proofpoint.

Fiche menace : ransomwares

En bref

Description :

Un ransomware chiffre les données critiques ou empêche les utilisateurs d'accéder à leurs terminaux jusqu'au paiement d'une rançon au cybercriminel, généralement une organisation criminelle.

L'arsenal :

CryptoLocker, WannaCry, Bad Rabbit, Cerber, Crysis, CryptoWall, GoldenEye, Jigsaw, Locky, Petya, Conti, Sodinokibi et Ryuk

Origine :

La première attaque mondiale de ransomware suspectée remonte à 1989, lorsque Joseph Popp a créé le cheval de Troie AIDS et distribué 20 000 disquettes infectées intitulées « AIDS Information — Introductory Diskettes » aux participants à la conférence internationale sur le SIDA de l'Organisation mondiale de la santé.

Types :

- **Ransomware Crypto ou cryptographique**
  Logiciel malveillant utilisé pour chiffrer les fichiers stockés sur un ordinateur afin d'empêcher l'utilisateur d'y accéder.
- **Ransomware Locker ou verrouilleur d'écran**
  Logiciel malveillant utilisé pour bloquer l'accès à l'ordinateur d'un utilisateur jusqu'au paiement d'une rançon.
- **Scareware**
  Logiciel malveillant conçu pour amener l'utilisateur à croire que son ordinateur a été infecté par un ransomware et à transférer des fonds au cybercriminel. Bien qu'il ne s'agisse pas d'un ransomware techniquement parlant, le scareware produit le même effet sur les victimes.

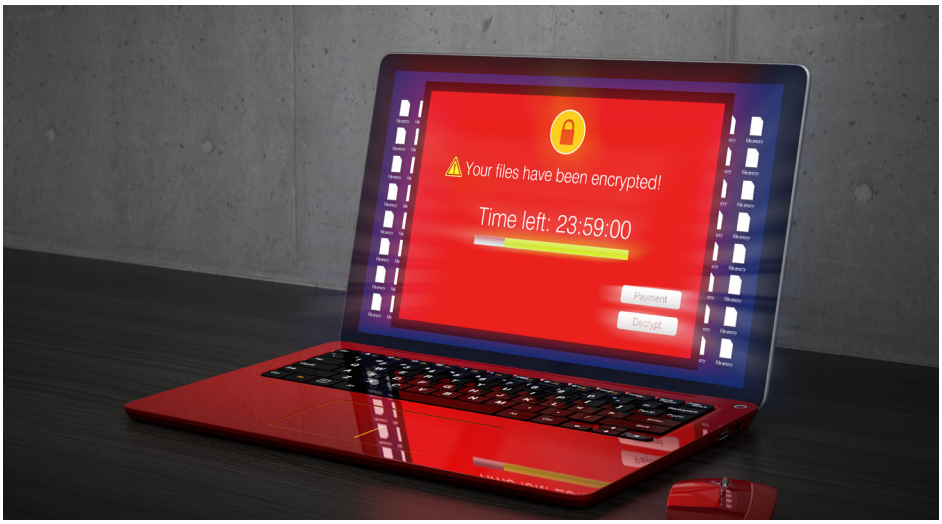
Facteurs de risque :

- Logiciels et systèmes vulnérables
- Sauvegardes difficiles d'accès
- Cybersécurité inefficace ou inexistante
- Utilisateurs insuffisamment formés et vulnérables

Dommages possibles :

- Pertes financières
- Perte de données sensibles ou propriétaires
- Atteinte potentielle à la réputation
- Interruption des activités et perte de productivité

Le ransomware, qui doit son nom aux rançons qu'il exige pour débloquer les fichiers de la victime, est un véritable fléau pour les entreprises modernes. Il est l'une des cyberattaques actuelles les plus déstabilisantes, interrompant les activités de ses victimes, forçant les hôpitaux à renvoyer les patients chez eux et mettant les pouvoirs locaux complètement à l'arrêt. La meilleure protection contre le ransomware consiste à empêcher toute intrusion dans votre environnement. Voici quelques informations générales et conseils sur cette menace en pleine expansion.



Quelques attaques de ransomwares qui ont défrayé la chronique

Victime du ransomware Ryuk, Universal Health Services essuie une perte de 67 millions de dollars

Une attaque de ransomware a touché Universal Health Services (UHS), coûtant à l'entreprise près de 67 millions de dollars en temps d'arrêt et dépenses connexes. Ce groupe d'établissements de santé figurant au classement Fortune 500 occupe des dizaines de milliers de collaborateurs aux États-Unis et en Grande-Bretagne et génère des revenus qui s'élèvent à plus de 10 milliards de dollars[1].

L'UCSF verse une rançon de 1,14 million de dollars pour récupérer l'accès à ses données de recherche

Les cybercriminels s'en sont pris à l'université en bloquant les systèmes informatiques de sa faculté de médecine. Les recteurs ont rapidement tenté de circonscrire l'infection et d'isoler certains systèmes, afin d'empêcher le ransomware d'atteindre le cœur du réseau de l'UCSF et de causer davantage de dommages[2].

Cognizant délestée de 50 à 70 millions de dollars à la suite d'une attaque de ransomware

Le prestataire de services informatiques Cognizant a été la cible d'une attaque de ransomware en avril 2020, qui lui a coûté ses bénéfices du 2e trimestre. L'incident a entraîné des coûts juridiques, de consultation et autres pour enquêter sur l'incident, restaurer les services et réparer les systèmes[3].

1 Phil Muncaster (*Infosecurity*), « Universal Health Services Estimates $67 Million in Ransomware Losses » (Universal Health Services estime les pertes dus à l'attaque de ransomware à 67 millions de dollars), mars 2021.
2 Charlie Osborne (*ZDNet*), « University of California SF pays ransomware hackers $1.14 million to salvage research » (L'Université de Californie SF verse une rançon de 1,14 millions de dollars pour sauver ses recherches), juin 2020.
3 Catalin Cimpanu (*ZDNet*), « Cognizant expects to lose between $50m and $70m following ransomware attack » (Cognizant évalue les pertes à 50 à 70 millions de dollars à la suite d'une attaque de ransomware), mai 2020.

Une attaque de ransomware perturbe l'approvisionnement en carburant des États-Unis

L'un des plus grands pipelines américains a été mis hors service en mai 2021 à la suite d'une attaque de ransomware, causant l'arrêt des opérations du réseau de 8 850 km de pipelines assurant près de la moitié de l'approvisionnement en carburant de la côté est[4]. L'exploitant du pipeline a versé la somme de 4,4 millions de dollars pour débloquer ses données, mais « cela n'a pas suffi pour rétablir immédiatement les systèmes de pipelines »[5].

Le plus grand transformateur de viande interrompt la production de bœuf à la suite d'une attaque de ransomware

L'entreprise brésilienne a fermé ses usines de conditionnement de viande implantées au Colorado, dans l'Iowa, dans le Minnesota, en Pennsylvanie, dans le Nebraska et au Texas à la suite d'une attaque qui, d'après les autorités américaines, trouverait son origine en Russie[6]. Dans un communiqué de presse, l'entreprise a déclaré avoir détecté l'attaque sur ses réseaux informatiques d'Amérique du Nord et d'Australie. Heureusement, ses serveurs de sauvegarde n'ont pas été infectés lors de l'attaque[7].

Anatomie d'une attaque de ransomware

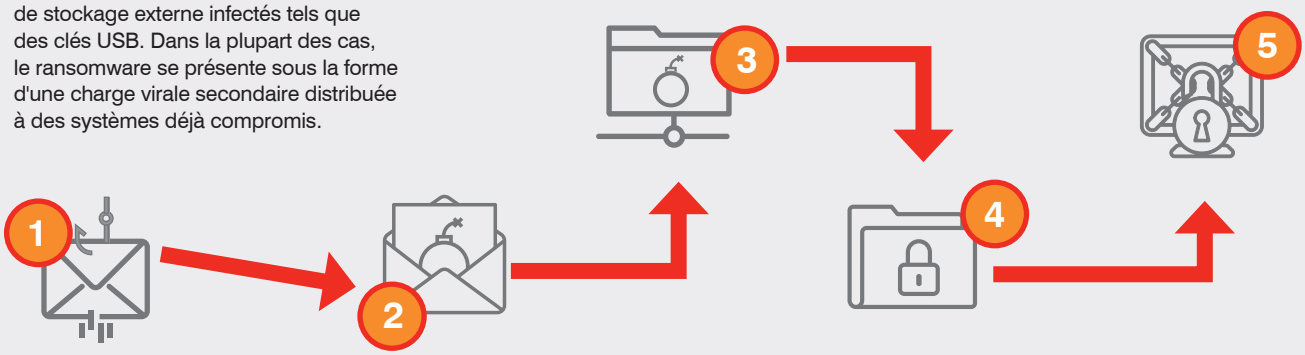
Ces trente dernières années, les ransomwares n'ont cessé d'évoluer pour devenir l'une des cybermenaces les plus redoutables. D'une part, la collecte de rançons par les cybercriminels a été facilitée par l'avènement des monnaies virtuelles telles que le Bitcoin. D'autre part, les cyberpirates se montrent de plus en plus futés et ciblent des systèmes vieillissants et obsolètes.

Déroulement de la plupart des attaques de ransomwares :

1. Distribution | Les cybercriminels poussent les utilisateurs à accéder au logiciel malveillant au moyen d'emails de phishing, de techniques d'ingénierie sociale, de liens malveillants qui mènent à des sites Web factices et de périphériques de stockage externe infectés tels que des clés USB. Dans la plupart des cas, le ransomware se présente sous la forme d'une charge virale secondaire distribuée à des systèmes déjà compromis.

3. Implantation | La charge virale du ransomware injectée par le fichier se dissimule et s'intègre au système.

5. Avis de rançon | Un avis de rançon s'affiche sur l'écran de la victime, l'invitant à payer une certaine somme pour obtenir le déverrouillage de ses fichiers.

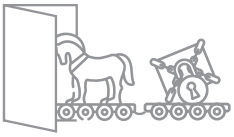


2. Infection | Les utilisateurs téléchargent à leur insu un fichier exécutable appelé « chargeur » (ou « téléchargeur »), qui installe le ransomware.

4. Analyse et chiffrement | Le logiciel malveillant analyse ensuite le système et le réseau et chiffre les fichiers.

Les cybercriminels ont également découvert que la plupart des victimes de ransomware possèdent des sauvegardes de données, de sorte qu'elles refusent de se plier à leur demande de rançon. Les cybercriminels se sont donc adaptés. Ils commencent par voler et chiffrer des fichiers, puis menacent de divulguer les données dérobées. Ces données pouvant être extrêmement sensibles ou personnelles, leur divulgation au grand public pourrait avoir des conséquences désastreuses. Les souches de ransomwares les plus sophistiquées vont jusqu'à rechercher et chiffrer les sauvegardes.

4 David E. Sanger, Clifford Krauss et Nicole Perlroth (*The New York Times*), « Cyberattack Forces a Shutdown of a Top U.S. Pipeline » (Une cyberattaque met à l'arrêt un important pipeline des États-Unis), mai 2021.
5 Collin Eaton et Dustin Volz (*The Wall Street Journal*), « Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom » (Le PDG de Colonial Pipeline explique pourquoi il a versé une rançon de 4,4 millions de dollars aux cybercriminels), mai 2021.
6 Jacob Bunge (*The Wall Street Journal*), « Meat Buyers Scramble After Cyberattack Hobbles JBS » (Les acheteurs de viande se retrouvent chiffrés à la suite d'une cyberattaque ciblant JBS), juin 2021.
7 Hamza Shaban, Ellen Nakashima et Rachel Lerman (*The Washington Post*), « JBS, world's largest meat processor, shut down U.S. beef plants amid cyberattack » (JBS, le plus grand transformateur de viande au monde, met à l'arrêt ses installations américaines à la suite d'une cyberattaque), juin 2021.



L'ÉVOLUTION DES ATTAQUES DE RANSOMWARES

Autrefois charge virale principale des campagnes email malveillantes, le ransomware est aujourd'hui davantage perçu comme une infection secondaire.

Les cybercriminels qui distribuent des chevaux de Troie et d'autres types de malwares autorisent les auteurs d'attaques de ransomwares à utiliser des portes dérobées d'accès aux systèmes infectés en échange d'une part des profits.

Pour la plupart des entreprises, la première ligne de défense contre les ransomwares consiste donc à se protéger contre l'infection initiale. En d'autres termes, il leur faut bloquer le chargeur pour bloquer le ransomware.

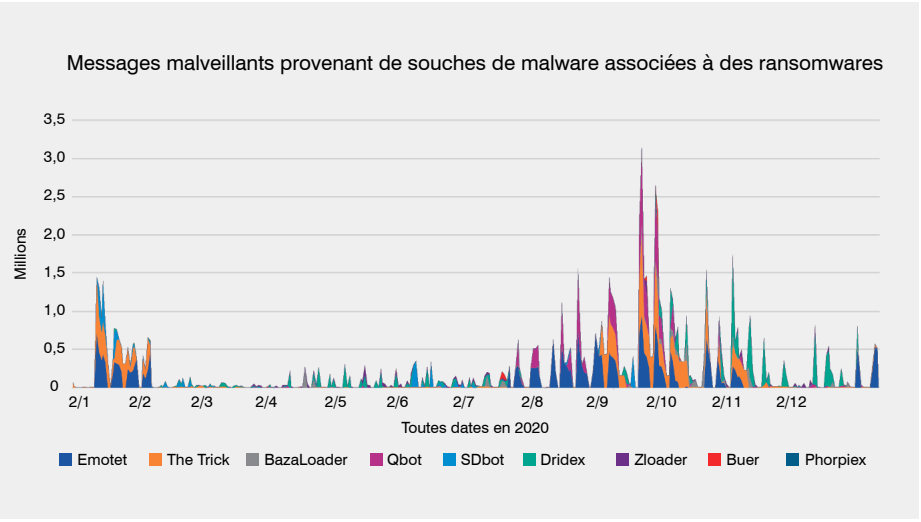
Le point sur la recherche

Un ransomware est généralement distribué dans le cadre d'une infection secondaire, après la compromission initiale d'un système par un email malveillant. Bon nombre des souches de malware les plus prolifiques sont étroitement associées à une infection consécutive par ransomware, d'après nos observations et celles d'autres chercheurs.

Voici la liste des souches de malware les plus courantes et des ransomwares qui leur sont étroitement associés.

MALWARE/TÉLÉCHARGEUR	RANSOMWARE ASSOCIÉ
Emotet	Ryuk
The Trick	Conti
Dridex	BitPaymer/DoppelPaymer
Qbot	Egregor
SDBbot	Clop
ZLoader	Egregor et Ryuk
Buer (Buer Loader)	Ryuk
Phorphiex/Trik	Avaddon

Emotet, The Trick, Dridex et Qbot font partie des malwares les plus prolifiques observés en 2020, caractérisés par des volumes réguliers tout au long de l'année et des pics importants à l'automne.



Davantage d'entreprises paient la rançon, avec des résultats mitigés

D'après le rapport State of Phish 2021 de Proofpoint, 68 % des entreprises américaines sondées ont déclaré avoir payé une rançon en 2020. C'est deux fois plus que la moyenne mondiale. En Espagne, 41 % des entreprises ont refusé de payer la rançon après avoir été infectées. À l'échelle mondiale, elles sont considérées comme les entreprises les moins enclines à négocier avec les cybercriminels.

78 % des entreprises françaises qui ont payé une rançon unique après une attaque ont récupéré l'accès à leurs données. Les entreprises américaines occupent la deuxième place avec un taux de 76 %.

Les professionnels de la sécurité des informations ont révélé qu'en 2020, 34 % des entreprises ont été infectées et ont choisi de payer la rançon, 32 % ont été infectées et ont refusé de payer et 34 % ont déclaré ne pas avoir été victime d'une attaque de ransomware.

Comment protéger votre entreprise

Face aux attaques de ransomwares, la meilleure stratégie consiste naturellement à les éviter.

Avant l'attaque

Partez de l'hypothèse que vous serez tôt ou tard victime d'une attaque de ransomware. Pensez alors prévention, détection et intervention. Par exemple :

- Sauvegardez les données sensibles, testez les procédures de restauration des données et conservez des sauvegardes segmentées de vos systèmes de fichiers principaux.
- Mettez vos systèmes à jour et appliquez les correctifs nécessaires.
- Informez et formez les utilisateurs.
- Investissez dans des solutions de sécurité centrées sur les personnes.
- Appliquez une segmentation du réseau pour limiter la propagation.
- Décidez avant l'attaque si l'entreprise payera la rançon, à quelle hauteur et dans quelles circonstances.

Pendant l'attaque

Une fois l'attaque perpétrée, appliquez toutes les mesures utiles pour prévenir de nouveaux dommages et déclenchez un plan d'intervention. Par exemple :

- Contactez les autorités.
- Déconnectez-vous du réseau.
- Déterminez l'ampleur du problème sur la base de la threat intelligence.
- Orchestrez la réponse.
- Appliquez une segmentation du réseau pour limiter la propagation.
- Analysez les autres points de vulnérabilité, logiciels malveillants et compromissions du système susceptibles d'être associés au ransomware.
- Ne vous fiez pas aux outils gratuits de déchiffrement des ransomwares.
- Restaurez les données sensibles et assurez-vous de l'absence de tout logiciel malveillant qui aurait été sauvegardé avec d'autres données.

Après l'attaque

Lorsque l'attaque est terminée, restaurez les données et résolvez les problèmes causés par l'attaque. Par exemple :

- Nettoyez et réparez le système.
- Procédez à une analyse post-mortem de la sécurité.
- Évaluez la sensibilisation des utilisateurs.
- Appliquez des contrôles basés sur les risques et centrés sur les personnes.
- Réexaminez la sécurité du système et réorientez les investissements en fonction des domaines les plus à risque.

Faut-il payer la rançon ?

Même si les conséquences d'une attaque pour vos activités et vos clients peuvent être graves, sachez qu'en payant la rançon, vous financez la criminalité. La solution idéale n'est pas toujours claire.

Les entreprises doivent prendre en compte différents facteurs avant de décider de la marche à suivre :

- Sécurité des clients et des collaborateurs
- Temps et ressources nécessaires pour remédier à la situation
- Responsabilité à l'égard des actionnaires en termes de maintien des activités
- Type d'activité criminelle que le paiement de la rançon servira potentiellement à financer

Quelle que soit la décision, elle doit être prise avant que ne survienne l'attaque, à un moment où les dirigeants ne sont pas sous pression dans un contexte d'urgence et de perturbations majeures des activités. Outre la décision de payer ou non la rançon, les entreprises doivent également déterminer le montant qu'elles sont prêtes à verser et à quelles conditions. Gardez à l'esprit que certains paiements, tels que ceux effectués en faveur de cybercriminels figurant sur les listes de sanctions américaines, peuvent être illégaux.

EN SAVOIR PLUS

Le moyen le plus efficace d'éviter les ransomwares est de se concentrer sur la prévention. Un plan robuste de prévention des attaques de ransomware doit s'accompagner d'une solution de sécurité centrée sur les personnes. Il doit également prévoir la sensibilisation de vos collaborateurs et leur formation sur la base de techniques d'attaque réelles. Il doit détecter et bloquer les téléchargeurs de ransomwares et de malwares ciblant vos collaborateurs. Enfin, il doit vous aider à intervenir rapidement et à prendre les mesures nécessaires avant que les choses ne tournent mal.

Pour découvrir comment bloquer efficacement un ransomware, téléchargez le rapport Le ransomware — Guide de survie.

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.