TLP : BLANC

ENJOY SAFER TECHNOLOGY™

RANSOMWARES :
Regard sur l'art des pressions et des manipulations criminelles

V 2.0

Auteur : Ondrej Kubovič

TABLE DES MATIÈRES

V 2.0

Auteur : Ondrej Kubovič
Remerciements : Cette édition actualisée s'appuie sur la contribution fondamentale de Stephen Cobb de 2018, et sur les efforts actuels (2021) de mes collègues d'ESET : Rene Holt, James Shepperd, Nick FitzGerald, Hana Matušková et Klára Kobáková.

Auteur de l'édition d'origine : Stephen Cobb
Remerciements : Ce livre blanc doit beaucoup au travail de mes talentueux collègues d'ESET, James Rodewald, Ben Reed et Fer O'Neil, et aux compétences de mon équipe : Aryeh Goretsky, Bruce P. Burrell et Cameron Camp.

Août 2021

OBJECTIFS

Ce document a pour objectifs de démontrer à quel point les ransomwares sont devenus dangereux, de décrire les toutes dernières techniques utilisées par les gangs de pirates, et de suggérer ce que votre entreprise peut faire pour réduire son exposition aux attaques de ransomwares et les dommages qui en découlent. Trois vecteurs d'attaque de ransomwares sont abordés dans cet ordre : accès à distance, email et chaîne d'approvisionnement.

RANSOMWARES — LA PIRE DES CYBERMENACES

Une attaque de ransomware peut être définie comme une tentative d'extorsion, en empêchant une entreprise d'accéder à ses données. Les ransomwares sont un sous-ensemble des malwares, un terme collectif désignant toutes les formes de programmes malveillants, y compris les virus et les vers informatiques.

Les ransomwares sont probablement l'une des cybermenaces les plus graves auxquelles votre entreprise sera confrontée. Pourquoi ? Ces dernières années, les groupes de cybercriminels qui exploitent des ransomwares sous forme de services ont en effet perfectionné une approche différente et plus ciblée de ce type d'attaques, dont le volume est beaucoup plus difficile à mesurer.

Les cybercriminels trouvent également constamment de nouvelles méthodes pour s'assurer de recevoir la somme qu'ils demandent, généralement en augmentant la pression sur la victime. En 2019, ils ont notamment commencé à s'appuyer sur la double extorsion, qui combine le chiffrement « habituel » des données avec leur exfiltration. De cette manière, ils n'empêchent pas seulement l'accès aux fichiers critiques, précieux ou autrement sensibles de la victime, mais peuvent également les voler ou les vendre à d'autres acteurs malveillants.

Pour faire monter les enchères, certains opérateurs de ransomwares ont adopté la triple extorsion, en ajoutant une étape supplémentaire consistant à contacter les partenaires commerciaux ou les clients des victimes qui n'ont pas obtempéré à la demande de rançon. Les cybercriminels informent les partenaires/clients de la victime que leurs données sensibles ont été fuitées suite à l'attaque de ransomware, suggérant à ces partenaires/clients de faire pression sur la victime du ransomware pour qu'elle paie afin d'empêcher la publication de ces données. Dans certains cas, les attaquants exigent même un paiement auprès de ces partenaires/clients.

Ces dernières années, les pirates sont passés de la victimisation d'un grand nombre de personnes choisies au hasard, avec des demandes de rançon d'un montant modeste, à une approche plus ciblée, avec des demandes de rançon beaucoup plus importantes pour un plus petit nombre de victimes. Ces dernières se caractérisent par des entités aux moyens financiers plus importants, qui peuvent difficilement se permettre de perdre l'accès à leurs données ou le contrôle de celles-ci.

Exemples de cibles notables touchées par des ransomwares en 2021 :

- Kaseya corrigeait une vulnérabilité zero-day lorsque le ransomware REvil a déclenché son attaque
- Le ransomware REvil touche un prestataire d'armement nucléaire américain
- Les services de santé irlandais ont reçu une demande de rançon de 20 millions de dollars
- Une cyberattaque oblige la fermeture d'un important oléoduc américain
- ADATA frappé par l'attaque du ransomware Ragnar Locker
- Les services en ligne de la ville de Tulsa ont été perturbés par un ransomware

Une analyse de ces attaques montre que les victimes sont issues de différents secteurs, aussi bien publics que privés. Aucune entreprise ne jouit d'une immunité contre les ransomwares ciblés et, bien qu'il ne s'agisse pas de la menace la plus complexe sur le plan technique, la protection contre celle-ci est une préoccupation majeure pour de nombreuses équipes de sécurité.

LES RANSOMWARES SONT UN BUSINESS JUTEUX

Personne ne sait vraiment combien gagnent les opérateurs de ransomwares. L'estimation actuelle placerait les demandes de rançon à environ 170 000 dollars en moyenne, selon Group-IB. Toutefois, les chercheurs ajoutent que les groupes les plus effrontés demandent des dizaines de millions de dollars. Sodinokibi (alias REvil) a exigé ainsi 50 millions de dollars chacun à Quanta et Acer. Autres exemples de sommes demandées :

- Rapport de l'ENISA sur les ransomwares : 10 milliards d'euros de versements en 2019
- 144 millions de dollars de paiements à Ryuk entre 2013 et 2019, selon le FBI
- 100 millions de dollars de bénéfices en 2020 selon Sodinokibi, ce qui peut être exagéré
- 150 millions de dollars versés à Ryuk en 2020, selon AdvIntel
- 40 millions de dollars versés à Phoenix Locker en 2021 par CNA Financial ; le paiement le plus élevé
- 17,5 millions de dollars versés à Darkside en 2021 suite à l'attaque contre Colonial Pipeline
- 350 millions de dollars de versements en 2020 selon une estimation de Chainanalysis
- 70 millions de dollars demandés par Sodinokibi en 2021 pour un déchiffreur après l'attaque contre Kaseya

COMMENT LES RANSOMWARES AGISSENT PSYCHOLOGIQUEMENT

Les ransomwares utilisent la pression comme tactique de base. Parmi les nombreuses approches utilisées par les ransomwares, la principale menace qu'ils représentent consiste à chiffrer des données importantes et les mettre hors de portée de la victime. Qu'elles soient considérées comme des propriétés intellectuelles, personnelles ou professionnelles, les données sont sensibles et précieuses dans tous les cas.

Les points de pression augmentent lorsque les individus ou les entreprises peuvent se permettre de subir des atteintes à leur réputation, l'interruption de leur activité, voire des sanctions juridiques et financières. Le risque de tels dommages est exacerbé par une nouvelle tendance, appelée « doxing », employée par de nombreux gangs de ransomwares, qui passent au peigne fin les systèmes de leurs victimes à la recherche de données sensibles, qu'ils menacent ensuite de divulguer à moins qu'une somme supplémentaire ne soit versée en plus de la rançon. C'est une sorte de double extorsion. Le groupe Maze, qui a lancé la tendance en novembre 2019, a même amélioré son approche d'origine en créant son propre site de publication sur le Dark Web. Les victimes peuvent ainsi difficilement faire retirer leurs données divulguées.

Lorsque la pression augmente, la manipulation devient inévitable. Les multiples facettes des points de contact numériques des victimes sont souvent affectées, qu'il s'agisse d'attaques DDoS sur leur site web ou la présence désagréable des criminels sur leur réseau. Il s'agit notamment d'approches traumatisantes telles que le « print bombing », qui consiste à ordonner à plusieurs imprimantes d'un réseau d'imprimer la note de rançon, empêchant ainsi potentiellement la direction de conserver le contrôle de l'annonce interne et externe d'un incident. La pression peut également être exercée de manière plus directe, par exemple en accédant aux données des clients d'une entreprise puis en la démarchant par téléphone pour lui adresser de nouvelles menaces, ou la harceler publiquement pendant que son service informatique tente d'atténuer les impacts de l'attaque.

Ce ne sont là que quelques-unes des tactiques qui accompagnent les campagnes de ransomwares d'aujourd'hui. En termes simples, les ransomwares peuvent transformer un incident malencontreux en une guerre psychologique visant à forcer les victimes à agir contre leur propre volonté et dans leur meilleur intérêt. Alors que les criminels impliqués dans des enlèvements physiques commencent généralement leurs campagnes de pression avec un certain atout dans leurs manches, mais peuvent être à court d'options par la suite, les cybercriminels disposent d'une variété encore plus grande de méthodes qu'ils peuvent utiliser pour prendre le dessus et anéantir tout espoir de récupération des données.

Pour atteindre leurs objectifs malveillants, les cybercriminels utilisent de multiples approches qui leur permettent potentiellement d'obtenir un accès à distance, de surveiller les activités de leurs victimes, puis d'exercer une pression chirurgicale ciblée. Cela démontre la mainmise qu'ils peuvent avoir sur les données, les réseaux, la continuité des activités et la réputation de leurs victimes. Ces attaques n'ont pas nécessairement besoin de provenir de malwares personnalisés, d'exploitations de vulnérabilités zero-day ou de campagnes de persistance à long terme. Elles peuvent simplement être le résultat de mauvaises pratiques de sécurité de la part des collaborateurs, d'une mauvaise configuration de RDP ou d'autres outils d'accès à distance, ou de lacunes dans les pratiques et les processus, tant au niveau de votre entreprise que de celui de vos prestataires de services ou d'autres acteurs de votre chaîne d'approvisionnement.

COMMENT LES RANSOMWARES PROCÈDENT TECHNIQUEMENT

Les ransomwares constituent un fléau depuis plus d'une décennie, et leur champ d'action s'est élargi tout au long de la période d'accélération de la transformation digitale provoquée par la pandémie de COVID-19. Une corrélation claire est rapidement apparue entre les confinements dus à COVID-19 et les emails de phishing qui étaient souvent basés sur des craintes actuelles d'impacts négatifs sur l'entreprise et d'opportunités perdues.

Ce phénomène s'est également manifesté par le fait que des collaborateurs devaient soudainement travailler depuis leur domicile et accéder (souvent pour la première fois) aux systèmes et services internes de l'entreprise via le protocole d'accès à distance RDP. C'est devenu un vecteur très courant pour diffuser des ransomwares. Avec les droits d'administration qui accompagnent certains cas d'utilisation de RDP, les ransomwares peuvent apparaître en même temps qu'un certain nombre d'autres problèmes de sécurité dans un réseau.

Nous pouvons également avancer que le maniement des ransomwares comme outil de cybercriminalité sert à des fins ambitieuses à grande échelle. Des acteurs peu qualifiés peuvent se lancer et programmer des malwares imparfaits qui auront un impact sur un nombre très limité de victimes à l'aide du spam. D'autres peuvent tenter leur chance en propageant des malwares, y compris des ransomwares, via des téléchargeurs ou des botnets. Des acteurs plus ambitieux peuvent s'abonner à un ransomware entièrement paramétré et le déployer pour en tirer un bénéfice, devenant ainsi des affiliés des développeurs du ransomware grâce à un modèle commercial de ransomware sous forme de services (RaaS).

Les acteurs criminels qui font appel au RaaS exploitent souvent des vulnérabilités pour accéder à une machine, puis se déplacent latéralement vers un serveur et dans l'ensemble du réseau, et décident ensuite d'utiliser un ransomware. S'ils disposent de ressources importantes, ces gangs peuvent acheter des exploitations de vulnérabilités zero-day ou même développer les leurs, ce qui leur permet de contourner de nombreux types de technologies d'atténuation proactive. Enfin, que ce soit dû à la chance, à des compétences ou d'importants investissements tant humains que financiers, les pirates peuvent mener des attaques contre des chaînes d'approvisionnement pour accéder à des écosystèmes informatiques entiers. Par exemple, en prenant le contrôle des plateformes des prestataires de services managés (MSP) et des outils de productivité les plus populaires, les cybercriminels peuvent diffuser des ransomwares sur plusieurs réseaux (et donc plusieurs entreprises) à grande échelle. Le recours à une attaque contre une chaîne d'approvisionnement pour positionner un ransomware est un autre scénario redoutable auquel les entreprises doivent faire face.

Il est essentiel de s'informer sur la diversité croissante des approches et la rapidité avec laquelle les ransomwares peuvent évoluer, afin de déterminer la posture de sécurité nécessaire qui évitera l'interruption des activités. L'innovation dans le domaine des ransomwares évolue rapidement, comme l'ont observé les chercheurs qui ont étudié Sodinokibi (alias REvil). Il est capable de chiffrer silencieusement des fichiers en mode sans échec sur un PC, mais cela oblige quand même l'utilisateur à se connecter. En l'espace d'un mois,

cette nouvelle fonctionnalité a été améliorée. Les pirates peuvent modifier le mot de passe de connexion et configurer le PC pour qu'il redémarre automatiquement en mode sans échec, ce qui en fait un vecteur viable pour une campagne à grande échelle.

Les dispositifs de stockage réseau (NAS), qui sont couramment utilisés pour partager des fichiers et effectuer des sauvegardes, ont également attiré l'attention des gangs de ransomwares. En 2021, le fabricant d'appareils NAS QNAP a prévenu ses clients que le ransomware eCh0raix attaquait ses appareils, en particulier ceux avec des mots de passe faibles. La télémétrie d'ESET pour le quatrième trimestre 2020 a montré qu'eCh0raix était le ransomware qui ciblait le plus les appareils NAS.

RANSOMWARES VIA RDP

Un terminal RDP est un appareil sous Windows qui utilise le logiciel RDP (protocole d'accès à distance) afin d'être accessible via un réseau tel qu'Internet. RDP permet d'accéder à distance à des postes Windows d'une entreprise, comme si leurs claviers et leurs écrans se trouvaient sur votre bureau. Les avantages du déploiement de RDP peuvent être multiples : administration et dépannage des appareils des collaborateurs, accès à des ressources centralisées telles que des ordinateurs de bureau pouvant exécuter des charges de travail lourdes, des applications ou des bases de données.

RDP doit être activé sur les systèmes de l'entreprise auxquels les employés doivent accéder à distance. Idéalement, une authentification à deux facteurs (2FA) devrait également être activée. Les collaborateurs se connectent ensuite à ces systèmes via le logiciel RDP, par exemple sur leur ordinateur portable. Lorsque l'adresse réseau du système distant est saisie, le logiciel client se connecte au port désigné sur le système distant (le port par défaut pour RDP est 3389, mais cela peut être modifié). Le système distant présente un écran de connexion qui demande un nom d'utilisateur et un mot de passe. Vous pouvez voir à quoi cela ressemble sur un système Windows dans la Figure 1.

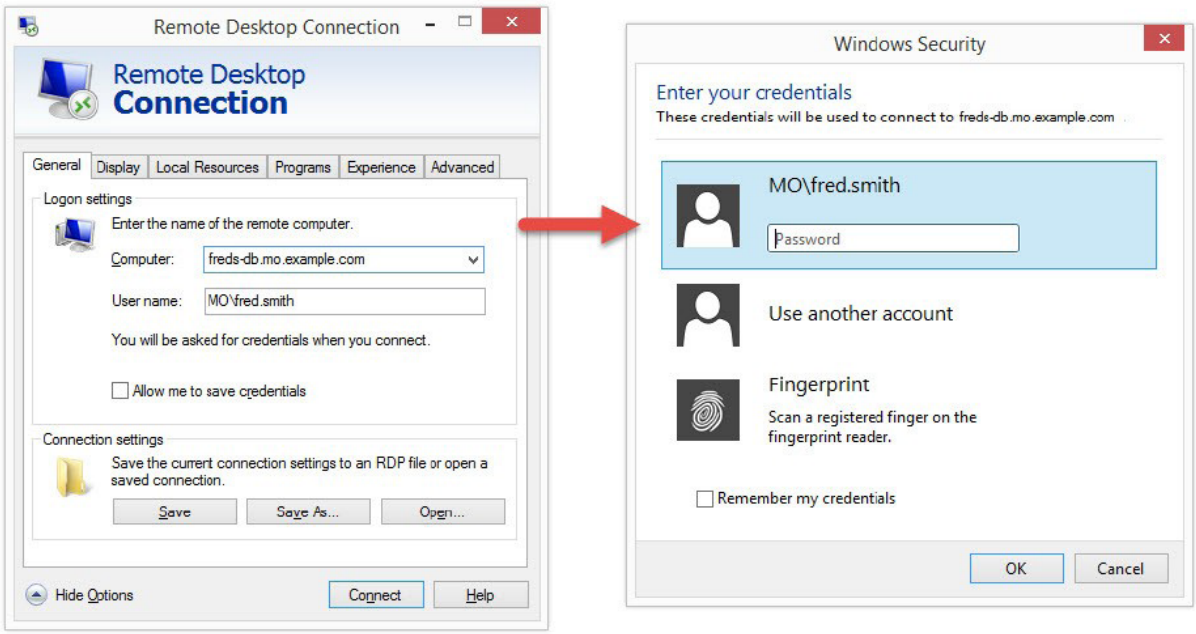

Figure 1 // Écran de connexion RDP

Les entreprises utilisent principalement RDP de deux manières :

1. La première pour gérer les programmes exécutés sur un serveur, par exemple un site web ou une base de données de back-end. Dans ce scénario, un administrateur système ouvre le port 3389 au monde extérieur pour permettre l'administration à distance. C'est la configuration la plus simple.
2. La seconde consiste à permettre l'accès à distance à des postes de travail ou à des machines virtuelles qui ont à leur tour accès à des ressources non accessibles depuis l'extérieur du réseau de l'entreprise. L'accès à ces systèmes via RDP signifie qu'il n'est pas nécessaire d'ouvrir directement des serveurs internes sensibles au monde externe. Il se peut également que les ordinateurs de bureau disposent d'une puissance de traitement nécessaire à de nombreux processus ou qu'ils soient équipés de logiciels spécialisés coûteux dont le personnel a besoin pour accomplir certaines (voire la plupart) de ses tâches. Encore une fois, lorsque cela se fait par Internet, le port 3389 est souvent ouvert.

Pour les criminels, il est facile de trouver des systèmes accessibles depuis le monde extérieur et de les utiliser à des fins malveillantes, car :

- Les systèmes RDP vulnérables sont faciles à trouver.
- Des pirates peuvent facilement prendre pied sur des systèmes RDP mal configurés,
- ce qui est le cas de nombreux systèmes RDP.
- Les outils et les techniques d'escalade de privilèges et d'obtention de droits d'administration sur des systèmes RDP compromis sont largement connus et disponibles.

Les systèmes RDP peuvent être identifiés par des moteurs de recherche spécialisés tels que Shodan, qui parcourent constamment Internet à la recherche d'appareils connectés et en collectent des informations. Au 15 juin 2021, Shodan indiquait qu'il y avait plus de 3 millions de systèmes ouverts à Internet via le port 3389 (une inscription peut être nécessaire pour consulter les requêtes Shodan filtrées). Comme vous pouvez le voir sur l'interface Shodan à la Figure 2, plus d'un million de ces systèmes se trouvaient aux États-Unis.

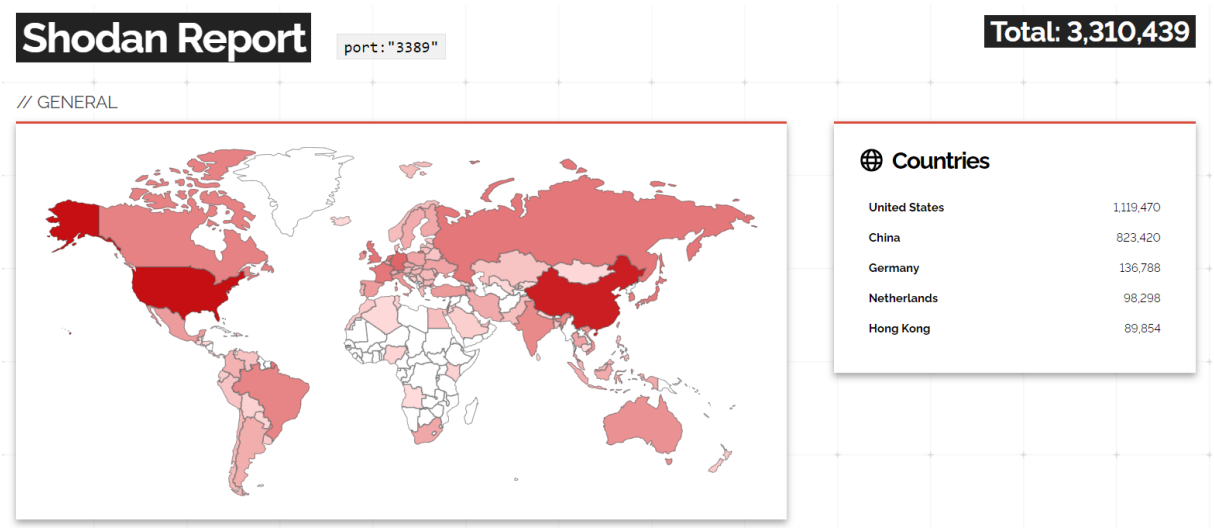

Figure 2 // Plus de 3 millions de systèmes sur Internet utilisant le port 3389 (Source : Shodan)

En lançant une requête différente, nous avons découvert que plus de 2,7 millions de machines utilisaient explicitement RDP. Pour un pirate, toutes ces machines sont des cibles potentielles. Si la connexion à un système RDP nécessite généralement un nom d'utilisateur et un mot de passe, ceux-ci peuvent être étonnamment faciles à deviner pour les attaquants, et beaucoup d'entre eux y parviendront.

Pour ceux disposant de fonds suffisants, il suffit simplement d'acheter un accès à des systèmes RDP compromis. Leurs identifiants sont disponibles sur les places de marché du Dark Web. Notez que les ransomwares ne sont pas la seule raison d'acheter des identifiants RDP piratés. Parmi les autres utilisations

d'un système RDP compromis figurent l'envoi de spam, l'hébergement de malwares, le craquage de mots de passe, l'extraction de cryptomonnaie, et toute une série d'activités pour lesquelles l'anonymat est souhaitable et l'attribution ne l'est pas, par exemple des achats frauduleux et le blanchiment d'argent.

Si seuls un nom d'utilisateur et un mot de passe sont nécessaires pour accéder aux appareils à distance, un attaquant ayant identifié ces cibles peut essayer d'en deviner les identifiants en faisant plusieurs tentatives. On parle d'attaque par force brute lorsqu'une base de données d'identifiants plausibles est utilisée pour tenter des connexions à un rythme élevé. En l'absence de tout mécanisme permettant de limiter le nombre de mauvaises suppositions, ces attaques peuvent être très efficaces et même conduire au piratage d'un réseau entier.

La télémétrie d'ESET confirme que RDP est l'un des vecteurs d'attaque les plus courants, avec un volume dépassant 71 milliards de détections entre janvier 2020 et juin 2021. Si l'augmentation la plus notable a eu lieu au premier semestre 2020, 2021 a vu les chiffres les plus élevés à ce jour. En comparant le premier semestre 2020 au premier semestre 2021, ESET a constaté une multiplication par six des attaques par force brute détectées contre RDP.

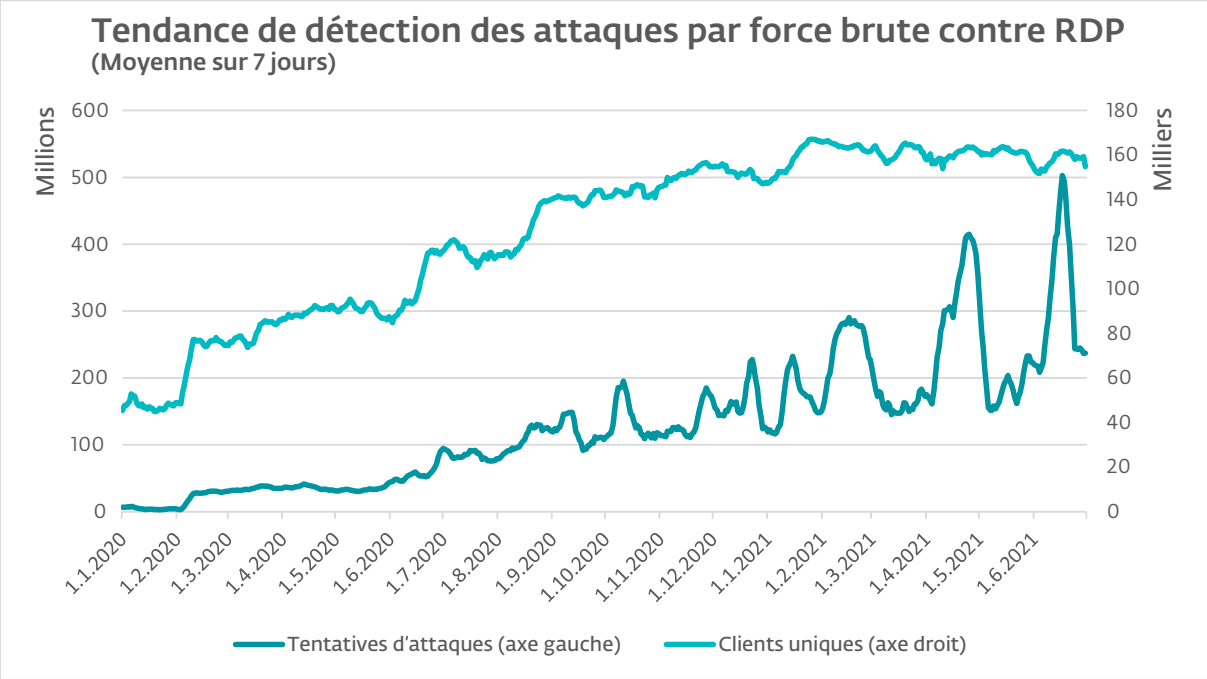

Figure 3 // Tendances des tentatives de connexion RDP et des clients uniques entre janvier 2020 et juin 2021, moyenne mobile sur sept jours

L'obtention d'un accès non autorisé depuis Internet à des appareils utilisant RDP peut nécessiter plus d'efforts au départ qu'une attaque de ransomware par email, mais le vecteur RDP offre aux pirates des avantages considérables, tels que le détournement d'un accès légitime, la possibilité d'échapper aux mécanismes de protection des terminaux, et la possibilité de compromettre rapidement plusieurs systèmes, voire l'ensemble du réseau, au sein d'une même entreprise.

> « Les attaques via RDP peuvent passer sous le radar de nombreuses méthodes de détection, ce qui signifie moins de mesures et moins de sensibilisation aux menaces. »

Par exemple, toute entreprise dotée d'un programme bien conçu de sécurité de l'information détectera et bloquera un ransomware intégré dans un fichier joint à un email entrant. Ces incidents sont généralement consignés et signalés par les programmes de protection des terminaux, et les éditeurs de ces programmes rassemblent des statistiques anonymes sur les tendances des menaces à partir de ces signalements.

Il en va souvent de même pour les tentatives visant à inciter les utilisateurs à consulter des sites web malveillants propageant des ransomwares. Toutefois, lorsqu'un pirate disposant de privilèges d'administrateur système sur un serveur compromis désactive le logiciel de protection avant de déployer son ransomware, cette attaque peut très bien échapper à toute détection.

Mouvement latéral et détournement de ressources légitimes

Pour un opérateur de ransomwares, un système RDP compromis peut signifier bien plus qu'une extorsion d'argent pour déchiffrer les fichiers sur cette machine. C'est particulièrement vrai si ce système peut fournir un point d'entrée à un réseau entier, permettant potentiellement le chiffrement à grande échelle de tous les postes qui y sont présents ou le vol de données critiques. C'est ce qui s'est passé dans de nombreux cas cités plus haut, et les techniques pour mener à bien ce type d'attaque ne sont pas un secret.

Après avoir obtenu un accès à distance, l'attaquant voudra en savoir plus sur la machine compromise, notamment la possibilité de la détourner pour établir des connexions à d'autres systèmes. Si l'accès n'a pas été obtenu avec les identifiants administrateur, plusieurs techniques peuvent être utilisées pour élever les privilèges à un niveau administrateur. Si une protection des terminaux est installée sur le système et qu'elle peut être désactivée par un utilisateur disposant de privilèges administrateur, l'attaquant essaiera probablement de le faire. Il lui sera ainsi plus facile de télécharger des malwares supplémentaires. Notez que dans le texte suivant, lorsque des actions sont décrites comme étant effectuées « par l'attaquant », elles peuvent ne pas être effectuées par une personne au clavier mais par un logiciel utilisé pour automatiser certains aspects de l'attaque.

Certains attaquants tenteront d'introduire le moins de malwares possible afin de minimiser les chances de détection. Au lieu de cela, une stratégie appelée « living off the land » sera employée, qui a pour objectif d'utiliser des logiciels légitimes, souvent les mêmes que ceux utilisés par les administrateurs réels du système, et même des outils standard installés dans le système d'exploitation de base, afin de pénétrer dans le reste du réseau. Par exemple, PsExec et Windows Management Instrumentation Command-line (WMIC) sont souvent détournés pour effectuer des mouvements latéraux dans des réseaux compromis. Comme il existe des raisons valables d'utiliser ces programmes, la détection d'une utilisation détournée par un attaquant peut être difficile, mais pas impossible. Pour plus d'informations sur les possibilités de détection, voir la discussion sur les outils de détection et de traitement pour terminaux (EDR) ci-dessous.

Le terme « mouvement latéral » décrit une stratégie consistant à prendre pied sur un système et l'utiliser pour compromettre d'autres appareils qui peuvent être atteints à partir de là. Par exemple, des pirates peuvent utiliser des identifiants compromis pour cibler un serveur qui n'est même pas présent dans l'entreprise ciblée, et utiliser sa connexion à l'infrastructure principale pour transmettre un ransomware.

En plus de détourner des ressources légitimes, les attaques de ransomwares peuvent tirer parti de vulnérabilités non corrigées dans des logiciels légitimes. L'un des exemples les plus archétypaux est sans doute le ransomware WannaCryptor, qui s'est propagé via EternalBlue, une grave vulnérabilité dans l'implémentation du protocole Server Message Block de Microsoft. Malgré la disponibilité publique de correctifs pendant environ deux mois avant la campagne WannaCryptor du 12 mai 2017, les attaquants ont quand même réussi à trouver et infecter plus de 200 000 machines vulnérables. Même dans les derniers stades de cette épidémie, les appareils infectés sont restés des menaces, car les utilisateurs peuvent par exemple avoir introduit sans le savoir des ordinateurs portables compromis dans ce que les administrateurs considéraient être un périmètre sécurisé.

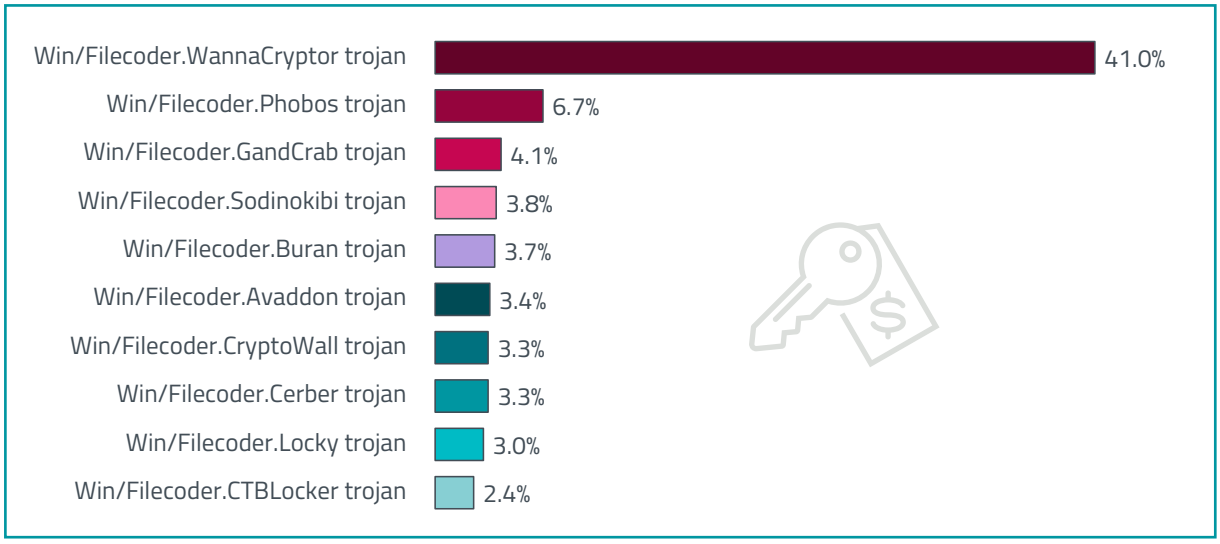

Figure 4 // Les 10 principales familles de ransomwares en T1 2021 (% de détections de ransomwares)
Quatre ans après son attaque dévastatrice de 2017, WannaCryptor figure toujours parmi les familles de ransomwares les plus détectées (source des données : Rapport d'ESET sur les menaces de T1 2021)

Bien sûr, il est possible que le premier point de contact d'un attaquant avec une entreprise soit un serveur exécutant une base de données critique, auquel cas un criminel opportuniste peut décider d'économiser du temps et des efforts, et réaliser rapidement des profits en volant simplement des données, en chiffrant et en rançonnant les fichiers utilisés par cette seule ressource. Cependant, la persistance permet de réaliser beaucoup plus de gains, c'est pourquoi de nombreux opérateurs de ransomwares continueront probablement d'effectuer des opérations de reconnaissance même après le vol des données et avant de les chiffrer, juste pour s'assurer qu'ils ont suffisamment de poids face à leur victime.

Comment se défendre contre les attaques ciblant RDP

Il est possible de défendre les systèmes fonctionnant sous RDP contre les accès non autorisés et de priver ainsi les criminels de ce vecteur d'attaque de plus en plus populaire, qu'ils diffusent des ransomwares ou qu'ils se livrent à d'autres accès non autorisés au système. Des stratégies de défense sont abordées dans cette section, et une checklist plus technique est disponible dans la section Protection de RDP contre les ransomwares.

Bien sûr, votre entreprise a peut-être déjà mis en place des politiques pour assurer la sécurité de l'accès à distance. Vous pouvez avoir configuré des règles exigeant que tous les accès RDP soient acheminés via un VPN (réseau privé virtuel), sécurisés par une authentification multifacteur (MFA), limités à des rôles spécifiques, sur des systèmes spécifiques configurés de manière sécurisée, corrigés rapidement, surveillés en permanence, dotés d'un pare-feu approprié et sauvegardés régulièrement.

Mais même si vous avez mis en place de telles règles ou que vous vous efforciez de les mettre en place, elles ne pourront garantir à elles seules que votre accès à distance ne soit jamais piraté. Vous devez toujours veiller à ce que tout le monde respecte les règles, tout en vous préparant à faire face à une attaque qui, d'une manière ou d'une autre, réussira malgré ces règles.

Une première étape fondamentale pour se défendre contre les attaques de ransomwares RDP consiste à faire l'inventaire de vos ressources en contact avec Internet. Dire que vous ne pouvez pas défendre un système si vous n'êtes pas au courant de son existence peut sembler une évidence, mais d'après nos enquêtes, le scénario suivant n'est pas si inhabituel : une entreprise est attaquée via une ressource connectée à Internet dont le personnel de sécurité de l'entreprise n'a appris l'existence qu'après l'attaque.

Vous devez mettre en place des processus pour vous assurer que cela n'arrive pas à votre entreprise. Il ne devrait par exemple pas être possible pour un prestataire ou un collaborateur de connecter un serveur

physique ou virtuel à la fois au réseau de l'entreprise et à Internet, à moins que ce serveur ne soit configuré de manière sécurisée. Cette configuration doit être effectuée avant que le serveur ne soit mis en service, en particulier s'il utilise RDP avec un compte d'administrateur de domaine.

Lorsque vous avez fini de dresser l'inventaire des ressources connectées à Internet, vous devez documenter celles pour lesquels l'accès à distance est activé, puis décider si cet accès est nécessaire. Si un accès est nécessaire, exigez des mots de passe longs pour les comptes concernés. Quelle longueur ? Les mots de passe de 15 caractères ou plus peuvent sembler d'une longueur rédhibitoire, mais ils sont facilement mémorisables si l'on utilise des phrases de passe. Les mots de passe de cette longueur n'ont pas besoin d'être assortis de règles de complexité, qui ont tendance à pousser les gens à adopter de mauvaises pratiques de mots de passe d'après certaines études. Après avoir défini des exigences strictes en matière de longueur de mot de passe pour les comptes, déterminez s'il est possible ou non de limiter ces systèmes au réseau interne et d'y accéder à distance en utilisant un VPN d'entreprise.

Si un système doit être accessible depuis Internet via RDP et que l'utilisation d'un VPN n'est pas possible, utilisez au moins la MFA afin de ne pas dépendre uniquement des mots de passe pour la protection. Veillez cependant à utiliser une solution de MFA qui ne s'appuie pas sur les SMS. Les criminels disposent de nombreux moyens pour déjouer l'authentification par SMS (souvent développés par des auteurs de malwares ciblant les clients des banques en Europe, où la MFA par SMS est utilisée depuis de nombreuses années pour confirmer les transactions bancaires).

Si vous êtes obligé de vous fier aux mots de passe parce que la MFA n'est pas disponible, peut-être en raison d'une politique budgétaire peu perspicace, empêchez au moins les intrus potentiels de faire des tentatives répétées pour deviner les identifiants. Définissez un seuil de trois tentatives de connexion invalides, après quoi toute tentative de connexion est refusée pendant une période donnée, par exemple trois minutes. Dans la Figure 3 , vous pouvez voir à quoi cela ressemble dans Windows.

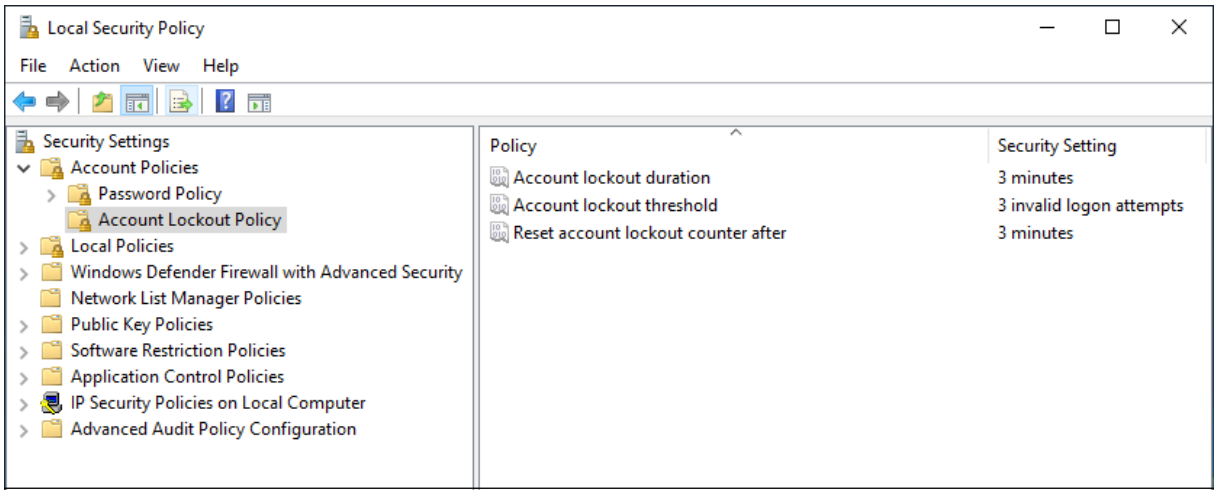

Figure 5 // Politique de verrouillage des comptes

Vous pouvez également changer le port d'écoute RDP, afin que les pirates aient légèrement plus de difficultés à le trouver. Cela peut se faire via des paramètres système, mais vous devrez également modifier les règles du pare-feu pour prendre en compte le port désigné. Gardez à l'esprit qu'il s'agit d'une simple sécurité par obscurcissement, et qu'il ne faut pas s'y fier pour assurer la sécurité des systèmes RDP (voir la section Protection de RDP contre les ransomwares pour plus de détails).

Le durcissement et l'application de correctifs doivent être effectués pour tous les appareils accessibles à distance. En plus de veiller à ce que toutes les vulnérabilités de sécurité soient identifiées et corrigées, vous

devez vous assurer que tous les services et composants non essentiels ont été supprimés ou désactivés, et que les paramètres sont configurés pour maximiser la sécurité.

Par exemple, sur les systèmes Windows, vous pouvez utiliser des stratégies de restriction logicielle (SRP) pour empêcher l'exécution de fichiers à partir de dossiers tels que AppData et LocalAppData, qui sont parfois utilisés par des malwares. Vous pouvez également utiliser AppLocker pour contrôler les applications et les fichiers que les collaborateurs sont autorisés à exécuter sur leurs machines. Bien entendu, un système de sauvegarde et de récupération complet et bien testé est la dernière ligne de défense contre les ransomwares RDP. Étant donné que la sauvegarde est essentielle pour survivre aux ransomwares, quel que soit le vecteur d'attaque, elle sera abordée après la présentation des trois autres vecteurs, à savoir la messagerie, la chaîne d'approvisionnement et les vulnérabilités.

Petite parenthèse : le protocole SMB, second coupable derrière RDP

Le protocole SMB (Server Message Block), qui est principalement utilisé pour le partage de fichiers et d'imprimantes dans les réseaux d'entreprise, est également largement détourné par les ransomwares pour s'introduire à distance. Durant les quatre premiers mois de 2021, les technologies ESET ont bloqué 335 millions d'attaques par force brute contre des services SMB accessibles au public. Bien que cela représente une baisse de 50 % par rapport aux quatre derniers mois de 2020, les attaques via SMB restent une menace importante. Par exemple, le ransomware WannaCryptor (alias WannaCry), qui représentait 41 % des détections de ransomwares au cours de la même période, se propage en exploitant le protocole vulnérable SMBv1.

Suivez ces conseils pour vous protéger contre les menaces ciblant le protocole SMB :

- Désactivez SMBv1 et SMBv2 en gardant à l'esprit que toutes les dépendances à ces versions obsolètes doivent être gérées.
- Passez à la dernière version du protocole SMB, qui est actuellement SMBv3.
- Utilisez les paramètres de politique de groupe pour veiller à ce que la signature SMB soit requise entre les hôtes et les contrôleurs de domaine afin d'empêcher les attaques dites par rejeu sur votre réseau.
- Bloquez les ports TCP 445 et 139, ainsi que les ports UDP 137 et 138 depuis Internet. Cela empêchera toutes les versions de SMB d'être accessibles depuis l'extérieur de votre réseau.

Protection de RDP contre les ransomwares

Stratégies et techniques à envisager :

1. **Documentez le problème**
   Veillez à ce que toutes les ressources de votre entreprise connectées à Internet soient connus des personnes chargées de les sécuriser. Mettez en place un processus pour vous assurer que tous les nouveaux appareils soient inclus.
2. **Limitez les ressources exposées**
   Veillez à ce qu'aucune ressource digitale ne soit accessible à distance directement depuis Internet, à moins que son utilisation n'ait été approuvée de cette manière et que sa configuration soit appropriée. Demandez pourquoi l'accès à la ressource ne peut pas être effectué via VPN. Désactivez RDP lorsqu'il n'est pas nécessaire (ces articles montrent comment procéder sur différentes versions de Microsoft Windows : Serveur 2019, Serveur 2016, Serveur 2008/R2, Windows 10, Windows 8, Windows 7).
3. **Protégez les ressources exposées**
   Si vous devez absolument utiliser le protocole RDP sans VPN, assurez-vous de prendre toutes les mesures suivantes :

a. Changez régulièrement le mot de passe du compte utilisateur auquel vous vous connectez sur la machine distante. Veillez à modifier le mot de passe par défaut qui est parfois généré automatiquement pour les instances dans le Cloud.

b. Veillez à ce que des mots de passe complexes (une phrase de passe longue de plus de 15 caractères, sans information liée à l'entreprise, aux noms des produits ou aux utilisateurs, est obligatoire) soient utilisés.
c. Définissez un seuil de verrouillage de l'accès à distance après plusieurs tentatives de connexion infructueuses.

   En paramétrant votre ordinateur pour qu'il verrouille un compte pendant un certain temps après un certain nombre de tentatives incorrectes, vous ferez obstacle aux attaquants qui utilisent des outils automatisés pour deviner les mots de passe (attaque par force brute). Pour définir une politique de verrouillage de compte dans Windows :

   Rendez-vous dans Démarrer-->Programmes-->Outils administratifs-->Politique de sécurité locale

   Sous Politiques de comptes-->Politiques de verrouillage de comptes, définissez des valeurs pour les trois options : trois tentatives invalides avec des durées de verrouillage de trois minutes sont des choix raisonnables.
d. Testez et déployez des correctifs pour toutes les vulnérabilités connues, et veillez à ce que celles qui sont les plus courantes telles que BlueKeep et EternalBlue figurent parmi les failles corrigées. Lorsqu'un ordinateur ne peut pas être corrigé, prévoyez rapidement de le remplacer.
e. Utilisez l'authentification au niveau du réseau pour renforcer la sécurité de l'hôte de la session d'accès à distance, en exigeant que l'utilisateur soit authentifié auprès du serveur de l'hôte avant la création d'une session.
f. Choisissez un autre port que le port 3389 par défaut de RDP, mais notez qu'il s'agit simplement d'une sécurité par obscurcissement et que ce ne doit pas être la seule mesure que vous prenez.

   Pour changer le port, modifiez la valeur dans la base de registre (AVERTISSEMENT : n'effectuez pas cette opération si vous n'êtes pas familier avec la base de registre Windows et TCP/IP) : HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber.
g. Limitez l'accès à RDP aux seules adresses IP publiques autorisées à s'y connecter. Cela peut être fastidieux si les utilisateurs distants n'ont pas d'adresse IP statique, par exemple lorsqu'ils se déplacent ou travaillent à domicile.
h. Utilisez plus d'un facteur d'authentification. Il existe trois possibilités : des choses que vous connaissez, telles que les noms d'utilisateur et les mots de passe ; des choses qui vous décrivent, telles que des empreintes digitales ou vocales ; des choses que vous possédez, telles que votre téléphone, qui peut recevoir un code d'accès à usage unique ou exécuter une application d'authentification pour en générer un pour vous.

   Cependant, si vous utilisez des codes envoyés aux téléphones comme second facteur, évitez les codes SMS car les criminels ont l'habitude de déjouer l'authentification par SMS (comme décrit dans cet article). Il existe de bonnes solutions de MFA qui tirent parti de l'omniprésence des téléphones mais qui ne communiquent pas par SMS (telles qu'ESET Secure Authentication).
i. Renforcez les permissions et les droits utilisateurs. Désactivez l'exécution de fichiers à partir des dossiers AppData et LocalAppData. Bloquez l'exécution à partir du sous-répertoire Temp (qui fait partie de l'arborescence AppData par défaut). Bloquez l'exécution de fichiers à partir des répertoires de travail de différents utilitaires de décompression (par exemple WinZip ou 7-Zip). Par ailleurs, si vous disposez d'un bon produit de protection des terminaux, vous pouvez créer des règles HIPS pour n'autoriser que certaines applications à fonctionner sur l'ordinateur, et bloquer toutes les autres par défaut).
j. Pour accéder aux serveurs, utilisez des mots de passe uniques sur les comptes locaux disposant de droits d'administration (par exemple en utilisant LAPS ou un service robuste de gestion des mots de passe). Limitez également les droits d'accès au serveur à un groupe restreint d'utilisateurs. Cela réduit la surface d'attaque des serveurs en limitant le nombre d'utilisateurs autorisés à y accéder.
k. Configurez si possible le niveau de chiffrement de la connexion du client RDP sur « élevé ». Sinon, utilisez le niveau de chiffrement le plus élevé disponible pour les connexions.

l. Installez une passerelle VPN pour négocier toutes les connexions RDP provenant de l'extérieur de votre réseau local.
m. Protégez par un mot de passe votre solution de protection des terminaux pour empêcher la modification de ses paramètres sans authentification, la désactivation de la protection ou même sa désinstallation (utilisez un mot de passe différent de celui utilisé pour les identifiants de connexion RDP).
n. Activez le blocage des exploitations dans les logiciels de protection des terminaux, qui est une technologie de détection des anomalies sans recours à des signatures pour surveiller le comportement des applications couramment ciblées.
o. Isolez tout ordinateur non sécurisé auquel vous devez accéder depuis Internet via RDP.
p. Lorsque le personnel et les prestataires se situent dans le même pays, ou parmi une courte liste de pays, envisagez de bloquer l'accès depuis les pays exclus en instaurant un géoblocage des adresses IP au niveau de la passerelle VPN afin d'empêcher les connexions d'attaquants depuis l'étranger.

RANSOMWARES PAR EMAIL

Tout expert en sécurité chevronné vous le dira : les menaces qui pèsent sur les systèmes d'information sont cumulatives. Par exemple, ce n'est pas parce que certains criminels se sont tournés vers les serveurs accessibles à distance comme vecteur d'attaque des ransomwares que vous devez ignorer les autres vecteurs. Certains criminels utilisent encore des pièces jointes à des emails pour installer des malwares qui servent d'étape initiale d'infection, laquelle se termine par un ransomware.

Ils peuvent utiliser ce vecteur pour diffuser des téléchargeurs qui installent des malwares sur l'ordinateur du destinataire de l'email, ou pour s'implanter sur un ordinateur connecté en réseau. Cette intrusion peut servir de base à une tentative de vol de données précieuses et de chiffrement des fichiers de toute l'entreprise, avant une demande de rançon très élevée, comme c'est souvent le cas dans les attaques ciblées de ransomwares via RDP.

En particulier, la messagerie est l'un des principaux vecteurs des botnets, tels que Trickbot, Qbot et Dridex, qui utilisent généralement des documents Microsoft Office avec des macros malveillantes pour l'intrusion initiale, et des ransomwares comme étape finale. Voici quelques-unes des relations déjà observées entre les familles de botnets et de ransomwares : Emotet avec Qbot, Trickbot, Ryuk et Conti ; Dridex avec FriedEx (alias BitPaymer) ; Nemucod avec Avaddon, Dridex, Ursnif, et Trickbot ; et SmokeLoader et Zloader avec LockBit et Crysis.

Les forces de police ont mis Emotet hors service au début de l'année 2021, ce qui a donc contribué à une très forte baisse des téléchargements diffusés par email. Nous décrivons les impacts des campagnes d'Emotet, à la fois avant et après son démantèlement, dans le Rapport d'ESET sur les menaces de T1 2021, le Rapport d'ESET sur les menaces de Q4 2020 et le Rapport d'ESET sur les menaces de Q3 2020.

Malgré le déclin significatif des téléchargeurs, les acteurs malveillants utilisant des macros compromises sont restés la principale menace contre la messagerie en 2021. Le mois de janvier a même été marqué par un pic d'emails contenant des documents Office malveillants conduisant aux téléchargeurs Dridex et Emotet.

Les activités de Trickbot, un autre botnet répandu, ont été perturbées en octobre 2020, mais il semble qu'il ne s'agissait que d'un contretemps temporaire, car ses opérateurs ont lancé dès le mois de janvier 2021 une nouvelle campagne de phishing visant des cabinets juridiques et des sociétés d'assurance en Amérique du Nord. Il semble que des efforts supplémentaires seront nécessaires à l'avenir pour se débarrasser définitivement de Trickbot.

Lorsqu'il s'agit de protéger votre entreprise contre les attaques de ransomwares par email, la première ligne de défense consiste à filtrer tous les emails entrants pour détecter le spam et les tentatives de phishing. Il y avait plusieurs bonnes raisons de le faire avant même que la messagerie ne devienne un vecteur de

transmission de ransomwares, et de nombreuses entreprises ont déjà mis en place un système de filtrage du spam et de détection du phishing.

Vous pouvez aller plus loin et bloquer tous les types de pièces jointes que votre entreprise ne s'attend pas à recevoir par email. Toutefois, la pertinence de cette stratégie dépendra du type d'entreprise dans laquelle vous travaillez et peut impliquer de changer certaines habitudes de travail. Par exemple, si les collaborateurs ont l'habitude de s'envoyer des feuilles de calcul Excel et des documents Word par email, l'entreprise devra peut-être d'abord adopter une solution de partage de fichiers ou un cadre de collaboration sécurisé, et habituer le personnel à l'utiliser avant de pouvoir appliquer rigoureusement un filtrage plus strict des pièces jointes aux emails.

Assurez-vous que tous les terminaux utilisent un logiciel de protection des terminaux (EPP) de haute qualité qui empêchera les collaborateurs d'accéder à des pages web connues pour héberger des malwares. Vous pouvez également filtrer les contenus web, comme couche supplémentaire de protection. En plus de bloquer les sites web malveillants, ce filtrage peut empêcher les collaborateurs de consulter des sites web jugés inappropriés pour le travail.

Votre EPP doit être administré de manière centralisée afin d'appliquer les politiques de sécurité pertinentes, telles que limiter la possibilité de désactiver la protection des terminaux ou d'introduire des supports amovibles. Veillez à ce que tous les terminaux utilisent la dernière version du produit et qu'il récupère correctement les mises à jour. Si l'éditeur de votre EPP dispose d'un composant pour le Cloud, veillez à ce qu'il soit activé, car il permet de réagir encore plus rapidement aux nouvelles menaces. Le composant d'ESET pour le Cloud s'appelle LiveGrid®, et ESET Dynamic Threat Defense dans certains produits.

Des conseils de configuration contre les ransomwares sont disponibles ici pour les prestataires de services managés chargés du paramétrage des produits ESET déployés sur les réseaux des clients.

L'application rapide et complète de correctifs aux systèmes d'exploitation et aux applications contribuera à empêcher l'introduction de ransomwares par le biais de pièces jointes à des emails ou de téléchargements automatiques. Une configuration sécurisée peut également être utile. Par exemple, envisagez d'utiliser la politique de groupe pour désactiver complètement les macros de Microsoft Office. Cela limitera la surface d'attaque pour les ransomwares, bien que cela ne soit pas toujours possible si le flux de travail de l'entreprise repose sur des macros.

De nos jours, il ne fait aucun doute que la sécurité est une responsabilité partagée. Veillez donc à ce que la formation de vos collaborateurs à la cybersécurité soit à jour et reflète les dernières tendances des menaces. Comme indiqué dans la formation de sensibilisation gratuite d'ESET à la cybersécurité : « Vous pouvez réduire le nombre d'incidents de malwares auxquels votre entreprise doit faire face en précisant aux collaborateurs ce à quoi ils doivent faire attention en matière de phishing et autres contenus malveillants. »

Faites comprendre aux employés qu'ils doivent immédiatement signaler les pièces jointes et les messages suspects au service d'assistance ou à l'équipe de sécurité. Outre la possibilité de prévenir ou de limiter les dommages, des alertes précoces peuvent aider l'entreprise à ajuster le filtrage du spam et des contenus, et renforcer ses pare-feux et autres défenses.

RANSOMWARES VIA DES CHAÎNES D'APPROVISIONNEMENT

La chaîne d'approvisionnement logicielle est un vecteur d'attaque de ransomwares qui mérite une attention particulière ces derniers temps. De même que les ransomwares remontent au siècle dernier, les risques liés à la chaîne d'approvisionnement logicielle le sont tout autant. À l'époque où les disquettes étaient le principal vecteur d'attaque des virus informatiques et le principal moyen d'acquérir des logiciels, des malwares se retrouvaient parfois sur les disquettes de produits commerciaux ou de versions d'évaluation distribuées avec des magazines informatiques.

En 2017, ESET a découvert qu'un logiciel de comptabilité légitime était utilisé par des criminels pour propager le malware NotPetya/DiskCoder.C. Les attaquants ont pénétré dans les serveurs de mise à jour de l'éditeur et ont ajouté leur propre code aux fichiers de mise à jour des applications légitimes. Lorsque les utilisateurs du logiciel de comptabilité installaient les mises à jour du programme, ils installaient également une porte dérobée conduisant à ce qui est devenu la cyberattaque la plus dévastatrice de l'histoire. La première ligne de défense contre ce type d'attaque est un bon produit de protection des terminaux, complété par des outils d'EDR.

Ainsi, en raison de la complexité des impacts que ces attaques peuvent déclencher et des mesures d'atténuation ensuite requises, les chercheurs et les administrateurs de sécurité sont à l'affût. Le 2 juillet 2021, une série d'événements se sont produits avec le logiciel d'administration informatique de Kaseya pour les MSP, qui portait toutes les caractéristiques d'une attaque de ransomwares contre une chaîne d'approvisionnement à l'aide du cheval de Troie Win32/Filecoder.Sodinokibi.N. Une enquête ultérieure a montré que l'incident reposait sur l'exploitation d'une vulnérabilité zero-day, mais son implication dans une chaîne d'approvisionnement a suscité une réaction rapide. Kaseya, pour sa part, s'est empressé de catégoriser l'incident et d'envoyer des notifications aux personnes potentiellement concernées, en leur conseillant de fermer immédiatement les serveurs VSA sur site.

L'intensité croissante des attaques sur des chaînes d'approvisionnement est également clairement illustrée par le nombre d'articles d'ESET décrivant l'utilisation de ce vecteur d'attaque. Entre novembre 2020 et février 2021, quatre cas d'attaques sur des chaînes d'approvisionnement ont été découverts exclusivement par ESET, soit un nombre très élevé par rapport aux années précédentes.

Pour se défendre contre ce type d'attaque, il convient d'appliquer des correctifs, d'utiliser un logiciel de protection des terminaux et une solutions d'EDR, et de sensibiliser les utilisateurs aux emails non sollicités qui les incitent à consulter des sites web inconnus.

RANSOMWARES VIA DES EXPLOITATIONS DE VULNÉRABILITÉS

Si les cybercriminels peuvent tirer profit des vulnérabilités connues et inconnues, l'obtention de vulnérabilités zero-day appartient généralement au monde des groupes de pirates et des acteurs parrainés par des États. Malgré la menace de ces zero days, les vulnérabilités connues donnent plus qu'assez de maux de tête aux administrateurs de la sécurité, aux chercheurs et aux propriétaires d'entreprises.

Ainsi, presque tous les éditeurs de produits de cybersécurité détectent encore la vulnérabilité EternalBlue de 2017 et ses nombreuses variantes, ainsi que la vulnérabilité du protocole de partage de fichiers SMBv1 de Microsoft. La longue durée de vie des vulnérabilités et des menaces comme WannaCryptor (alias WannaCry) est généralement due à une mauvaise gestion des mises à jour et des correctifs dans les entreprises et les institutions.

La complexité croissante du paysage des menaces a par ailleurs donné naissance à de nouveaux outils permettant de lutter contre des menaces plus modernes, mais ceux-ci s'accompagnent également d'exigences techniques supplémentaires, à savoir la recherche des vulnérabilités des produits et la gestion rigoureuse des correctifs.

L'augmentation considérable de l'utilisation des VPN à des fins professionnelles et personnelles est remarquable. Deux cas de vulnérabilités viennent ici à l'esprit, identifiées dans les services de VPN de Pulse Secure et de Fortinet, qui ont permis la prolifération de ransomwares parmi les clients. L'utilisation du VPN dans les grandes institutions et les entreprises, bien que très efficace, ajoute une responsabilité supplémentaire de mise à jour du produit selon les besoins. Ces mises à jour en temps opportun devraient être secondées par l'utilisation de l'authentification multifacteur lors de la connexion aux services VPN. En cas de soupçon de détournement d'identifiants, les entreprises doivent procéder à une réinitialisation complète des comptes.

Ces défis trouvent également un écho dans la recrudescence mondiale de l'utilisation des grandes plateformes de productivité et de collaboration. En mars 2021, une frénésie d'activité a éclaté parmi les pirates, les principaux éditeurs de logiciels et l'ensemble du secteur de la cybersécurité lorsque Microsoft a publié en urgence des mises à jour pour corriger quatre failles zero-day affectant les versions 2013, 2016 et 2019 de Microsoft Exchange Server. Des pirates ont par la suite exploité ces vulnérabilités pour accéder à des serveurs Exchange et voler des emails, télécharger des données et compromettre des machines avec des malwares pour un accès à long terme aux réseaux des victimes.

Cet événement de grande ampleur a finalement permis à au moins 10 groupes de pirates d'assiéger des serveurs Exchange. Les chercheurs d'ESET ont rapidement cherché à déterminer si les entreprises ont été sondées et infiltrées pour de futures attaques, y compris par des ransomwares. Le mécanisme probable ? En prenant pied sur un serveur Microsoft Exchange, les attaquants disposent d'un accès très privilégié à une entreprise, éventuellement même des droits d'administrateur, et peuvent ensuite planifier une future attaque.

Comme nous l'avons déjà mentionné dans la section sur les attaques contre la chaîne d'approvisionnement ci-dessus, l'attaque de ransomware Kaseya VSA a touché plus de 50 MSP, impactant plus de 1 000 clients finaux. Les pirates ont utilisé un certain nombre de vulnérabilités zero-day, dont CVE-2021-30116, pour compromettre le logiciel de gestion informatique Kaseya VSA, un outil prisé par les MSP. Ils ont affirmé avoir touché plus d'un million de systèmes, ce qui pourrait être exagéré. La télémétrie d'ESET a révélé la présence de victimes dans 17 pays, dont le Royaume-Uni, l'Afrique du Sud, le Canada, l'Allemagne et les États-Unis.

Même si les premières indications d'une attaque sur une chaîne d'approvisionnement n'ont pas été confirmées, une attaque zero-day de ce type est très grave et a effectivement produit des effets sur la chaîne d'approvisionnement en aval. En raison de la popularité des systèmes Kaseya, des impacts ont été enregistrés sur des entreprises n'ayant qu'un lien indirect avec la plateforme VSA pour MSP. Le 2 juillet, la chaîne de supermarchés scandinave Coop a pris des mesures pour fermer environ 500 magasins car son prestataire de traitement des paiements et fournisseur de ses systèmes de point de vente reposait sur des systèmes hébergés par Kaseya. Donc bien que Coop n'ait pas été directement touchée, elle l'a été de manière significative en raison de sa dépendance à un autre service qui a été interrompu à cause de l'attaque de Kaseya.

Les administrateurs informatiques, les responsables de la sécurité des systèmes d'information et les cadres supérieurs devraient avoir pris note de l'ampleur et de l'impact des incidents de Microsoft Exchange et de Kaseya, afin de se concentrer à nouveau sur l'environnement des menaces et l'impact que peuvent avoir les ransomwares. Pour en savoir plus sur certaines des vulnérabilités les plus fréquemment mentionnées :

- Kaseya VSA
- Pulse Connect Secure
- Hyperviseur Citrix
- VPN Fortinet
- Microsoft Exchange Server - Voir l'article dans la dernière édition de notre rapport sur les menaces.
- Passerelle et contrôleur de mise en production d'applications Citrix
- Contrôles communs de Microsoft Office
- Windows Win32k
- Appliance de transfert de fichiers Accellion

CLOUDS ET SEGMENTS

Quel que soit le vecteur d'attaque utilisé par les ransomwares, s'ils pénètrent dans votre entreprise, il y a de fortes chances qu'ils essaient de se propager sur le plus grand nombre de machines possible, ce qui pourrait avoir un impact sur l'ensemble des activités de votre entreprise. Il est clair que le fait de limiter le nombre de machines qu'un attaquant peut atteindre à partir d'un seul point d'entrée présente des avantages importants en tant que stratégie défensive. Il existe plusieurs approches pour mettre en œuvre une telle stratégie, notamment la segmentation du réseau.

Une discussion sur l'architecture du réseau dépasse du cadre de ce document, et la conversion d'un réseau « à plat » facile à traverser en un réseau segmenté peut être à la fois difficile et coûteuse (ce rapport KPMG fournit une perspective utile). Cependant, chaque entreprise doit comprendre les forces et les faiblesses de son architecture réseau actuelle du point de vue de la sécurité. Un simple audit effectué à partir d'entretiens peut améliorer cette compréhension en posant la question suivante : « Puis-je aller d'ici à là ? » ou « Qu'est-ce qui empêche quelqu'un d'aller d'ici à là ? »

Ces dernières années, la migration des données vers le Cloud était une stratégie d'architecture système répandue, mais celle-ci n'offre pas d'immunité automatique contre les attaques de ransomwares (malgré les efforts déployés par des prestataires peu scrupuleux pour donner l'impression que Cloud = sécurité). En fait, le faible coût et la facilité relative avec laquelle de nouveaux serveurs peuvent être provisionnés dans le Cloud et connectés au reste de l'infrastructure de l'entreprise ont fait du Cloud un terrain de chasse fertile pour les criminels. Il est clair que toute utilisation du Cloud par une partie quelconque de l'entreprise doit être correctement autorisée et configurée pour maximiser la sécurité. Comme tous les autres systèmes, ceux du Cloud doivent être intégrés aux processus de sauvegarde et de récupération appropriés.

CORRECTIFS ET SAUVEGARDES : DÉFENSE CONTRE LES RANSOMWARES

La mise à jour et la sauvegarde sont deux aspects de l'exploitation et de l'administration des systèmes qui jouent un rôle essentiel dans la défense contre une attaque de ransomware. L'application de correctifs aux systèmes ferme les voies d'attaque potentielles et peut empêcher les ransomwares de pénétrer dans votre entreprise, ou peut réduire les dommages s'ils sont parvenus à y pénétrer.

Bien sûr, comme tout administrateur système le sait, l'application de correctifs peut être beaucoup plus compliquée qu'il n'y paraît. Les correctifs et les mises à jour doivent être testés avant d'être déployés. La mise à jour vers la dernière version d'une application ou d'un système d'exploitation peut entraîner le dysfonctionnement de certains systèmes qui en dépendent. Cependant, le coût élevé de l'entrée d'un ransomware dans votre réseau justifie l'effort à fournir pour relever ces défis et appliquer rapidement des correctifs pour bloquer les ransomwares.

On dit souvent que si un ransomware pénètre dans votre entreprise, que ce soit via RDP, un email, la chaîne d'approvisionnement logicielle ou un collaborateur malintentionné, un processus de sauvegarde et de récupération complet et correctement géré constitue un mécanisme de défense essentiel qui est crucial pour vos efforts de rétablissement.

C'est plutôt vrai dans l'ensemble, et il existe beaucoup de bonnes raisons de disposer d'un tel processus. Mais n'oubliez pas que certaines attaques de ransomwares sont menées sur une certaine période, au cours de laquelle le ransomware peut également faire partie des sauvegardes, ce qui compromet la possibilité d'une récupération sans heurts. C'est pourquoi la sauvegarde n'est pas un moyen de défense que vous devez mettre en place puis l'oublier. Elle doit être supervisée, et le processus de récupération doit être régulièrement testé.

De nos jours, il existe plus d'options que jamais pour la sauvegarde et la récupération, notamment le stockage dans le Cloud, qu'il soit à distance, sur site ou hybride. Il existe également plus de données à sauvegarder, provenant de plusieurs sources. À moins que vous ne disposiez d'une stratégie de sauvegarde

complète, il y a toujours une chance que les opérateurs de ransomwares trouvent le seul appareil que vous n'avez pas sauvegardé.

Selon les experts en sauvegarde de Xopero, membre de l'Alliance technologique ESET, la sauvegarde complète comprend les données et l'état du système de tous les terminaux, serveurs, boîtes de messagerie, lecteurs réseau, appareils mobiles et machines virtuelles.

Une discussion détaillée sur la stratégie de sauvegarde et de récupération des données de l'entreprise dépasse du cadre de ce livre blanc, mais il est clair qu'il est plus important que jamais de disposer d'une telle stratégie. Les ransomwares ne font que s'ajouter à la longue liste des raisons pour lesquelles votre entreprise ne doit pas lésiner sur cet aspect des responsabilités du département informatique. Il existe toutefois des mises en garde spécifiques aux ransomwares. Par exemple, lorsque le stockage est « actif en permanence », son contenu peut être vulnérable à un ransomware, de la même manière que le stockage local ou connecté à un réseau.

Pour éviter que les ransomwares ne l'atteigne, optez pour un stockage hors site qui :

- n'est pas en ligne de façon régulière et permanente
- protège les données sauvegardées contre la modification ou l'écrasement automatique et silencieux par des malwares lorsqu'il est en ligne
- protège les sauvegardes antérieures, de sorte que même si une catastrophe frappe les toutes dernières sauvegardes, vous pouvez au moins récupérer certaines données, y compris les versions antérieures des données actuelles
- protège le client en précisant les responsabilités légales/contractuelles du prestataire, ce qui se passe s'il fait faillite, etc.

Ne sous-estimez pas non plus l'utilité des supports en écriture unique pour l'archivage des données. Les fichiers stockés sur des supports qui ne sont pas réinscriptibles sont à l'abri des prédations des ransomwares.

Bien sûr, il existe de nombreuses autres raisons pour lesquelles votre entreprise a besoin d'un processus de sauvegarde et de récupération, notamment le rétablissement après un incendie, une inondation, une tempête, etc.

RÉPONSE À UNE ATTAQUE DE RANSOMWARE

En plus d'ériger des défenses contre les ransomwares, chaque entreprise doit être prête à répondre à toute attaque qui réussit à pénétrer ces défenses. Afin de s'y préparer, il est essentiel que les politiques de sécurité de l'entreprise soient mises à jour pour couvrir les ransomwares. Vous devez préciser comment les collaborateurs à tous les niveaux doivent réagir aux demandes des ransomwares. Veillez à ce que vos politiques répondent à ces questions :

- À qui les collaborateurs doivent-ils signaler les ransomwares ?
- Quelle est la politique de l'entreprise en matière de paiement des demandes de rançon ?
- Qui est autorisé à payer/négocier les rançons ? Les politiques doivent être élaborées de manière à éviter les problèmes suivants :
  - Les collaborateurs ne signalent pas les ransomwares par crainte de représailles.
  - Les administrateurs réseau paient les rançons parce que c'est plus facile que de récupérer des systèmes à partir de sauvegardes.
  - Communication non autorisée d'informations sur des attaques réelles ou présumées de ransomwares.
- Quelles mesures l'entreprise est-elle tenue de prendre en cas d'atteinte à la sécurité des données ?
- Quelle est la politique de l'entreprise concernant l'extinction des machines concernées ? Qui prend cette décision ? L'extinction des machines élimine des preuves potentielles stockées dans leur mémoire, et peut être considérée comme étant une infraction de la réglementation.

Après avoir mis à jour vos politiques de sécurité de l'information pour tenir compte des ransomwares, vous devez vous assurer que vos programmes de sensibilisation à la sécurité et de formation des collaborateurs incluent un contenu approprié sur les ransomwares.

Vous devrez également vous assurer que vos plans de reprise après sinistre, de traitement des incidents/de réponse aux crises sont prêts en cas d'attaque de ransomware. Voici un aperçu des points que votre plan d'intervention doit couvrir :

- Aux premiers signes d'une attaque, prévenir le personnel désigné
- Isoler et analyser les machines affectées
- Extinction : S'il n'est pas possible d'isoler les machines touchées, sauvegardez une image du système et le contenu de la mémoire, puis mettez-les hors tension pour éviter que l'attaque de ransomware ne se propage davantage
- Une fois l'attaque confirmée, déclenchez l'intervention de vos équipes spécialisées
- Alertez le conseiller juridique
- Contactez les prestataires qui peuvent être en mesure de fournir une assistance
- Rappelez aux collaborateurs la politique de communication avec la presse et les réseaux sociaux
- Évaluez la portée de l'attaque et les spécificités du ransomware (par exemple si une clé de déchiffrement est disponible)
- Contactez les services de police
- Préparez une déclaration à l'avance
- Si les fichiers ont été chiffrés, déterminez s'ils peuvent être restaurés à partir de la sauvegarde
- Tenez les collaborateurs au courant de la situation
- Au besoin, activez votre plan de continuité des activités
- Collectez les journaux pertinents et les indicateurs possibles de compromis, tels que les binaires, les notes de demande de rançon, les adresses IP, les entrées de la base de registre ou d'autres fichiers
- Documentez l'enquête initiale sur l'attaque et les mesures prises pour y remédier

Il est bon d'avoir au moins un scénario applicable aux ransomwares dans votre manuel de planification de crise, et de le réviser dans un exercice avec le personnel concerné, y compris les dirigeants. Cela peut révéler des manques dans les plans de sauvegarde et de récupération, et vous aider à anticiper l'impact de l'impossibilité d'accéder aux services de base en raison du chiffrement des systèmes (notamment les services de messagerie, de téléphonie VoIP et d'accès à Internet).

DÉTECTION ET TRAITEMENT SUR LES TERMINAUX

Il existe une catégorie de logiciels de sécurité qui peut contribuer à limiter l'impact des attaques de ransomwares : les outils de détection et de traitement pour terminaux, ou EDR pour faire court. Qu'il s'agisse d'un ensemble d'outils développés en interne ou d'un produit de sécurité intégré, l'EDR peut faciliter les efforts manuels de détection des menaces sur vos réseaux et automatiser un large éventail de mesures défensives.

Dans la Figure 6, vous pouvez voir plusieurs règles d'EDR associées aux ransomwares, conçues pour alerter le personnel de sécurité en cas d'activité suspecte (cette solution d'EDR particulière est ESET Enterprise Inspector).

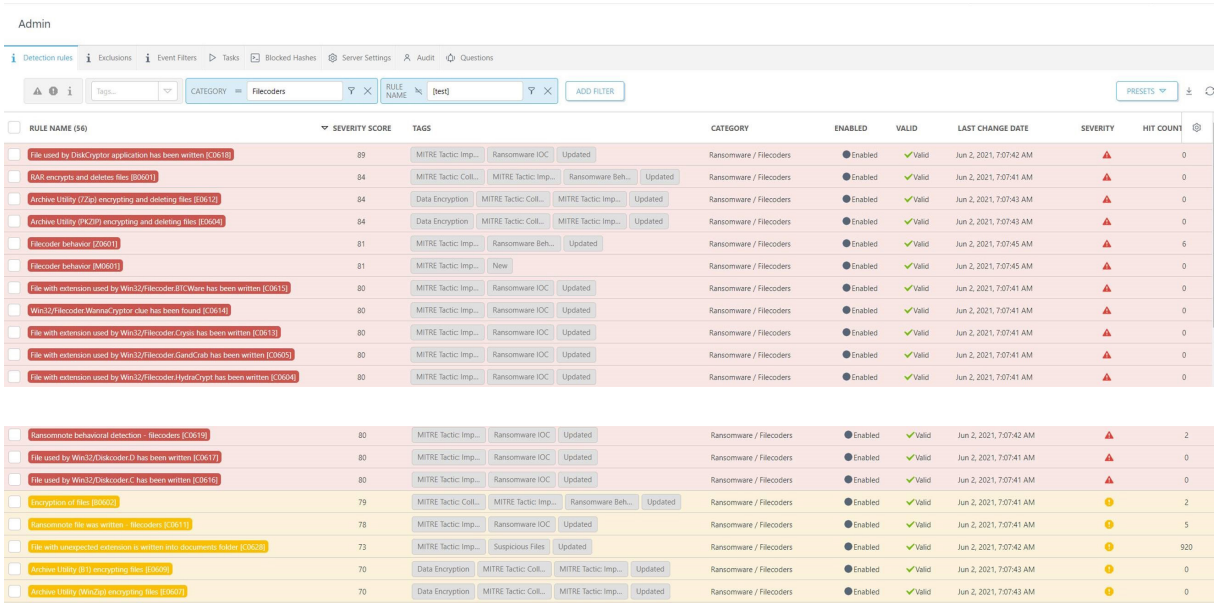

Figure 6 // Tableau de bord d'ESET Enterprise Inspector avec des règles relatives aux ransomwares

Un outil d'EDR est en mesure de surveiller tous les terminaux de votre entreprise pour détecter toute activité anormale et suspecte, comme le changement d'extension des fichiers, généralement observée lors d'une attaque de ransomware. Votre équipe de sécurité aimerait certainement être alertée de la présence d'outils d'attaque tels que Mimikatz, créés pour voler les identifiants des utilisateurs dans la mémoire, ou Cobalt Strike Beacon, souvent utilisé par les attaquants pour s'implanter dans un système et exécuter des commandes à distance.

Les signes précurseurs d'une intrusion peuvent être programmés dans des règles et des alarmes. Ils peuvent être continuellement affinés à l'aide de données fraîches provenant de sources de renseignements sur les menaces, telles que les listes d'indicateurs de compromis (IoC). Un bon système de détection des intrusions comporte des règles qui permettent à l'opérateur de trouver les systèmes compromis dès qu'une règle est déclenchée, d'isoler ces systèmes, puis de diagnostiquer le problème, y compris de revenir en arrière dans l'historique des commandes exécutées par les systèmes concernés. Grâce à ces fonctionnalités, le système d'EDR peut accroître la capacité de votre équipe de sécurité à déjouer des attaques, ou effectuer des analyses après une attaque.

UN MOT SUR LE PAIEMENT DE RANÇON

Et ce mot est : jamais. Pourquoi ? Parce que payer le criminel qui a chiffré vos fichiers signifie que :

- Vous validez le modèle économique du crime
- Vous encouragez la poursuite des activités criminelles
- Vous permettez aux cybercriminels de rechercher des vulnérabilités zero-day et de les exploiter
- Vous risquez de subir de nouvelles attaques et de nouvelles demandes de rançon

Payer les criminels qui ont chiffré vos fichiers ne garantit en aucun cas que vous obtiendrez la clé de déchiffrement. Même en payant, vous pourriez ne pas pouvoir récupérer vos fichiers pour de nombreuses raisons :

- Certaines données peuvent avoir été corrompues pendant le chiffrement et ne sont donc pas récupérables
- L'outil de déchiffrement fourni peut être associé à d'autres malwares, ne fonctionne pas correctement ou est beaucoup plus lent que la récupération à partir de sauvegardes
- Le processus de remise de la clé de déchiffrement peut échouer de plusieurs façons
- L'attaquant est de mauvaise foi et n'a aucune intention de fournir de clé de déchiffrement

Ce qui précède devrait suffire à dissuader les entreprises d'obtempérer aux demandes de rançon, mais pour bien souligner ce conseil, voici ce que préconise le FBI à propos du paiement : « Payer une rançon ne garantit pas à une entreprise qu'elle récupérera ses données. Nous avons vu des cas où des entreprises n'ont jamais obtenu de clé de déchiffrement après avoir payé la rançon. Le paiement d'une rançon non seulement enhardit les cybercriminels à cibler davantage d'entreprises, mais incite également d'autres criminels à s'engager dans ce type d'activité illégale. Enfin, en payant une rançon, une entreprise peut involontairement financer d'autres activités criminelles. »

En pratique, il semble y avoir deux arguments en faveur du paiement d'une rançon, le premier étant « nous ne pouvons pas restaurer les informations chiffrées à partir des sauvegardes. » Cela peut être dû au fait que les sauvegardes n'existent pas, ou qu'elles existent mais sont incomplètes ou endommagées d'une manière ou d'une autre. Il peut y avoir des alternatives au paiement. Avant de décider d'envoyer l'argent, vérifiez auprès de l'éditeur de votre solution de sécurité (a) s'il s'agit de l'une des rares situations où un outil de déchiffrement est disponible, et donc que la récupération est possible sans payer la rançon, et (b) s'il s'agit d'un cas connu où le paiement de la rançon ne permettra pas la récupération de cette variante particulière de ransomware.

Le deuxième argument courant est que « c'est moins cher que de restaurer à partir des sauvegardes. » Si cette affirmation se fonde uniquement sur des calculs de temps et de main-d'œuvre, elle peut être techniquement correcte, mais la décision de payer est néanmoins profondément erronée pour les raisons mentionnées précédemment, notamment le manque de fiabilité des promesses de déchiffrement, la probabilité d'être à nouveau attaqué après le premier paiement, et le fait que vous soutenez une activité criminelle et que vous rendez ainsi plus probables d'autres attaques contre d'autres personnes.

Vous avez peut-être entendu dire que certains opérateurs de ransomwares offrent aux victimes la preuve que le déchiffrement fonctionne. Cela arrive, ou peut également entraîner d'autres problèmes. Supposons que les agresseurs vous demandent de leur envoyer un fichier chiffré qu'ils déchiffrent ensuite et vous le renvoient comme preuve de leur bonne foi ; vous venez de faciliter la divulgation du contenu de ce fichier à des personnes de moralité douteuse et, si ces données contiennent des informations permettant d'identifier une personne, vous avez probablement commis une infraction à une ou plusieurs des législations sur la protection de la vie privée.

N'oubliez pas non plus que la suppression d'un ransomware actif à l'aide d'un logiciel de sécurité n'équivaut en aucun cas à la récupération des données. Si vous supprimez le ransomware et décidez ensuite de payer, il se peut que les données ne soient plus récupérables, même avec la coopération des criminels, car le mécanisme de déchiffrement fait souvent partie du malware. En d'autres termes, si vous décidez de payer, procédez avec prudence.

L'AVENIR DES RANSOMWARES

Exiger de l'argent pour rétablir l'accès aux systèmes et aux données vise spécifiquement leur disponibilité. Par essence, les ransomwares tirent parti de la dépendance d'une entreprise à l'égard de la technologie. Ainsi, plus les entreprises en viennent à dépendre de la technologie, plus le champ d'action des ransomwares s'agrandit. Cela signifie que nous pouvons nous attendre à ce que les ransomwares persistent et évoluent à l'avenir (à moins de changements imprévus dans la politique et l'économie mondiales).

D'après notre expérience des malwares depuis la fin des années 1980, nous pouvons affirmer que ce type de menace a tendance à évoluer ainsi :

- les vulnérabilités d'une nouvelle technologie sont découvertes et la possibilité de les détourner à des fins criminelles est évoquée
- les efforts pour remédier à ces vulnérabilités et les atténuer sont mis en œuvre
- les tentatives de détournement criminel des toutes dernières technologies sont d'abord rares, car les criminels gagnent facilement de l'argent avec des stratégies établies
- en l'absence de détournement criminel généralisé, les efforts de remédiation et d'atténuation s'essoufflent
- les criminels finissent par découvrir que cette « nouvelle » technologie est prête à être exploitée
- une nouvelle tendance émerge en matière de malwares

Les attaques de déni de service distribué qui exploitent les équipements de surveillance connectés à Internet (Mirai) et l'émergence de malwares ciblant les routeurs (VPNFilter) en sont des exemples. En ce qui concerne les ransomwares, la croissance explosive du nombre d'objets connectés mal sécurisés crée un paysage fertile pour de futurs attaques, tout comme l'utilisation croissante de systèmes de contrôle industriel connectés à Internet, de bâtiments intelligents et de véhicules, y compris les véhicules autonomes (voir l'article « RoT: Ransomware of Things » et le webinaire « Ransomware from the Dark Side »).

Plusieurs scénarios sont plausibles lorsqu'une baisse des revenus tirés de cybercrimes plus établis incite les criminels à se lancer dans de nouveaux projets. Les malwares installés sur les routeurs peuvent potentiellement limiter ou bloquer le trafic jusqu'à ce qu'un droit de péage soit payé, en menaçant de planter le routeur ou de révéler le contenu du trafic si vous essayez de supprimer le malware.

Le verrouillage à distance des véhicules, des maisons et des bâtiments pourrait être utilisé à des fins d'extorsion. La manipulation des systèmes d'automatisation des bâtiments, qui peuvent contrôler l'accès, le chauffage, la ventilation et la climatisation, pourrait servir de base à des extorsions, et nous en voyons déjà les signes. Quant aux robots commerciaux, la faisabilité d'attaques de ransomwares les ciblant a déjà été démontrée.

Ces scénarios de ransomware en constante évolution ont de multiples implications pour les entreprises. Les réponses suivantes sont recommandées :

- Commencez à tenir compte de ces menaces potentielles dans votre stratégie de gestion des risques et sa planification
- Commencez dès maintenant à vous occuper des ressources « susceptibles de faire l'objet d'une demande de rançon » : objets connectés, routeurs, robots, systèmes de contrôle, systèmes autonomes
- Tenez-vous au courant des vulnérabilités les concernant
- Tenez-vous au courant des correctifs et des mises à jour de leur microprogrammes
- Séparez les objets connectés et autres nouvelles technologies des réseaux de production

CONCLUSION

Les données, les techniques et les cas concrets présentés dans ce document montrent que les ransomwares sont vraiment devenus la cybermenace actuelle. Son essor peut être largement attribué au développement de la technique de la double extorsion (ou doxing), inaugurée en 2019 par le défunt groupe Maze. En plus de chiffrer les appareils de leurs victimes, les opérateurs de ce ransomware ont également volé les données les plus précieuses et les plus sensibles de leurs victimes, et ont menacé de les publier.

D'autres acteurs malveillants n'ont pas tardé à leur emboîter le pas, s'appuyant sur cette méthode efficace de double extorsion. De nouvelles méthodes ont été introduites, ciblant non seulement les données des victimes, mais également leurs sites web, leurs collaborateurs, leurs partenaires commerciaux et leurs clients, augmentant ainsi la pression et donc la dispositions à payer.

Profitant du chaos et de l'insécurité de la pandémie, les cybercriminels ont également commencé à forcer l'accès via RDP, pour finalement en faire l'un de leurs principaux moyens d'attaque. Les campagnes de spam diffusant des macros malveillantes, des liens dangereux et des binaires de botnets n'ont pas disparu pour autant disparues. Elles continuent de bombarder les victimes potentielles en plus des milliards d'attaques cherchant à deviner des mots de passe.

En raison de l'efficacité accrue des techniques d'extorsion et des nouveaux canaux de distribution, on estime que des centaines de millions de dollars ont fini sur les comptes de ces cybercriminels techniquement compétents, ce qui leur a permis de développer leur modèle commercial de ransomware sous forme de services et de recruter de nombreux nouveaux affiliés. N'ayant plus à faire le « sale boulot », certains gangs ont commencé à acquérir des vulnérabilités zero-day et acheter des identifiants volés, élargissant ainsi le nombre de victimes potentielles.

Le nombre croissant d'incidents de ransomwares indirectement liés à des attaques contre des chaînes d'approvisionnement représente une autre tendance inquiétante qui pourrait indiquer la direction que prendront ces gangs.

L'argent et l'ambition étant principalement du côté des gangs de ransomwares, tirer des enseignements des attaques et des analyses publiées quotidiennement dans les médias est devenu une nécessité pour tout professionnel de l'informatique et de la sécurité. Il a été démontré à maintes reprises depuis le début de 2020 que l'application de politiques de sécurité, une configuration adéquate et des mots de passe forts combinés à une authentification multifacteur peuvent être les éléments décisifs dans la lutte contre les ransomwares. Bon nombre des incidents cités dans ce document soulignent également l'importance de l'application rapide de correctifs, car les vulnérabilités connues font partie des vecteurs privilégiés de ces gangs.

Pour contrer les vulnérabilités zero-day, les botnets, le spam et d'autres techniques plus avancées, des technologies de sécurité supplémentaires sont nécessaires : une solution de protection multicouche sur les terminaux, capable de détecter et de bloquer les menaces entrantes dans les emails, les liens, RDP et d'autres protocoles réseau, ainsi que des outils de détection et de traitement sur les terminaux pour surveiller, identifier et isoler les anomalies et les signes d'activité malveillante dans l'environnement d'une entreprise.

Les nouvelles technologies, tout en apportant des avantages à la société, constituent également un champ d'opportunités toujours plus vaste pour les cybercriminels. Nous espérons qu'en expliquant à quel point la menace que représentent les ransomwares est grave, et en décrivant les moyens de s'en défendre, le présent document contribuera à concrétiser ces avantages tout en réduisant les pertes causées par les cybercriminels.

À PROPOS D'ESET

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique de pointe pour protéger les entreprises, les infrastructures critiques et les consommateurs du monde entier contre des menaces digitales de plus en plus sophistiquées. Protection des terminaux et des mobiles, détection et traitement des incidents, chiffrement et authentification multifacteur… les solutions performantes et faciles à utiliser d'ESET protègent et supervisent discrètement 24 heures sur 24, 7 jours sur 7, en mettant à jour les défenses en temps réel pour assurer sans aucune interruption la sécurité des utilisateurs et le bon fonctionnement des entreprises. L'évolution des menaces exige d'une entreprise de sécurité informatique qu'elle évolue également. C'est le cas d'ESET grâce à ses centres de R&D dans le monde entier travaillant à la protection de notre avenir commun. Pour plus d'informations, consultez www.eset.com ou suivez-nous sur LinkedIn, Facebook et Twitter.

ENJOY SAFER TECHNOLOGY™