RANSOMWARES

Conseils de sécurité pour les PME

Digital Security
Guide

ESET
Digital Security
Progress. Protected.

TABLE DES MATIÈRES

INTRODUCTION

LE NOMBRE DE RANSOMWARES EST EN HAUSSE

Ces dernières années, les groupes de cybercriminels qui exploitent des ransomwares sous forme de services ont en effet développé une approche différente et plus ciblée de ce type d'attaques, dont le volume est beaucoup plus difficile à mesurer.

Les cybercriminels sont de plus en plus agressifs et s'efforcent de découvrir la moindre faiblesse dans vos systèmes de sécurité informatique, en s'attaquant aux bases de données, aux serveurs web et aux smartphones. Les attaques par force brute contre le protocole d'accès à distance RDP ou les attaques DDoS contre le site web d'une entreprise ne sont qu'une infime partie de ce qui se passe actuellement.

LES RANSOMWARES COMME MENACE SUR LES PETITES ET MOYENNES ENTREPRISES

Les PME deviennent de plus en plus des cibles attrayantes pour les attaques de ransomwares. Pourquoi ? Ces entreprises accumulent en effet des données plus précieuses que les consommateurs, et ne disposent pas des mesures de sécurité robustes employées par les grandes entreprises ou institutions.

Ces facteurs constituent une situation idéale pour les cybercriminels et augmentent le risque d'attaques de ransomwares.

Comme les dirigeants de PME ne considèrent souvent pas leur entreprise comme une cible potentielle, les données vitales ne sont pas régulièrement sauvegardées et l'entreprise est ainsi moins bien préparée aux attaques de ransomwares.

COMMENT FONCTIONNENT-ILS TECHNIQUEMENT ?

Une attaque de ransomware peut être définie comme une tentative d'extorsion d'argent, en empêchant une entreprise d'accéder à ses données.

Il ne faut pas longtemps pour réaliser que vous êtes devenu une victime. Les ransomwares vous informent généralement peu après avoir infecté vos appareils, en affichant une note de rançon sur votre écran, en ajoutant un fichier texte aux dossiers touchés ou en modifiant l'extension des fichiers chiffrés.

Types de ransomwares

Ransomwares de verrouillage d'écran

Ils bloquent l'accès à votre appareil en verrouillant son écran, et vous ne pouvez utiliser que l'interface utilisateur du malware.

Ransomwares de verrouillage par PIN

Ils modifient le code PIN de votre appareil, rendant son contenu et ses fonctionnalités inaccessibles.

Ransomwares de chiffrement de disques

Ils chiffrent le MBR (zone d'amorçage) et/ou les structures critiques du système de fichiers, vous empêchant d'accéder à votre système d'exploitation.

Ransomwares de chiffrement de fichiers

Ils chiffrent les fichiers de votre disque.

COMMENT FONCTIONNENT-ILS TECHNIQUEMENT ?

Le champ d'action des ransomwares s'est élargi tout au long de la pandémie de COVID-19. Les confinements répétés ont entraîné une augmentation du nombre d'emails d'hameçonnage, ciblant principalement les collaborateurs qui ont commencé à télétravailler pour accéder aux systèmes et aux services internes des entreprises via le protocole d'accès à distance RDP, qui est devenu un vecteur très courant d'implantation de ransomwares.

Les cybercriminels qui utilisent des ransomwares sous forme de services (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 ou non un ransomware.

Les cybercriminels peuvent également mener des attaques contre des chaînes d'approvisionnement afin d'accéder à des écosystèmes informatiques entiers. 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 à grande échelle. Comme autre tendance, les dispositifs de stockage réseau (NAS), qui hébergent les données de différents utilisateurs et sont couramment utilisés pour partager des fichiers afin d'effectuer des sauvegardes, ont également attiré l'attention des gangs de ransomwares.

COMMENT FONCTIONNENT-ILS PSYCHOLOGIQUEMENT ?

Les opérateurs de ransomwares utilisent la pression comme principale tactique. Elle augmente à mesure que les individus ou les entreprises subissent des atteintes à leur réputation, des interruptions de leur activité, voire des sanctions juridiques et financières,

puis se termine inévitablement par des formes de manipulation. 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. Les approches suivantes ont pour objectif de choquer leurs victimes :

- Le bombardement d'impressions, qui consiste à ordonner à plusieurs imprimantes d'un réseau d'imprimer une note de rançon, menaçant ainsi la capacité de la direction à contrôler les communications internes et externes.
- L'accès aux données des clients d'une entreprise pour les contacter, voire les démarcher par téléphone ou même les menacer, a pour objectif d'humilier publiquement les victimes tandis que leurs services informatiques s'efforcent d'atténuer les effets de l'attaque.

PRESSION CROISSANTE SUR LES VICTIMES

Pour s'assurer de recevoir la somme qu'ils ont demandée, les cybercriminels multiplient souvent les méthodes d'extorsion.

Double extorsion

Elle combine chiffrement des données avec leur exfiltration. De cette manière, ils empêchent leurs victimes d'accéder à des fichiers critiques ou précieux, et les volent ou les vendent à d'autres acteurs malveillants. Une méthode appelée « doxing » consiste par exemple pour les cybercriminels à passer au peigne fin les systèmes de leurs victimes pour y découvrir des données sensibles, qu'ils menacent ensuite de divulguer, à moins qu'une somme supplémentaire ne soit versée en plus de la rançon.

COMMENT FONCTIONNENT-ILS PSYCHOLOGIQUEMENT ?

Triple extorsion

Certains opérateurs de ransomwares contactent les partenaires commerciaux ou les clients des victimes qui n'ont pas payé la rançon, pour les informer que leurs données sensibles ont été consultées dans le cadre de l'attaque de ransomware. Ils suggèrent ensuite que ces partenaires fassent pression sur l'entreprise victime pour qu'elle paie afin d'empêcher la divulgation de ces données, ou bien exigent le paiement directement auprès des partenaires.

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 leur meilleur intérêt. 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 fournisseurs de votre chaine d'approvisionnement.

La sécurité est une responsabilité partagée, c'est pourquoi la formation de vos collaborateurs à la cybersécurité doit être actualisée, et doit refléter les dernières tendances des cybermenaces. Dans notre livre blanc sur les ransomwares publié précédemment sur le Digital Security Guide, nous évoquions déjà quelques clés de compréhension essentielles pour se protéger : « Vous pouvez réduire le nombre d'incidents de malwares auxquels votre entreprise est confrontée en précisant aux collaborateurs ce à quoi ils doivent faire attention en matière d'hameçonnage et autres contenus malveillants. »

COMMENT FONCTIONNENT-ILS PSYCHOLOGIQUEMENT ?

Exemples de notes de rançon

Les disques durs de votre ordinateur ont été chiffrés avec un algorithme de chiffrement de haut niveau. Il n'y a aucun moyen de restaurer vos données sans une clé spéciale. Vous pouvez acheter cette clé sur la page du site indiquée à l'étape suivante
(Ransomware Petya)

Le système de sécurité de votre entreprise comportait une faille importante. Vous devriez être reconnaissant qu'elle ait été exploitée par des gens sérieux et non par des débutants. Ils auraient endommagé toutes vos données par erreur ou pour le plaisir.
(Ransomware LockerGoga)

Messieurs !

Votre entreprise est en grand danger. Le système de sécurité de votre entreprise comporte une brèche de taille. Nous nous sommes facilement introduits dans votre réseau. Personne ne peut vous aider à restaurer vos fichiers sans notre décodeur spécial.
(Ransomware Ryuk).

RANSOMWARES VS. INFRASTRUCTURE INFORMATIQUE

PROTOCOLE D'ACCÈS À DISTANCE RDP

Si vos collaborateurs ont besoin d'accéder à distance aux systèmes de votre entreprise, le protocole RDP doit être activé. Cela nécessite la mise en place d'un mandat critique, à la fois pour les collaborateurs et les administrateurs, obligeant à l'utilisation d'une authentification multifacteur (MFA) pour accéder à la plateforme. Après l'authentification, les collaborateurs peuvent se connecter en toute sécurité aux systèmes.

Infobox

Comment les entreprises peuvent-elles utiliser RDP ?

1) Pour gérer les programmes exécutés sur un serveur, par exemple un site web ou une base de données de back-end.

2) Pour permettre l'accès à distance à des postes de travail ou à des machines virtuelles capables d'accéder à leur tour à des ressources qui ne sont pas joignables 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.

RANSOMWARES VS. INFRASTRUCTURE INFORMATIQUE

Pourquoi la découverte des systèmes externes et leur détournement sont-ils aussi simples ?

- Les systèmes RDP vulnérables sont faciles à trouver (par ex. par des moteurs de recherche spécialisés comme Shodan)
- Des pirates peuvent facilement prendre pied sur des systèmes RDP mal configurés
- 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

7
milliards

Le nombre de détections du vecteur d'attaque RDP entre janvier 2020 et juin 2021 selon la télémétrie d'ESET.

Le nombre total de résultats pour le port RDP 3389 ouvert par défaut dans le moteur de recherche Shodan.io

Plus de
4 millions

Infographie

Tendance de détection des attaques par force brute contre RDP, moyenne sur 7 jours

Si l'augmentation la plus notable a eu lieu au premier semestre 2020, 2021 possède cependant 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 détections d'attaques par force brute contre RDP. De plus, les attaques via RDP peuvent échapper à de nombreuses méthodes de détection, ce qui signifie moins de mesures et moins de sensibilisation aux menaces.

RANSOMWARES VS. INFRASTRUCTURE INFORMATIQUE

COMMENT PROTÉGER VOTRE ENTREPRISE CONTRE LES ATTAQUES DE RANSOMWARES VIA RDP

- Mettez 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.
- Veillez 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.
- Dressez l'inventaire de vos ressources connectées à Internet. D'après nos études, le scénario suivant n'est pas si inhabituel : une entreprise est attaquée via une ressource connectée à Internet dont le personnel de sécurité n'a eu connaissance qu'après l'attaque.
- Ne permettez pas à un prestataire ou un collaborateur de connecter un serveur physique ou virtuel au réseau de l'entreprise et à Internet, à moins que ce serveur ne soit configuré de manière sécurisée. La configuration doit être effectuée avant la mise en service du serveur, en particulier s'il utilise RDP avec un compte d'administrateur de domaine.
- Précisez les ressources connectées à Internet pour lesquelles l'accès à distance est activé et décidez si cet accès est nécessaire. Si l'accès est vraiment essentiel, exigez des mots de passe longs pour les comptes qui auront cet accès, et déterminez s'il est possible de restreindre ces systèmes à un fonctionnement sur le réseau interne et d'y accéder à distance via une connexion VPN.
- Si un système doit être accessible depuis Internet via RDP, et que l'utilisation d'un VPN n'est pas possible, installez une authentification multifacteur (MFA), afin de ne pas dépendre uniquement des mots de passe. Veillez toutefois à utiliser une solution de MFA qui ne soit pas basée sur des SMS. Les criminels ont de nombreux moyens de déjouer l'authentification par SMS. Si vous ne pouvez utiliser que des mots de passe, 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.
- Durcissez et corrigez 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 aient été supprimés ou désactivés, et que les paramètres soient configurés pour maximiser la sécurité.

RANSOMWARES VS. INFRASTRUCTURE INFORMATIQUE

EMAIL

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 à un réseau d'entreprise. 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.

La messagerie est également 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.

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

Exemple

Un seul email suffit à rendre inutilisable la serrure électronique d'une porte de chambre d'hôtel

Les ransomwares ne se contentent pas de chiffrer les données de votre ordinateur. Le directeur général d'un hôtel quatre étoiles des Alpes autrichiennes a reçu un email comportant un ransomware se faisant passer pour une facture de Telekom Austria. Après avoir cliqué sur un lien dans l'email, les serrures électroniques des portes des chambres de son hôtel sont devenues inutilisables, et il n'a pas été en mesure de remettre de nouvelles clés à ses clients. Pour reprendre ses activités, il a décidé de payer la rançon de deux bitcoins.

Vous donnez aux criminels l'image d'une entreprise qui se conforme à payer une rançon. Compte tenu de ce contexte, il y a fort à parier que cet hôtel soit, malheureusement, à nouveau visé dans le futur par des attaques similaires.

Source : BBC

RANSOMWARES VS. INFRASTRUCTURE INFORMATIQUE

CHAÎNE D'APPROVISIONNEMENT

Une chaîne d'approvisionnement est un réseau de liens entre une entreprise et ses fournisseurs pour produire et distribuer un produit ou un service spécifique. Une attaque contre l'un des points de la chaîne d'approvisionnement aura des conséquences en aval.

Lorsque les attaques contre une chaîne d'approvisionnement sont numériques plutôt que physiques, les effets néfastes sont similaires. En s'attaquant à un seul des participants de la chaîne d'approvisionnement, les acteurs malveillants peuvent éventuellement obtenir un accès illimité et difficile à détecter à une grande partie des partenaires commerciaux et de la clientèle.

Exemple

Que peut-il se passer en cas d'attaque contre une chaîne d'approvisionnement ?

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.

Source : WeLiveSecurity

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 mises à jour et des correctifs, d'utiliser un logiciel de protection des endpoints et éventuellement une solution d'EDR, et de sensibiliser les utilisateurs aux emails non sollicités qui les incitent à consulter des sites web inconnus.

RANSOMWARES VS. INFRASTRUCTURE INFORMATIQUE

AUTRES 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. Cela a de quoi donner de nombreux maux de tête aux administrateurs de la sécurité et aux cadres dirigeants.

Presque tous les éditeurs de produits de cybersécurité détectent encore des activités autour de 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.

Enfin, les VPN exigent également de la proactivité de la part des administrateurs informatiques qui doivent mettre à jour les produits de cybersécurité en fonction des 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.

Exemple

Exploitation de vulnérabilités via Microsoft Exchange Server

En mars 2021, Microsoft a diffusé 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 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.

Source : WeLiveSecurity

STRATÉGIES DE DÉFENSE CONTRE LES RANSOMWARES

SEGMENTATION DES CLOUDS ET DES RÉSEAUX

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.

Ces dernières années, la migration des données vers le Cloud est devenue une stratégie d'architecture système courante. Mais le Cloud n'offre pas d'immunité automatique contre les attaques de ransomwares. 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.

STRATÉGIES DE DÉFENSE CONTRE LES RANSOMWARES

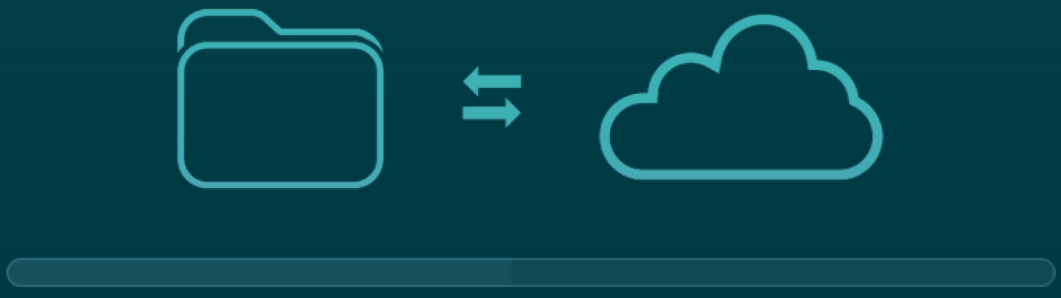
CORRECTIFS ET SAUVEGARDES

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 des attaques de ransomwares.

En corrigeant les systèmes, les voies d'attaque potentielles sont comblées pour empêcher les ransomwares de pénétrer dans votre entreprise. S'ils y parviennent, les dommages éventuels peuvent toutefois être réduits. Un plan de sauvegarde et de récupération correctement géré est également un mécanisme de défense essentiel, qui est crucial pour vos efforts de récupération lorsqu'un ransomware s'est introduit dans votre entreprise.

Cela peut être beaucoup plus compliqué qu'il n'y paraît. Pourquoi ? 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.

C'est plutôt vrai dans l'ensemble, mais n'oubliez pas que certaines attaques de ransomwares sont menées sur une période assez longue, 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.



STRATÉGIES DE DÉFENSE CONTRE LES RANSOMWARES

Il n'y a jamais eu autant d'options pour la sauvegarde et la récupération qu'à ce jour, notamment le stockage dans le Cloud, qu'il soit à distance, sur site ou hybride. Cependant, il y a également de plus en plus de données à sauvegarder, depuis des endroits toujours plus nombreux. 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 avez négligé de sauvegarder.

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 endpoints, serveurs, boîtes de messagerie, lecteurs réseau, appareils mobiles et machines virtuelles. 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.

Infobox

Comment empêcher la propagation des ransomwares

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.

RÉPONSE À UNE ATTAQUE DE RANSOMWARE

Même si vous êtes conscient des dangers des ransomwares et que vous avez mis en place toutes les mesures préventives possibles, votre entreprise doit être prête à répondre à une attaque de ransomware qui parviendrait malgré tout à pénétrer au sein de votre entreprise. Nous vous proposons donc ci-dessous un aperçu pratique afin de pouvoir répondre et réagir à une attaque de ransomware.

Infobox

Votre personnel comprend-il les politiques de sécurité ?

Adressez les questions suivantes dans votre entreprise :

- À qui les collaborateurs doivent-ils signaler les ransomwares ?
- Quelle est la politique de l'entreprise en matière de paiement des demandes de rançon ?
- Quelles mesures l'entreprise est-elle tenue de prendre en cas d'atteinte à la sécurité des données ?
- Qui est autorisé à payer/négocier les rançons ?
- 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.

Problèmes à éviter :

- 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.

RÉPONSE À UNE ATTAQUE DE RANSOMWARE

PLAN DE RÉTABLISSEMENT

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 de messagerie, de téléphonie VoIP et d'accès à Internet.

Exemple d'un plan efficace de traitement des incidents et de rétablissement :

1) Aux premiers signes d'une attaque, prévenir le personnel désigné.
2) Isoler et analyser les machines affectées.
3) 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.
4) Une fois l'attaque confirmée, déclenchez l'intervention de vos équipes spécialisées.
5) Alertez le conseiller juridique.
6) Contactez les prestataires qui peuvent être en mesure de fournir une assistance.
7) Rappelez aux collaborateurs les politiques relatives à la presse et aux réseaux sociaux afin de maintenir le contrôle des communications avec le public.
8) Évaluez la portée de l'attaque et les spécificités du ransomware (par ex. déterminez si une clé de déchiffrement est disponible).
9) Contactez les services de police.
10) Préparez une déclaration à l'avance.
11) Si les fichiers ont été chiffrés, déterminez s'ils peuvent être restaurés à partir de la sauvegarde.
12) Tenez les collaborateurs au courant de la situation.
13) Au besoin, activez votre plan de continuité des activités.

RÉPONSE À UNE ATTAQUE DE RANSOMWARE

14) Les administrateurs informatiques devraient collecter 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.

15) Documentez l'enquête initiale sur l'attaque et les mesures prises pour y remédier.

POURQUOI VOUS NE DEVRIEZ PAS PAYER LA 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 :

1) Certaines données peuvent avoir été corrompues lors du processus de chiffrement et ne sont donc pas récupérables.
2) L'outil de déchiffrement fourni peut être associé à d'autres malwares, ne pas fonctionner correctement ou s'avérer beaucoup plus lent que la récupération à partir de sauvegardes.
3) Le processus de livraison de la clé de déchiffrement peut échouer.
4) L'attaquant est de mauvaise foi et n'a aucune intention de fournir de clé de déchiffrement.
5) Le paiement d'une rançon peut être illégal. Par exemple, en octobre 2020, l'Office of Foreign Assets Control (OFAC) du département du Trésor des États-Unis a déclaré qu'il était illégal d'effectuer des paiements à des personnes, des organisations, des régimes, et dans certains cas des pays entiers, qui figurent sur la liste des sanctions.

Il existe par ailleurs des raisons éthiques de ne pas payer la rançon demandée. Parce que si vous le faites, vous...

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

Infobox

Arguments typiques pour payer une rançon

« C'est moins cher que de restaurer à partir des sauvegardes. »

Si cette affirmation s'appuie uniquement sur des calculs de temps et de main d'œuvre, elle peut être techniquement correcte. Néanmoins, la décision de payer est profondément erronée pour les raisons mentionnées précédemment. La suppression d'un ransomware actif à l'aide d'un logiciel de sécurité n'équivaut par ailleurs 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.

« Nous ne pouvons pas restaurer 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. Cependant, il existe de réelles alternatives au paiement. Vérifiez tout d'abord auprès de votre éditeur de logiciels de sécurité s'il existe un outil de déchiffrement permettant de récupérer les informations sans payer la rançon.

FUTURS SCÉNARIOS DE RANSOMWARES

Les ransomwares tirent parti de la dépendance d'une entreprise à l'égard de la technologie. Nous pouvons donc 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/d'un nouveau logiciel sont découvertes et la possibilité de les détourner à des fins criminelles est évoquée.
- 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.
- Les efforts pour remédier à ces vulnérabilités et les atténuer sont mis en œuvre.
- En l'absence de détournement criminel généralisé, les efforts de remédiation et d'atténuation s'essoufflent.
- Des criminels moins compétents finissent par découvrir que cette « nouvelle » technologie est prête à être exploitée.
- Une nouvelle tendance émerge en matière de malwares.

Ces scénarios de ransomware en constante évolution ont de multiples implications pour les PME. Il est temps de tenir compte de ces menaces potentielles dans votre propre 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 informé des notifications de vulnérabilité liées à ces ressources, ainsi que des correctifs et des mises à jour de leurs micrologiciels. Séparez les objets connectés et autres nouvelles technologies des réseaux de production en segmentant votre réseau.

En raison de l'efficacité accrue des techniques d'extorsion et des nouveaux canaux de diffusion de ransomwares, on estime que des centaines de millions de dollars ont fini sur les comptes de ces cybercriminels techniquement compétents, ce qui a permis à certains de développer leur modèle commercial de ransomwares sous forme de services (RaaS) et de recruter de nombreux nouveaux affiliés (des criminels ayant moins de compétences et d'expérience). Certains gangs ont commencé par ailleurs à acquérir des vulnérabilités zero-day et des identifiants volés, élargissant ainsi le nombre de victimes potentielles.

CONCLUSION

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 administrateur informatique, professionnel de la sécurité et cadre-dirigeant. Il a été démontré à maintes reprises 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.

Pour contrer les vulnérabilités zero-day, les botnets, le spam malveillant et d'autres techniques plus avancées, des technologies de sécurité supplémentaires sont nécessaires. Celles-ci peuvent prendre la forme d'une solution de protection multicouche sur les endpoints, capable de détecter et de bloquer les menaces entrantes dans des emails, via des liens web, RDP et d'autres protocoles réseau. Mais il peut s'agir aussi d'outils de détection et de traitement sur les endpoints pour surveiller, identifier et isoler les anomalies et les signes d'activité malveillante dans l'environnement d'une entreprise.

Protégez vos endpoints contre les ransomwares avec nos solutions ESET.
Contactez-nous pour en savoir plus..

À PROPOS D'ESET

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique pour protéger le patrimoine numérique des entreprises, les infrastructures critiques et les consommateurs du monde entier contre des cybermenaces. Nous protégeons les terminaux fixes et mobiles, les outils collaboratifs, et assurons la détection et le traitement des incidents. Établis dans le monde entier, nos centres de R&D récoltent et analysent les cybermenaces pour protéger nos clients et notre monde numérique.
Pour plus d'informations, consultez le site www.eset.com/fr/
ou suivez-nous sur LinkedIn, Facebook et Twitter.

Digital Security
Progress. Protected.