MANDIANT

DOUBLE EXTORSION : L'ÉVOLUTION DU RANSOMWARE

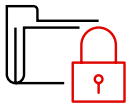
Une menace pour la sécurité des États

Les cybercriminels ont propulsé le ransomware en tête des principaux vecteurs d'attaque contre les structures de tout type et de toute taille. Paralysie d'infrastructures critiques, mise en danger de la santé et de la sécurité publiques, détournement de ressources publiques d'importance vitale, perturbation des établissements d'enseignement, compromission de la confidentialité des données… les auteurs d'attaques par ransomware ne reculent devant rien, au point de représenter dans certains cas un péril majeur pour la sécurité nationale.

Virulence accrue des attaques

Depuis 1989, date de la première attaque par ransomware recensée, les cybermalfaiteurs n'ont cessé de perfectionner leurs méthodes et d'accentuer leur pouvoir de nuisance pour créer un marché de plusieurs milliards de dollars, capable à lui seul de paralyser toute une économie. Pour aiguiser leurs moyens de coercition, ils exploitent désormais le lucratif filon du vol des données, assorti de menaces de publication de ces informations sensibles si les sommes demandées ne sont pas acquittées. Vu l'importance des enjeux, le montant des rançons s'est envolé. Pour preuve, un célèbre opérateur d'importance vitale (OIV) américain a dû verser 4,4 millions de dollars en bitcoins[1] pour relancer l'approvisionnement en carburants de toute la côte est des États-Unis.

C'est en 2020 que ce virage majeur a commencé à faire parler de lui, amenant Mandiant à qualifier ces nouvelles pratiques de « double extorsion », ou « extorsion multifacette ». La menace a d'ailleurs proliféré à une telle vitesse qu'elle figurait dans les gros titres du rapport M-Trends 2021 de Mandiant.



25 %

25 % des incidents dans le monde traités par Mandiant en 2020 relevaient du ransomware[2]

2 400

Aux États-Unis, près de 2 400[3] administrations, établissements de santé et d'enseignement ont subi une attaque par ransomware

JOURS

À l'échelle mondiale, la durée médiane de présence des ransomwares s'élève à 5 jours[2]

1. Forbes (juillet 2021). « The REvil Ransomware Hackers Have Gone Offline ».
2. FireEye (2021). M-Trends 2021.
3. IST (2021). A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force.

Portrait robot de la double extorsion

Si le ransomware et la double extorsion sont étroitement liés, cette dernière présente des risques bien plus sérieux pour les entreprises.

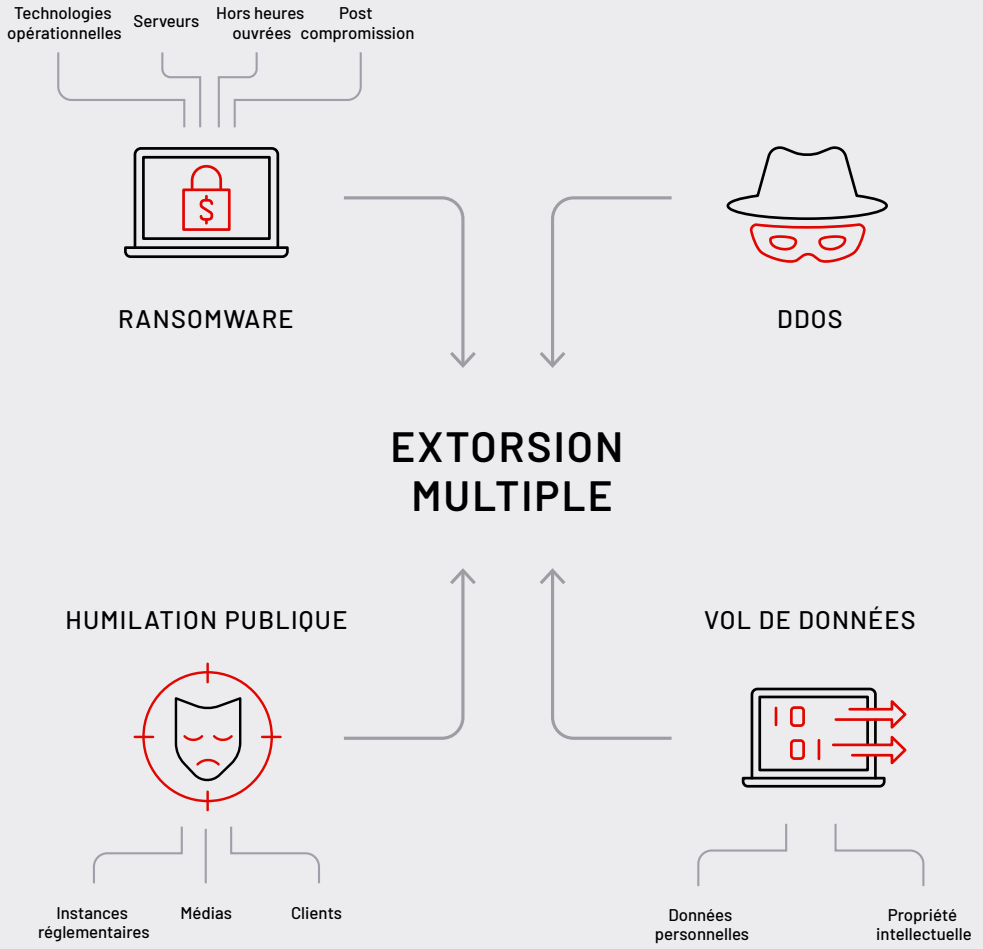
En général, les dirigeants et les responsables du risque associent les ransomwares au cryptage de fichiers. Le but recherché par les malfaiteurs ? Empêcher les utilisateurs légitimes d'y accéder, et ainsi nuire considérablement à la bonne marche de l'entreprise. Pour pallier ce risque d'attaque, les équipes de sécurité optent le plus communément pour un robuste programme de sauvegarde hors ligne. Toutefois, force est de constater qu'un tel dispositif ne suffit pas toujours à garantir une restauration simple ou sans heurts.

Avec la double extorsion, le potentiel de nuisance du ransomware classique monte d'un cran. En menaçant d'étaler ce vol de données hautement sensibles sur la place publique, ce qui n'était jusqu'à présent qu'une perturbation d'activité se transforme en une compromission en bonne et due forme. Comme l'illustre le schéma sur la page suivante, la double extorsion repose sur plusieurs points d'attaques : le cryptage par ransomware, le vol de données et « l'humiliation publique » de l'entreprise victime.

> *Réputation écornée, amendes pour infraction à la réglementation, recours collectifs en justice, coup d'arrêt aux projets de transformation digitale… les conséquences d'une compromission de données sont aujourd'hui bien plus graves qu'en 2019, année pivot où le ransomware a basculé dans la double extorsion.*
>
> — M-Trends 2021

L'extorsion et ses multiples facettes

En cas de double extorsion, les sauvegardes de données gardent certes toute leur utilité pour la reprise d'activité, mais elles ne peuvent rien face au vol de données en tant que tel. Au final, les entreprises ciblées se retrouvent coincées entre deux feux. D'un côté, l'attaquant et ses méthodes de coercition, à commencer par la menace de révéler au grand jour la compromission si la somme n'est pas acquittée. De l'autre, les instances réglementaires susceptibles de sanctionner les organisations piratées pour leur incapacité à protéger les données de leurs clients. Une double, voire triple, peine pour ces victimes si l'on ajoute le lourd préjudice en termes d'image.



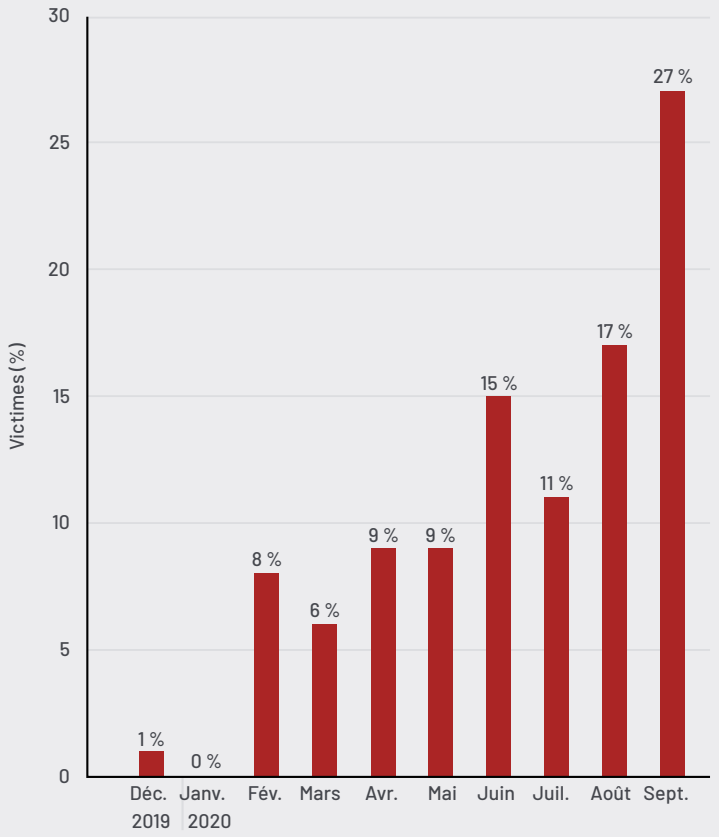
Des victimes sous haute pression

Lorsqu'elles sont victimes d'une double extorsion, les entreprises ont peu de contrôle sur le sort des données volées. Les cybermalfaiteurs utilisent la menace de divulgation comme moyen de pression dans les négociations, soit pour faire monter les enchères, soit pour exiger un paiement immédiat de la rançon. Du reste, pour semer le chaos au sein de l'entreprise, les attaquants disposent d'un véritable arsenal :

- **Harcèlement des collaborateurs**
- **Divulgation auprès des partenaires commerciaux**
- **Envoi de campagnes de spams**
- **Organisation d'une spéculation à la baisse sur le cours de l'action avant la révélation publique**
- **Fuite dans la presse et les médias**
- **Lancement d'une campagne d'humiliation publique sur les réseaux sociaux**
- **Création et mise à jour de sites web visant à jeter en pâture les victimes de compromission**

Dans certaines opérations d'extorsion, les sites « d'humiliation publique » se sont avérés particulièrement efficaces et ont fait des émules. En moyenne, Mandiant a recensé la création mensuelle d'au moins un site de ce genre entre mars et septembre 2020[4]. Et leur nombre connaît une croissance constante. Bien qu'aucun secteur d'activité ne soit épargné, l'industrie fait partie des cibles de choix.

Nombre de victimes jetées publiquement en pâture sur le Net



4. FireEye (avril 2021). M-Trends 2021.

Le prix fort des rançons

Pour les entreprises en proie à ce type d'extorsion, la révélation publique de leur attaque risque de gravement entacher leur réputation, et ainsi ébranler la confiance de leurs partenaires, actionnaires et clients. Cours de l'action, partenariat stratégique, chiffre d'affaires, rentabilité, fidélisation des clients et des talents… l'onde de choc crée des dégâts considérables. C'est pour cela que nombre d'entreprises n'hésitent pas à mettre la main au portefeuille, cédant ainsi aux méthodes crapuleuses, mais fort lucratives, de leurs assaillants. Pour autant, le paiement d'une rançon reste un énorme pari pour ces victimes qui ignorent si le mystérieux maître-chanteur tiendra parole.

En définitive, le versement ou non d'une rançon dépend du contexte de chaque entreprise et de la prise en compte de certains facteurs : délais de reprise de l'activité avec ou sans paiement, fiabilité des attaquants et degré de sensibilité des données subtilisées.

Au cours de ses interventions, Mandiant a observé les approches et caractéristiques suivantes chez les acteurs du ransomware :

Leur incapacité à recrypter les données ne les empêche pas pour autant de déployer d'autres moyens de pression pour extorquer encore plus d'argent de leurs victimes.

Ils tiennent parole dans un sens comme dans l'autre – ils libèrent les données lorsqu'ils reçoivent la rançon, mais ils savent aussi mettre leur menace à exécution en cas de non-versement.

Une fois la rançon acquittée, ils passent généralement à la victime suivante.

Ils ne garantissent pas la destruction des données volées (même s'ils en fournissent une soi-disant preuve)

Objectif prévention

Face à la recrudescence de ce type d'extorsion, les équipes de sécurité ont plus que jamais intérêt à prendre les devants pour mieux protéger leurs environnements. D'après les experts Mandiant, dans bien des cas, ces attaques auraient pu être neutralisées, voire évitées, si les entreprises s'étaient préalablement dotées de bonnes pratiques de configuration et de validation continue de la sécurité.

Place à la « prémédiation »

Contraction de « prévention » et de « remédiation », la prémédiation consiste à appliquer les mêmes contrôles et mesures de renforcement de sécurité qu'après une compromission, mais cette fois-ci avant.

Au cours de leurs missions de réponse aux incidents menées durant l'année 2020, les experts Mandiant ont relevé un certain nombre de points communs entre les entreprises victimes. Petit aperçu ci-contre :

> *C'est en réglant ces problèmes en priorité que vous réduirez les risques d'une attaque par ransomware ou d'une double extorsion.*

- Nombre important de comptes à privilèges élevés dans l'environnement Active Directory
- Recours aux noms principaux de service (SPN) pour configurer des comptes sans ordinateur à privilèges élevés
- Contrôles de sécurité non configurés pour minimiser l'exposition et l'utilisation des comptes à privilèges sur l'ensemble des terminaux
- Modification des objets Stratégie de groupe (GPO) par les attaquants pour déployer les ransomwares

Identifiez les menaces les plus sérieuses pour votre entreprise

Rien de tel qu'une Cyber Threat Intelligence (CTI) de terrain pour aider votre entreprise à renforcer ses défenses. Vous aurez ainsi toutes les cartes en main pour mieux cerner l'identité, les cibles, la chronologie, les motifs et les méthodes des acteurs cyber du moment. Priorisation et focalisation de votre action sur les menaces ciblant spécifiquement votre entreprise et secteur, tests de vos protocoles de sécurité, correction des vulnérabilités… la Threat Intelligence se prête à maints usages.

Mettez votre sécurité à l'épreuve

Testez en toute sécurité la résistance de vos défenses face à des scénarios de double extorsion réels. L'objectif ? Détecter les erreurs de configuration existantes et renforcer votre posture de sécurité. Ici comme ailleurs, la fatalité n'existe pas : une bonne préparation peut fortement réduire l'impact d'une attaque. Une simulation mettra ainsi en évidence vos points faibles et les ressources exposées dans votre environnement. De là, avec l'appui de services de sécurité spécialement conçus, vous pourrez évaluer votre capacité à détecter et à neutraliser les ransomwares et les risques associés, avec à la clé une amélioration de vos stratégies et tactiques de défense.

Pour en savoir plus, rendez-vous sur **www.mandiant.fr**

Mandiant
+1 833.3MANDIANT (362.6342)
info@mandiant.com

À propos de Mandiant

Depuis 2004, Mandiant® s'impose comme le partenaire de confiance des entreprises soucieuses de leur sécurité. Aujourd'hui, l'expertise et la Threat Intelligence leader de Mandiant sous-tendent des solutions dynamiques qui aident les organisations à développer des programmes plus efficaces et à instaurer une plus grande confiance dans leurs cyberdéfenses.

MANDIANT

M-EXT-EB-FR-FR-00396-02