et l'obscurcissement du code malveillant, l'élévation des privilèges sur le système cible, l'injection de processus qui imitent le processus standard du système d'exploitation, la désactivation des services de surveillance et de protection et, enfin, la préparation du système compromis pour une commande et un contrôle complets.

Après cette étape, au cours de laquelle l'appareil a été préparé pour être contrôlé et géré par l'attaquant, deux activités se déroulent généralement en même temps. Tout d'abord, l'exfiltration des données sensibles que l'adversaire a réussi à obtenir et ensuite le cryptage[18] de ces mêmes données dans l'appareil, qui est effectué grâce à des algorithmes exécutés en parallèle pour atteindre une efficacité maximale dans le processus. Une fois ce processus achevé, un message d'alerte est généré concernant le nouvel état de la machine et la demande de paiement pour récupérer les informations qui ont été compromises.

La littérature établit au moins quatre 4 types d'extorsions que les attaquants peuvent développer une fois qu'ils ont compromis des données: (MunichRe, 2022)

- **Extorsion simple:** demande de paiement pour la restitution de données cryptées
- **Double extorsion:** vol et menace de publication de données
- **Triple extorsion:** menace de lancer une attaque par déni de service distribué contre la victime si un paiement n'est pas effectué
- **Quadruple extorsion:** attaque des fournisseurs de la victime, de la chaîne d'approvisionnement et des clients pour élargir le champ et renforcer la pression pour obtenir le paiement

Ce type d'activité illicite étant une activité très rentable qui génère en moyenne mille milliards de dollars par an (Chainalysis, 2022), les gains économiques de cette extorsion reposent sur trois aspects fondamentaux: (Falco & Rosenbach, 2022, p.24)

1. Profiter de la vente de données volées à des tiers intéressés
2. Menacer les organisations de cyber-attaques ou de fuites d'informations sensibles
3. Logiciel rançonneur interdisant à une organisation d'accéder à ses données jusqu'à ce que le paiement soit effectué

Quel que soit le type d'extorsion pratiqué, l'institution sera confrontée à des pressions et à des exigences qui la rendront responsable des conséquences envers ses parties prenantes et, avec, en même temps, la reconnaissance des conditions et des capacités permettant à l'attaquant de concrétiser cette menace et d'atteindre ses objectifs: l'extorsion et/ou l'exfiltration.

Les gains économiques générés par les logiciels rançonneurs reposent sur trois aspects fondamentaux :
- Profiter de la vente de données volées à des tiers intéressés
- Menacer les organisations de cyber-attaques ou de fuites d'informations sensibles
- Logiciel rançonneur qui interdit à une organisation d'accéder à ses données jusqu'à ce que l'extorsion soit payée

18 Chiffrement d'une information par l'adversaire pour empêcher son propriétaire d'y accéder.

Références

Abrams, L. (2022). Conti ransomware finally shuts down data leak, negotiation sites. *Bleepingcomputer*. https://www.bleepingcomputer.com/news/security/conti-ransomware-finally-shuts-down-data-leak-negotiation-sites/

Baykara, M. & Sekin, B. (2018). A novel approach to ransomware: Designing a safe zone system. *2018 6th International Symposium on Digital Forensic and Security* (ISDFS), Antalya. 1-5. Doi: 10.1109/ISDFS.2018.8355317

Burgess, M. (2022). The Workaday Life of the World's Most Dangerous Ransomware Gang. *Wired*. https://www.wired.co.uk/article/conti-leaks-ransomware-work-life

Cano, J. (2020). Modelo SOCIA. Una reflexión conceptual y práctica desde la perspectiva del adversario. *Actas X Congreso Iberoamericano de Seguridad Informática 2020*. Universidad Politécnica de Madrid - Universidad del Rosario. Enero. Doi: 10.12804/si9789587844337.09

Chainalysis (2022). The 2022 crypto crime report. https://go.chainalysis.com/2022-Crypto-Crime-Report.html

Cohn, L. (2022). The Cutting Edge: 2Q22 Cool New Data Points. *Gartner Business Quarterly. Second Quarter*. 5-8. https://www.gartner.com/en/insights/gartner-business-quarterly

Coverware (2022). Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022. https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

El-Kosairy, A. & Azer, M. A. (2018). Intrusion and ransomware detection system. *2018 1st International Conference on Computer Applications & Information Security* (ICCAIS), Riyadh. 1-7, Doi: 10.1109/CAIS.2018.8471688

Falco, G. & Rosenbach, E. (2022). *Confronting cyber risk. An Embedded Endurance Strategy for Cybersecurity*. New York, NY. USA: Oxford University Press.

Herrera Silva, J. A.; Barona López, L. I.; Valdivieso Caraguay, A. L. & Hernández-Álvarez, M. (2019). A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters. *Remote Sens*. 11(10). 1-20. Doi: 10.3390/rs11101168

Interpol (2020). Cybercrimen: Covid-19 Impact. August. De: https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

Kardile, A. (2017). Crypto ransomware analysis and detection using process monitor. *Master Thesis*. University of Texas, Arlington. De: http://hdl.handle.net/10106/27184

MunichRe (2022). Global Cyber Risk and Insurance Survey 2022. *Global Report*. https://www.munichre.com/landingpage/en/global-cyber-risk-and-insurance-survey-2022.html

Osorio, A., Mateus, M. & Vargas, H. (2020). Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware. *Revista UIS Ingenierías*. 13(3). 131-142. doi: 10.18273/revuin.v19n3-2020013

Richard, L. (2022). "LA LUCHA POR UN TERRITORIO ES LA LUCHA DE TODAS". Forbidden Stories. https://forbiddenstories.org/es/la-lucha-por-un-territorio-es-la-lucha-de-todas/

Saydjari, O. (2018). *Engineering trustworthy systems: get cybersecurity design right the first time*. New York, USA.: McGraw Hill

Sittig, D. F., & Singh, H. (2016). A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. *Applied clinical informatics*, 7(2), 624–632. Doi: 10.4338/ACI-2016-04-SOA-0064

SpyCloud (2022). Ransomware defense report. https://spycloud.com/resource/ransomware-defense-report-2022

Stallings, W. (2019). *Effective cybersecurity. A guide to using best practices and standards*. USA: Addisson Wesley.

Tavella, F. (2021). Ransomware Conti: principales características y cómo operan sus afiliados. *ESET*. https://www.welivesecurity.com/la-es/2021/11/29/ransomware-conti-principales-caracteristicas/

Vicens, A. (2022). Hacking group focused on Central America dumps 10 terabytes of military emails, files. *CyberScoop*. https://www.cyberscoop.com/central-american-hacking-group-releases-emails/

Grimes, R. (2022). *Ransomware Protection Playbook*. Hoboken, NJ. USA: John Wiley & Sons.

Leo, P., Isik, O. & Muhly, F. (2022). The Ransomware Dilemma. *Sloan Management Review*. https://sloanreview.mit.edu/article/the-ransomware-dilemma/

2023

White paper series
Édition 10

Défis et stratégies:

Considérations sur les attaques de logiciels rançonneurs dans les Amériques

OEA | Plus de droits pour plus de personnes

aws