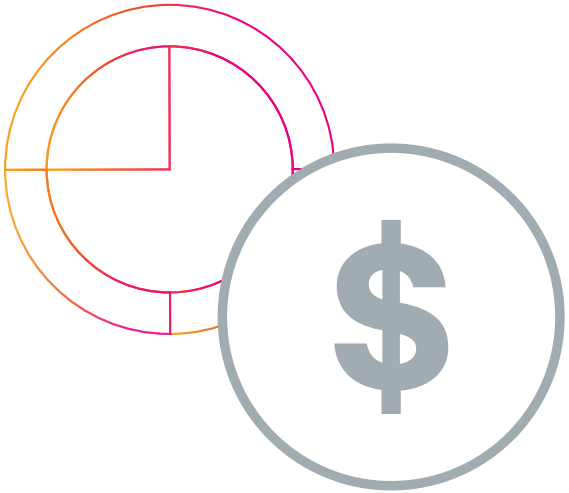
# Le guide essentiel des **ransomwares**

**Un bref historique des attaques par ransomware, des failles majeures et de l'évolution des malwares**

splunk>

## Sommaire





Les ransomwares représentent un problème de plus en plus conséquent pour les organisations, peu importe leur taille et leur type : les attaques se multiplient et les sommes dépensées pour s'en remettre augmentent sans cesse. Ces ransomwares sont devenus tellement problématiques qu'ils font régulièrement la une des journaux. En effet, parmi 1 200 leaders de la sécurité interrogés pour le rapport État de la cybersécurité en 2022 de Splunk, 79 % déclarent avoir été confrontés à des attaques par ransomware et 35 % admettent qu'une ou plusieurs de ces attaques leur ont fait perdre l'accès à leurs données et leurs systèmes.

## La plupart des organisations ont été les cibles de ransomwares

79 % ont repoussé une attaque… ou en ont été victimes.


Source : L'État de la sécurité 2022 | Splunk

Cependant, mieux vaut commencer par expliquer ce qu'est un ransomware pour mieux comprendre l'ampleur du problème. Il s'agit d'un type de malware qui chiffre les données réseau pour les prendre en otage tant qu'un certain montant n'a pas été versé.

D'après le rapport État de la cybersécurité, la somme dépensée par les organisations est élevée : le prix moyen tourne autour de 347 000 dollars. Environ 66 % des organisations ont déclaré avoir payé les criminels, soit par elles-mêmes (dans 39 % des cas), soit par le biais de leur compagnie d'assurance (27 %). La plupart des leaders de la sécurité rapportent que les victimes de ransomware ont avoué avoir payé. Seulement 33 % d'entre elles ont contourné la rançon en restaurant leurs sauvegardes. Les organisations qui ne sont pas totalement à jour en termes d'hygiène de sécurité sont les proies des attaques par ransomware qui ciblent généralement les vulnérabilités des points de terminaison. L'hygiène de sécurité est une barrière que les organisations mettent en place pour préserver, organiser et sécuriser leurs données sensibles.

Pour prendre un exemple simple, cela consiste notamment à s'assurer que les correctifs et les logiciels antivirus sont à jour. Quand bien même il peut être difficile et laborieux de maintenir une bonne hygiène de sécurité, elle réunit les fondamentaux les plus importants pour les organisations.

Dans cet article, nous allons découvrir l'histoire et l'expansion des ransomwares, les acteurs des menaces derrières ces attaques, les tactiques couramment utilisées pour infiltrer une organisation, les bonnes pratiques pour se protéger contre les attaques, et bien plus encore.

## L'évolution des ransomwares

Avec les progrès des capacités de chiffrement et l'adoption grandissante des cryptomonnaies qui motivent les hackers, les différents types d'attaques par ransomware ont augmenté depuis 2014. Cependant, les origines des attaques par ransomware remontent avant les années 1980 : les malfaiteurs de l'époque utilisaient des disquettes pour installer un malware à l'insu de leurs victimes.

Depuis, les attaques par ransomware sont devenues plus sophistiquées et faciles à déployer, en partie à cause d'Internet. D'après le Rapport d'investigation sur les failles de données de Verizon, les attaques par ransomware ont augmenté de 13 % entre 2020 et 2021. Elles ont causé des dégâts équivalents à 20 millions de dollars sur l'année 2021 seule. Et les chiffres ne font qu'augmenter. Selon un autre rapport, les ransomwares devraient coûter, par an et d'ici 2031, environ 265 millions de dollars aux victimes.

# Les ransomwares, un secteur florissant

L'étendue des informations rassemblées depuis divers domaines (identité, e-mail, données et cloud) offre un aperçu de l'économie mercenaire mise sur pied par les malfaiteurs, dont les outils facilitent l'entrée sur le marché de nouveaux pirates. En retour, ceux-ci continuent à verser des dividendes et à financer des opérations au travers de la vente des outils et le versement de commissions.

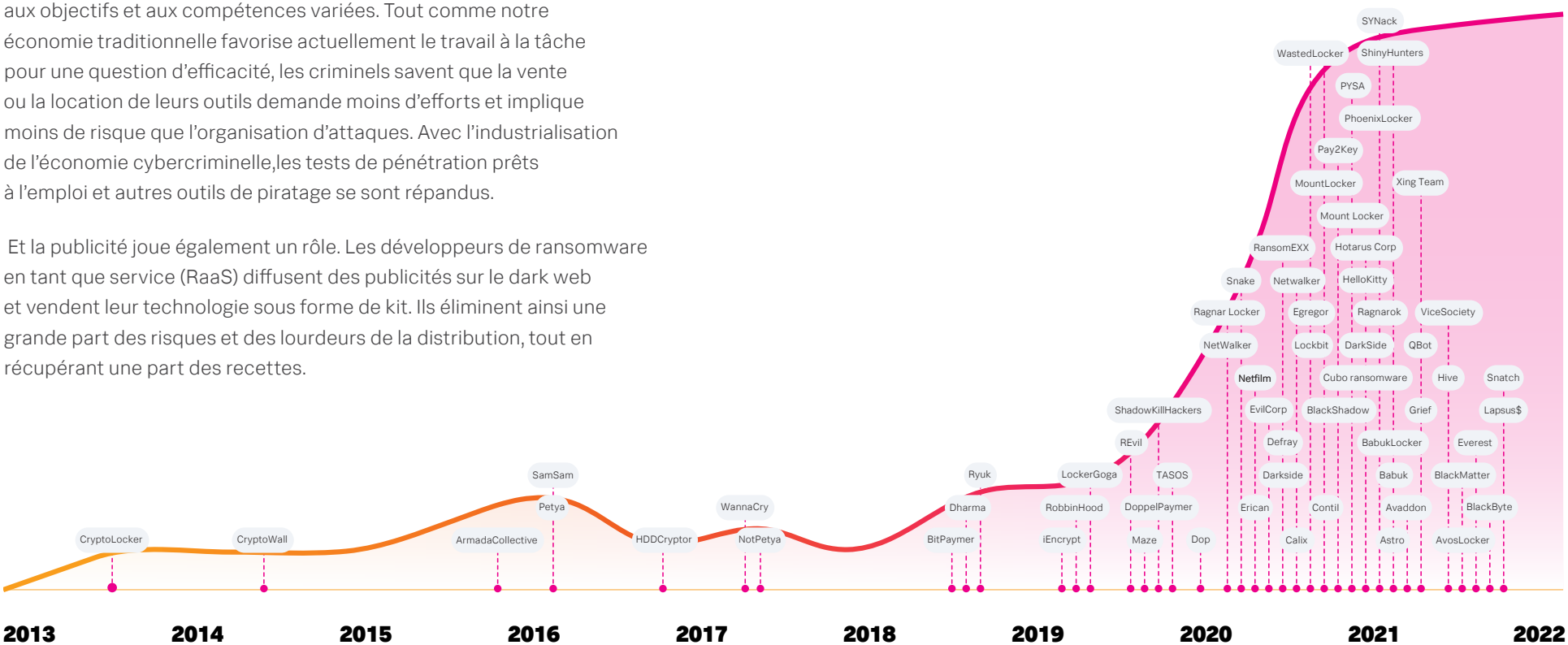
L'économie cybercriminelle est un écosystème connecté en constante évolution qui comprend de nombreux acteurs aux techniques, aux objectifs et aux compétences variées. Tout comme notre économie traditionnelle favorise actuellement le travail à la tâche pour une question d'efficacité, les criminels savent que la vente ou la location de leurs outils demande moins d'efforts et implique moins de risque que l'organisation d'attaques. Avec l'industrialisation de l'économie cybercriminelle,les tests de pénétration prêts à l'emploi et autres outils de piratage se sont répandus.

Et la publicité joue également un rôle. Les développeurs de ransomware en tant que service (RaaS) diffusent des publicités sur le dark web et vendent leur technologie sous forme de kit. Ils éliminent ainsi une grande part des risques et des lourdeurs de la distribution, tout en récupérant une part des recettes.

# Le paysage : qui sont les acteurs ?

Pour éviter les attaques, il faut avant tout comprendre qui prend les risques en matière de ransomware et comment ces acteurs opèrent. Il existe de nombreux groupes de ransomware, mais un petit nombre de groupes de malfaiteurs dirige la majeure partie de l'activité malveillante, dessinant un paysage de ransomwares plutôt centralisé.

De nouvelles vagues de ransomwares affluent régulièrement dans le paysage des menaces. Cette image offre un aperçu de l'essor des attaques par ransomware depuis 2013.




**Le total des coûts liés à ces attaques est toujours inconnu.**

## Groupes de ransomware notables

Les trois groupes de ransomware qui ont revendiqué le plus grand nombre d'attaques réussies pendant le premier trimestre de 2022 utilisaient le modèle RaaS. Sur la base des données provenant des sites où les opérateurs font fuiter les informations, 35,8 % de ces attaques étaient attribuées au collectif de hackers connu sous le nom de LockBit, 19 % à Conti et 9,6 % à BlackCat.

1. **LockBit**

   LockBit est un modèle RaaS qui chiffre les fichiers stockés localement ou dans des dossiers partagés sur le réseau. Il peut également identifier les systèmes supplémentaires dans un réseau et se propager via le protocole SMB (server message block). Avant de chiffrer les fichiers, LockBit efface les logs d'événements, supprime les sauvegardes shadow copy et met fin aux processus et services qui pourraient entraver le chiffrement des fichiers. Les fichiers chiffrés par LockBit présentent l'extension « .lockbit ». Les chercheurs de Mandiant ont observé l'utilisation de LockBit chez plus de dix groupes de menaces non catégorisés dont les objectifs étaient les gains financiers et l'espionnage.

2. **Conti**

   Si Conti est considéré comme un variant de ransomware basé sur le modèle RaaS, sa structure comporte des spécificités qui le différencient d'un modèle affilié typique. Les développeurs de Conti versent généralement un salaire à ceux qui déploient le ransomware plutôt qu'un pourcentage des recettes réalisées par les hackers affiliés, et reçoivent une part des recettes liées aux attaques réussies.

   Les acteurs de Conti obtiennent l'accès initial aux réseaux de plusieurs manières : hameçonnage, vol ou faiblesse des identifiants Remote desktop protocol (RDP), appels téléphoniques, promotion de faux logiciels par SEO, autres réseaux de distribution de malwares et vulnérabilités courantes dans les actifs externes.

3. **BlackCat/ALPHV**

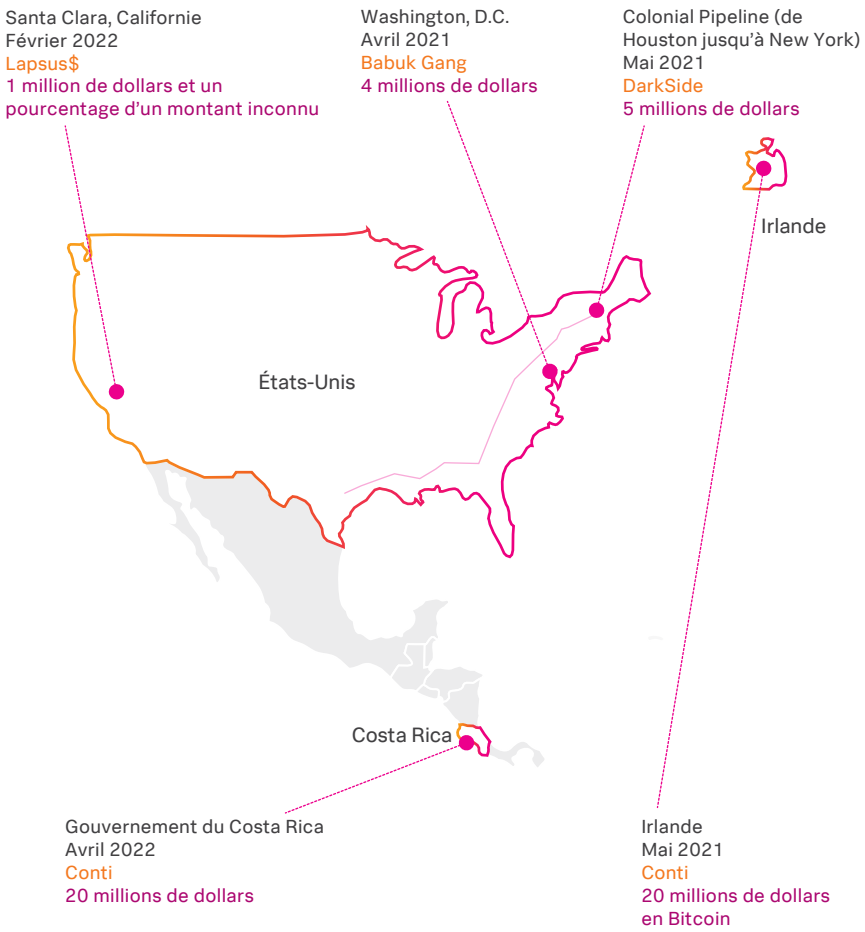
   Le ransomware BlackCat/ALPHV s'appuie sur les identifiants d'utilisateurs préalablement compromis pour obtenir l'accès initial au système de la victime. Après avoir obtenu l'accès, le malware compromet les comptes utilisateur et administrateur d'Active Directory Il se sert ensuite du planificateur de tâches de Windows pour configurer des stratégies de groupe (GPO) qui déploient le ransomware. Le déploiement initial du malware s'appuie sur des scripts PowerShell ainsi que le logiciel Cobalt Strike, et désactive les fonctionnalités de sécurité au sein du réseau de la victime. BlackCat/ALPHV opère également au travers des outils administratifs de Windows et des outils Sysinternals de Microsoft pendant la compromission.

## Nous avons cité les plus grands acteurs des ransomwares, mais d'autres groupes entrent tout de même en jeu :

- **REvil**
  REvil est une entreprise criminelle RaaS. On pense qu'elle pourrait être liée au groupe criminel connu sous le nom de GrandCrab. Dans un schéma RaaS, les acteurs malveillants s'associent à des affiliés pour étendre leurs botnets et récolter les bénéfices des extensions et des attaques que les affiliés ont effectuées pour eux. Les bénéfices sont partagés avec les affiliés, ce qui les motive à infecter davantage de victimes.
- **Hive**
  Le ransomware Hive opère généralement sur la base de l'affiliation et emploie une large variété de tactiques, techniques et procédures, ce qui crée des défis significatifs en termes de défense et de résolution des problèmes. Il utilise divers mécanismes, comme les e-mails d'hameçonnage avec pièce jointe malveillante, pour compromettre les réseaux des entreprises, puis obtenir l'accès au Remote desktop protocol (RPD) pour se déplacer latéralement au sein du réseau. Les pirates du ransomware Hive exfiltrent ensuite les données et chiffrent les fichiers du réseau. Les acteurs malveillants laissent une note qui fournit les instructions pour acheter le logiciel de déchiffrement dans chaque répertoire du système de la victime. Cette dernière menace également de faire fuiter les données exfiltrées sur le site Tor « HiveLeaks ».
- **Vice Society**
  Vice Society est un groupe de double extorsion peu connu avec une activité régulière. Il chiffre et exfiltre les données de ses victimes et les menace de faire fuiter leurs informations pour les pousser à payer une rançon. Contrairement aux autres groupes RaaS, Vice Society cherche avant tout à entrer dans le système de la victime pour déployer les binaires des ransomwares achetés sur les forums du dark web.
- **Black Basta**
  Black Basta vole les données et les documents des entreprises avant de chiffrer leurs appareils. Les données volées sont ensuite utilisées à des fins de double extorsion : les acteurs réclament une rançon en échange d'un outil de déchiffrement et de la non-publication des données de la victime. La partie « extorsion » des attaques est menée sur les sites Tor « Black Basta Blog » ou « Basta News», où se trouve une liste de toutes les victimes qui n'ont pas payé la rançon. Black Basta publie peu à peu les données de chaque victime pour les pousser à payer.
- **Ryuk**
  Ryuk chiffre les fichiers stockés sur les lecteurs locaux et dans les dossiers partagés. Il supprime également les fichiers de sauvegardes et les sauvegardes shadow copy. Certains variants de Ryuk peuvent se propager aux autres systèmes d'un même réseau. Mandiant a relevé l'utilisation de Ryuk chez FIN6, FIN12 et dix groupes de menaces aux motivations financières.
- **Lapsus$**
  Lapsus$ est connu pour utiliser un modèle reposant purement sur l'extorsion et la destruction sans déployer les charges utiles de ransomware. Au début, Lapsus$ visait les organisations du Royaume-Uni et d'Amérique du Sud, mais le groupe a fini par s'étendre mondialement et cibler les gouvernements et les secteurs de la technologie, des télécommunications, des médias, du détail et de la santé. Il est aussi connu pour prendre le contrôle des comptes individuels des utilisateurs lors des échanges de cryptomonnaie pour vider les portefeuilles.

## Attaques par ransomware notables

Les exemples suivants de ransomwares offrent un aperçu de la portée mondiale et des coûts liés à ces attaques, et donnent une idée des dégâts qu'elles peuvent causer aux entreprises et aux personnes.




# Les cibles courantes

En 2021, 79 % des organisations interrogées pour le rapport État de la cybersécurité de Splunk ayant elles-mêmes été victimes de ransomware, disent le plus souvent avoir été piégées par des campagnes d'e-mails malveillants. Cela coïncide avec le passage à des attaques ciblées axées sur des proies de grande valeur : les malfaiteurs entrent de force, analysent le réseau, se déplacent latéralement et suppriment les sauvegardes avant chiffrement.

En 2021, les attaques de cybercriminels ont augmenté, prenant pour cible les agences du gouvernement, les municipalités, les écoles, les infrastructures critiques, les hôpitaux et les établissements de santé, soit directement, soit au travers des prestataires de services gérés (MSP). Les opérateurs de ransomware ont poursuivi leurs projets d'intimidation en compromettant les systèmes stratégiques, en terrorisant les organisations et en demandant des rançons importantes.

Refuser de payer la rançon impose souvent de remplacer les équipements et recommencer à zéro, confrontant la direction des organisations touchées à des difficultés financières, à des décisions stratégiques et à la colère des actionnaires ou des usagers. Les organisations ciblées pensent souvent que payer la rançon est le moyen le plus rentable de récupérer leurs donnés. C'est peut-être vrai, mais ce faisant, elles financent directement le développement de la prochaine génération de ransomwares.

# Les vecteurs d'infection

Bien que les ransomwares existent depuis des dizaines d'années, les créateurs sont de plus en plus sophistiqués dans leurs façons d'infecter les systèmes, d'éviter la détection et de déjouer les efforts de déchiffrement. Il est nécessaire de comprendre la manière dont les ransomwares entrent dans un système pour mieux s'en protéger.

1. **E-mail**

   L'e-mail est une cyberarme répandue : il peut exploiter les utilisateurs en créant un sentiment d'urgence et en donnant une apparence de légitimité à certaines actions. Avec ses pièces jointes camouflées en fichiers innocents ou avec ses liens qui mènent au téléchargement d'un logiciel, il n'est pas surprenant qu'il reste le vecteur d'attaque le plus commun. Un clic suffit à ouvrir la voie à l'infection.

2. **Téléchargement parallèle**

   L'infection par ransomware survient au cours de la visite d'un site web compromis, généralement à cause d'un navigateur obsolète, d'un plug-in ou d'une application tierce non à jour. Le site web infecté exécute un kit d'exploitation qui recherche les vulnérabilités non corrigées.

3. **Protocole Remote Desktop (RDP)**

   Les sessions RDP exposées sur Internet sont des moyens d'infection courants. Idéalement, ces sessions sont utilisées pour se connecter à des ordinateurs Windows à distance et permettre à un utilisateur de contrôler l'ordinateur en toute sécurité. Malheureusement, les hackers sont maintenant capables d'attaquer ces ordinateurs exposés par force brute. Ils utilisent à la fois des méthodes de force brute et l'achat d'identifiants sur les marchés du dark web pour exploiter les vulnérabilités RDP.

4. **Serveurs et services vulnérables tournés vers le public**

   Les malfaiteurs peuvent tenter de tirer avantage d'une faiblesse d'une machine ou d'un programme exposé à Internet en utilisant un logiciel, des données ou des commandes afin de provoquer des comportements inattendus. La faiblesse peut être un bug, un problème ou une vulnérabilité de conception. Il peut s'agir de sites web mais aussi de bases de données (par exemple SQL), de services standards (comme SMB ou SSH), de protocoles de gestion et d'administration des périphériques réseau (SNMP, Smart Install), et de toute autre application qui possède des sockets ouverts accessibles par Internet, comme les serveurs web et les services liés.

# Cyber-assurance, cryptomonnaie et augmentation des ransomwares

Ces dernières années, les cibles des ransomwares se sont notamment étendues à ceux qui possèdent une cyber-assurance et à ceux qui utilisent la cryptomonnaie. Posséder une cyber-assurance semble une bonne idée, mais vous devez comprendre votre police et la manière dont votre assureur compte réagir à une attaque pour sécuriser le réseau d'une organisation sans verser le moindre centime à un groupe de ransomware. N'oublions pas non plus que la prévalence accrue de la cryptomonnaie a entraîné une forte augmentation de la fréquence, de la sophistication et de l'effet destructeur des attaques par ransomware.

## Cyber-assurance

Les spécialistes de la gestion des risques accusent les compagnies d'assurance d'être responsables de la forte augmentation des attaques par ransomware dans les secteurs privé et public. Les forces de l'ordre exhortent les organisations à refuser de payer toute rançon, mais les preuves que le système de cyber-assurances aggrave le problème sont de plus en plus nombreuses. Indirectement, elles encouragent l'activité criminelle des groupes de ransomware.

Les compagnies d'assurance sont incitées à payer les rançons, et poussent les organisations à répondre aux demandes des malfaiteurs car c'est moins coûteux, plus rapide et plus facile que de tout redémarrer à zéro. Les pirates le savent, et ils ciblent les institutions sous cyber-assurance. Ils mènent des missions de reconnaissance pour déterminer le montant de la police et la probabilité que l'organisation paie. Ils placent ensuite la barre de la rançon juste en dessous de ce prix. Si les compagnies d'assurance offrent des services de négociation et apportent leur soutien au rétablissement après une attaque par ransomware, il n'en reste pas moins que les organisations sous cyber-assurance sont plus enclines à payer la rançon que les autres.

Nous pourrions toutefois assister à un retournement de situation du côté des assureurs. Certes, ils étaient prêts à payer les rançons il y a quelques années, quand il s'agissait de sommes à trois ou quatre chiffres, mais la prévalence des rançons d'un montant de plusieurs millions de dollars a complètement changé la donne. Le secteur des assurances a récemment abattu ses cartes.

D'après des rapports récents, la hausse des pertes liées aux ransomwares a fait décoller les primes des cyber-assurances de 92 % en 2021, tandis qu'un audit industriel récent effectué par le Council of Insurance Agents & Brokers (CIAB) nous informe que les cyber-primes ont décollé de 34,3 % au cours du dernier trimestre 2021, ce qui représente la plus forte augmentation des primes sur un trimestre depuis le 11 septembre 2001.

Les assureurs refusent de plus en plus de couvrir les dégâts, à moins que l'entreprise ne prouve qu'elle dispense des formations de sécurité efficaces et qu'elle a implémenté des protections clés, comme l'authentification multifacteurs (MFA), qui ne peut être compromise que dans des circonstances extrêmes et offre une meilleure protection qu'un simple mot de passe.

## Cryptomonnaies

À la naissance des ransomwares, les méthodes de paiement étaient encore limitées. Quelques pirates pouvaient demander à ce qu'on leur envoie de l'argent via Western Union ou sur un compte bancaire, mais les autorités pouvaient tracer ces virements. Puis vint le Bitcoin.

Le Bitcoin est une méthode de paiement sécurisée et intraçable, que ce soit pour envoyer ou recevoir de l'argent. Il est plus flexible que les méthodes de paiement traditionnelles dont l'utilisation nécessite des informations financières ou des identifiants de connexion. Il fonctionne comme une monnaie décentralisée grâce à laquelle les personnes peuvent payer dans le monde entier sans intermédiaire, sans supervision et sans règles. Il offre ainsi un niveau d'anonymat acceptable pour les malfaiteurs.

Si le Bitcoin est la cryptomonnaie la plus connue, les analystes industriels suivent le Monero, qui est fortement utilisé sur les marchés du dark web et devient une méthode de paiement de choix pour les ransomwares grâce à son côté confidentiel. Les chances que la cryptomonnaie facilite l'augmentation de la cybercriminalité sont difficiles à évaluer mais les tentatives d'extorsion sont en train de monter en flèche.

# Tendances des ransomwares

Les créateurs de ransomwares sont de plus en plus sophistiqués dans leurs approches pour infecter les systèmes, éviter la détection et déjouer les efforts de déchiffrement. On observe plusieurs tendances dans le domaine des ransomwares :

- **Campagnes mixtes**
  Les groupes malveillants qui agissent pour le compte d'États-nations associent le minage de cryptomonnaie et les campagnes de ransomwares pour générer des revenus ou détourner l'attention d'autres attaques.
- **Chasse au gros gibier**
  Les méthodes Spray and pray sont abandonnées au profit d'attaques ciblées qui visent une proie d'importance, comme un hôpital ou une grande société, pour une somme exorbitante. Les ransomwares sont personnalisés en fonction de la cible afin de causer le maximum de dégâts et demander des rançons plus élevées.
- **Collecte d'informations**
  Les groupes criminels de ransomware rassemblent des informations sur les victimes ciblées. En plus de s'introduire dans le réseau et de mener des opérations de reconnaissance, les malfaiteurs étudient les déclarations financières déposées à la SEC par les entreprises et utilisent ces informations pour adapter les demandes de rançon.
- **Furtivité et discrétion**
  Plusieurs stratégies permettent de passer sous le seuil de détection :
  - randomisation du processus plutôt qu'un chiffrement linéaire ;
  - exécution retardée des attaques pour contourner les défenses traditionnelles ;
  - code polymorphe qui évolue dans le temps ;
  - attaques multi-threadées qui lancent des processus enfants.
- **Augmentation de l'impact**
  Les acteurs malveillants peuvent augmenter l'impact de leur attaque et contrecarrer la récupération de plusieurs manières :
  - en chiffrant le disque dur et le master boot record ;
  - en attaquant les lecteurs réseau partagés ;
  - en attaquant les fichiers stockés dans une infrastructure en tant que service ;
  - en supprimant les sauvegardes shadow copy Windows et tous les fichiers avec des extensions de sauvegarde ;
  - en ciblant les actifs de grande valeur comme les serveurs web, les serveurs d'applications et les outils de collaboration.
- **Attaques dirigées contre les prestataires de services gérés (MSP)**
  Les prestataires de services gérés représentent une cible de plus en plus importante pour les auteurs d'attaques par ransomware. Les attaques ciblant les MSP peuvent potentiellement détruire toute organisation ou presque. Les malfaiteurs exploitent les systèmes de sécurité vulnérables que l'on trouve généralement chez les fournisseurs de services qui gèrent de nombreuses entreprises et municipalités avec des ressources limitées. Ils réalisent ainsi des économies d'échelle et peuvent faire pression pour percevoir leur rançon.
- **Les attaques dirigées contre les fournisseurs de services cloud**
  Les auteurs des ransomwares ont commencé à cibler les fournisseurs de services cloud à l'aide d'attaques par chiffrement de fichiers réseau pour prendre en otage le maximum de clients. Les répercussions des attaques de ransomwares ciblant les fournisseurs de services cloud sont terribles car elles chiffrent les systèmes d'entreprise de tous les clients hébergés dans le cloud.
- **Wiperwares**
  Le ransomware est utilisé comme une couverture pour dissimuler des incidents plus graves, comme une faille de données. Bien que l'attaque ressemble à un ransomware habituel distribué par e-mail d'hameçonnage, l'objectif est de distraire l'organisation pendant que d'autres événements de sécurité ont lieu sur le serveur, puis de supprimer les traces des attaques auxiliaires. L'auteur espère que l'organisation, soulagée de s'être rétablie d'une attaque par ransomware, ne réalisera pas d'investigation plus poussée.
- **Les bonnes vieilles méthodes**
  Les ransomwares exploitent encore les anciennes vulnérabilités et celles qui affichent de plus petits scores de sécurité. Des recherches indiquent que des vulnérabilités qui remontent à 2010 sont toujours exploitées. Prenons l'exemple de Log4j, développé il y a 20 ans. Ce framework de journalisation est déployé sur des centaines de millions de systèmes dans le monde. Sa vulnérabilité zero-day était l'une des plus critiques de la dernière décennie. Malheureusement, ce ne sera pas la dernière. Il est temps de faire le point sur les implications à long terme de cette vulnérabilité et sur celles à venir pour les responsables de la sécurité. Les organisations qui se réfèrent uniquement au score CVSS pour classer les vulnérabilités à corriger vont passer à côté des vulnérabilités utilisées par les ransomwares.
- **Double extorsion**
  Comme souligné plus tôt, les attaques par ransomware ont pris une mauvaise tournure quand leurs auteurs ont entrepris de faire fuiter les fichiers des victimes pour exercer davantage de pression et les pousser à payer la rançon. Désormais, avec des attaques d'une telle envergure, les victimes doivent non seulement s'inquiéter de la récupération de leurs fichiers chiffrés mais aussi des conséquences d'une possible divulgation des fichiers non chiffrés.

# L'impact des ransomwares sur les entreprises

Les ransomwares drainent des milliards à l'économie mondiale et ne montrent aucun signe de ralentissement. Au-delà des rançons, les coûts les plus importants sont liés aux interruptions, aux pertes de données, aux dommages à la réputation, à la récupération et la reconstruction des systèmes, ainsi qu'aux amendes imposées par les organismes de régulation. Malheureusement, l'impact sur les entreprises continue à prendre de l'ampleur :

- les rançons allant de 50 000 à 400 000 dollars sont devenues habituelles. Selon la cible, certaines demandes de rançons atteignent les millions. Cybersecurity Ventures prévoit que le coût des ransomwares atteindra environ 265 milliards de dollars américains par an pour les victimes en 2031.

# L'impact des ransomwares sur le secteur public

La hausse de ransomwares a eu des conséquences particulièrement lourdes sur le secteur public dans le monde entier, avec l'augmentation des attaques contre les agences de gouvernement, les municipalités et les établissements scolaires. Cela n'a fait qu'empirer pendant la pandémie : le gouvernement américain s'est vu dans l'obligation de communiquer un mémo au sujet des bonnes pratiques à adopter contre les attaques par ransomware. Le président Joe Biden est allé encore plus loin en émettant un ordre exécutif au sujet du renforcement de la cybersécurité de la nation. Ce dernier détaille cinq pratiques pour se protéger des ransomwares :

- implémenter l'authentification multifacteurs (MFA) ;
- implémenter un système de détection et de réponse au niveau des terminaux pour appuyer des activités de détection proactive, de chasse aux menaces, de confinement, de correction et de réponse aux incidents ;
- chiffrer les données ;
- employer une équipe de sécurité compétente et autonome ;
- partager et intégrer la threat intelligence.

Les États-Unis ne sont qu'un exemple des nombreux gouvernements qui s'inquiètent de la propagation des ransomwares. En effet, selon le Rapport sur les cybermenaces 2022, les gouvernements du monde entier ont vu les attaques par ransomware augmenter de 1 885 %, tandis que l'augmentation s'élève à 755 % dans le secteur de la santé en 2021.

## La sécurité orientée données face aux ransomwares

Heureusement, même si les organisations devraient faire preuve de vigilance face aux menaces des ransomwares, elles ne doivent pas nécessairement en avoir peur. Il est possible d'éviter ce type de malware. Pour le moment, deux options se présentent : suivre le trafic du réseau suspect avec un système de détection et réponse sur les terminaux, capable de bloquer un hash et d'empêcher la création de nouveaux processus par des exécutables néfastes, ou bien détecter tout domaine associé à des ransomwares connus. Il est aussi possible d'automatiser la réponse de sécurité en fonction des variants des ransomwares connus et de leurs comportements.

Mais que se passe-t-il si vous détectez l'attaque trop tard ?

La direction de l'entreprise doit réfléchir aux circonstances dans lesquelles elle déciderait ou non de verser une rançon, puis mettre en place des processus de prise de décision et d'investigation. Établir au préalable une politique et une stratégie de communication orientées par des facteurs juridiques, commerciaux et métier réduira le stress et permettra d'apporter une réponse informée.

Voici quelques conseils d'experts supplémentaires pour bien se préparer et se défendre face aux attaques par ransomware :

- créez une politique sur la gestion des incidents liés aux ransomwares ;
- développez votre écosystème d'informations en collaboration avec les communautés de partage ;
- étoffez vos fondamentaux en vous dotant d'une équipe, de processus et d'une technologie efficaces en matière de détection et de réponse ;
- étant donné que les acteurs des menaces attaquent le cloud, assurez-vous d'avoir une visibilité complète sur les services cloud.
- maintenez tous les logiciels à jour, systèmes d'exploitation inclus, et tenez un inventaire clair de tous les actifs numériques et de leur emplacement ;
- identifiez les données importantes et segmentez le réseau. Évitez de placer toutes les données dans un seul système de partage accessible par tout le personnel de l'entreprise ;
- effectuez des sauvegardes quotidiennes, en incluant les données des appareils des employés. Pensez aux emplacements en ligne, locaux et hors site sécurisés ;
- effectuez des tests de pénétration pour trouver et corriger les vulnérabilités, vérifiez que les ports RDP ne sont pas accessibles avec des identifiants par défaut et maintenez une bonne hygiène de sécurité ;
- formez le personnel aux pratiques de sécurité en rappelant qu'il ne faut jamais ouvrir les pièces jointes ou les liens provenant de sources inconnues ;
- les logiciels de sécurité des terminaux bloquent de nombreuses tentatives d'infections par e-mail, mais la protection des terminaux ne suffit plus. Employez une solution multicouche de défense contre les menaces ;
- créez un plan d'isolation pour supprimer les systèmes infectés du réseau ;
- si vous subissez une attaque, effectuez une recherche pour déterminer si des malwares similaires ont été analysés par d'autres équipes IT et s'il est possible de déchiffrer les données par vous-même.

**Prenez de l'avance** sur les attaques en utilisant les contenus de sécurité de l'équipe de recherche sur les menaces de Splunk et Splunk SURGe, source de confiance en matière de recherche et de conseils opportuns sur la sécurité.

Essayez également Splunk Online Demo Experience—Endpoint, où vous pourrez utiliser des échantillons de données pour vous entraîner aux techniques d'investigation en toute sécurité. Essayez également la version de démo en ligne de Splunk Security Essentials pour apprendre à traiter les différents scénarios de malwares et à élaborer un portefeuille solide en matière de sécurité.

splunk>



22-25821-Splunk-Essential Guide to Ransomware_SS-106