Se protéger contre les rançongiciels

La sécurité à vérification systématique pour un personnel moderne

Le rançongiciel est là pour longtemps

Le rançongiciel a évolué rapidement en tant que stratégie d'attaque. Autrefois une reprise hostile de parc d'ordinateurs solitaires, aujourd'hui les enjeux augmentent. Les malfaiteurs s'en prennent de plus en plus à des cibles géopolitiques, à des systèmes commerciaux et à des infrastructures critiques (par exemple, la chasse au gros gibier), ce qui pourrait entraîner des dommages sans précédent. Aujourd'hui, les rançongiciels sont l'une des plus grandes menaces en matière de cybersécurité, augmentant de 150 % en 2020 en raison du passage soudain au télétravail.

Les rançongiciels sont désormais classés dans la catégorie du cyberterrorisme, et le récent décret du président américain Biden confirme que des mesures doivent être prises dès maintenant pour assurer la sécurité des systèmes. Une approche à vérification systématique est la norme pour se protéger contre les rançongiciels. Selon le National Institute of Standards and Technology (NIST), « la mise en œuvre d'une architecture à vérification systématique est devenue un mandat de cybersécurité et un impératif commercial. »

La fiche d'information de la Maison-Blanche indique que « les récents incidents de cybersécurité tels que SolarWinds, Microsoft Exchange et l'incident de Colonial Pipeline nous rappellent que les entités du secteur public et privé américain sont de plus en plus confrontées à des cyberactivités malveillantes sophistiquées de la part d'acteurs étatiques et de cybercriminels. »

« Les récents incidents de cybersécurité tels que SolarWinds, Microsoft Exchange et l'incident de Colonial Pipeline nous rappellent que les entités du secteur public et privé américain sont de plus en plus confrontées à des cyberactivités malveillantes sophistiquées de la part d'acteurs étatiques et de cybercriminels. »

Fiche d'information de la Maison-Blanche des États-Unis d'Amérique.

Qu’est-ce qu’un rançongiciel?

En résumé, les rançongiciels utilisent diverses tactiques pour cibler les utilisateurs, principalement par le biais d’infections par des logiciels malveillants, qui commencent généralement par un hameçonnage par courriel, un mot de passe volé ou une attaque par force brute. Une attaque par rançongiciel peut être réalisée en chiffrant des fichiers ou des dossiers, en empêchant l’accès du système au disque dur et en manipulant l’enregistrement de démarrage principal pour interrompre le processus de démarrage du système. Une fois le logiciel malveillant installé et diffusé, les pirates peuvent accéder aux données sensibles et aux données de sauvegarde, qu’ils chiffrent afin de prendre les informations en otage. Les pirates peuvent agir rapidement ou passer des mois à fouiller sans être détectés pour comprendre l’infrastructure du réseau avant de lancer une attaque.

Le détournement de données est destiné à susciter la peur et le sentiment d’urgence chez les victimes. Leurs informations sont inaccessibles jusqu’à ce que le paiement (principalement en bitcoins) puisse être effectué. Même dans ce cas, les entreprises peuvent ne pas récupérer toutes leurs données. Il existe de nombreuses variantes de rançongiciel mais, pour l’essentiel, les cryptorançongiciels sont les plus répandus. En raison du polymorphisme (programmes malveillants qui changent constamment), il existe de nombreuses variantes qui peuvent échapper à la détection.

Le cryptorançongiciel qui verrouille les données s’améliore rapidement. En 2006, les rançongiciels utilisaient un cryptage maison de 56 bits. La version avancée actuelle du rançongiciel utilise les algorithmes symétriques AES et le chiffrement à clé publique RSA ou ECC pour bloquer les données.

Les rançongiciels se transforment en entreprise

Le rançongiciel, qui continue de gagner du terrain, est devenu une activité professionnelle gérée par des organisations criminelles (principalement situées en Chine, en Russie, en Corée du Nord et en Europe de l’Est) qui se consacrent au marquage et à la perturbation de cibles de grande valeur et à l’extraction d’argent en échange de données. Pour y parvenir efficacement, ces organisations sont allées jusqu’à mettre en place des centres d’appels pour guider les cibles dans le processus d’achat de bitcoins et de paiement de la rançon. Certains sont même très bien notés par leurs cibles pour leur bon service à la clientèle.

Parfois, pour inciter au paiement, les attaquants fournissent un « rapport de sécurité » détaillant exactement comment ils ont mené l’attaque après l’échange de la rançon. S’il était judicieux pour les gangs de déchiffrer les fichiers en échange d’argent afin de préserver leur réputation pour la prochaine cible, ce n’est pas toujours le cas. Selon le rapport L'état des rançongiciels 2020 (The State of ransomeware 2021) de Sophos, seuls 8 % des victimes récupèrent leurs données et 29 % en récupèrent plus de la moitié. Parfois, les données sont récoltées et échangées avec d’autres attaquants ou conservées en vue d’une future demande de rançon.

Ces dernières années, les acteurs malveillants ont mis en place un système de rançongiciel-service (RaaS), une solution prête à l’emploi entièrement intégrée permettant à quiconque de déployer une attaque de rançongiciels sans savoir coder. Tout comme les produits SaaS (Software-as-a-Service), le RaaS donne un accès relativement bon marché et facile à ces types de programmes malveillants pour une somme inférieure au coût de la création de votre propre programme. Les fournisseurs de RaaS prennent généralement une part de 20 à 30 % du bénéfice généré par la rançon. Il existe désormais des modèles d’abonnement et d’affiliation qui permettent de mener à bien des attaques réussies. Le groupe de pirates REvil avait un modèle d’affiliation qui permettait de partager les bénéfices avec toute personne ayant contribué à la réussite d’une attaque par rançongiciel. Ce modèle a conduit à l’augmentation spectaculaire du volume des attaques par rançongiciel

D’abord attribuée au gang Maze, une autre tendance est la double extorsion, dans laquelle les pirates prennent les informations détournées et menacent de les publier sur le Web profond ou Internet si leurs demandes ne sont pas satisfaites. Ils disposent d’une infrastructure intégrée pour gérer ces décharges de données, selon le rapport 2020 de Verizon sur les enquêtes relatives aux violations de données. La tactique du « nom et honte » est désormais populaire auprès de la plupart des gangs de rançongiciel, tout comme le modèle de la « pénalité », où le prix augmente à mesure que le temps passe.

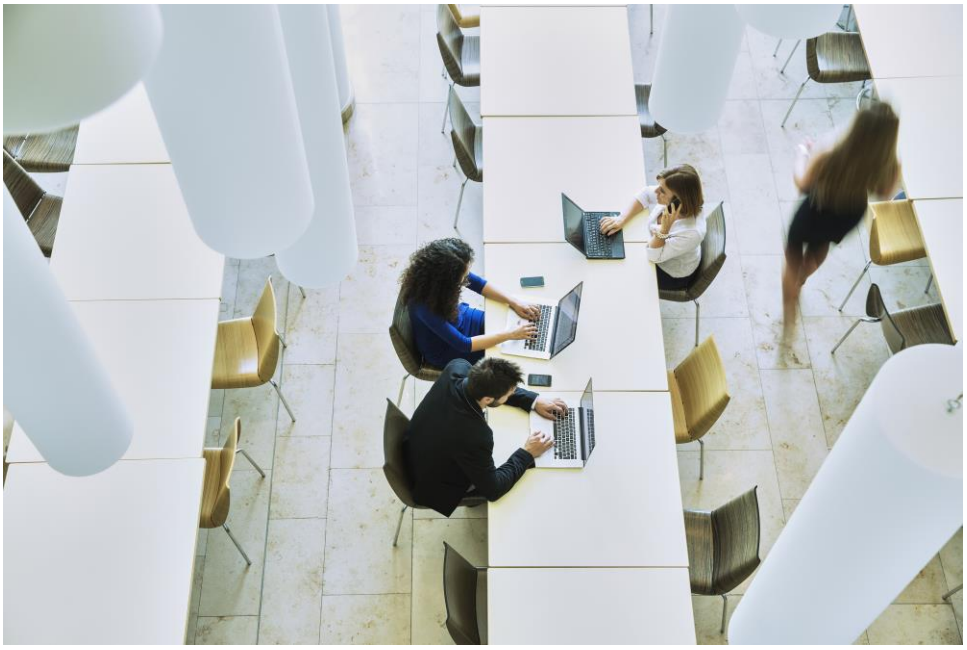
Alors que les entreprises renforcent leur dispositif de sécurité pour les ordinateurs et les réseaux contre les attaques par rançongiciel, les pirates se tournent désormais vers l'exploitation des appareils mobiles. Les appareils mobiles ont un écran beaucoup plus petit et ne fournissent pas des informations complètes au premier coup d'œil (le courrier électronique par exemple), ce qui facilite le clic des victimes sur les liens malveillants. Les attaques de l'Internet des objets (IDO) sont également en hausse, car les rançongiciels et le manque de sécurité peuvent transformer les appareils et les objets en points d'entrée pour les outils de rançongiciel. En 2020, les attaques de rançongiciel ciblant les appareils d'IDO ont augmenté de 109 % dans l'ensemble des États-Unis.

Ces facteurs, associés à des pays qui servent de refuge aux attaquants, ont conduit à l'augmentation des crimes liés aux rançongiciels. Il y a eu une attaque réussie de rançongiciel toutes les 10 secondes en 2020, et selon une enquête Anomali Harris Poll, un Américain sur cinq est victime d'une attaque de rançongiciel. En outre, Infosecurity Magazine rapporte que la méthode d'attaque la plus populaire « était de loin le trafic de réseau de zombies (28 %), suivi par les cryptomineurs (21 %), les voleurs d'informations (16 %), les mobiles (15 %) et les programme malveillant bancaires (14 %). » En réaction, les entreprises s'empressent de consacrer plus d'argent à la sécurité (150 milliards de dollars en 2021 selon Gartner).

Les attaques contre les particuliers sont en baisse; les pirates se concentrant sur des cibles spécifiques plus lucratives. Les fournisseurs de services gérés (MSP) signalent une augmentation de 85 % des attaques contre les PME. Les entreprises, ainsi que les sociétés d'infrastructure, de soins de santé, les administrations publiques et les entreprises manufacturières sont plus que jamais ciblées, avec des prix se chiffrant en millions en échange de leurs données. Le montant d'une rançon a doublé l'année dernière, les attaquants s'en prenant à des entreprises plus importantes. Les attaques contre les vendeurs, les sous-traitants et les logiciels tiers ont également fortement augmenté. Les entreprises ont dû se fier à la sécurité de ces parties extérieures qui ont accès à leurs systèmes.

L'essor des gangs de rançongiciels	Le premier cas connu de rançongiciel provient de disquettes contenant des études sur le sida et des logiciels malveillants, distribuées dans le monde entier en 1989 par le Dr Joseph Popp. Les disques chiffraient les fichiers du système de la victime et lui refusaient l'accès jusqu'à ce qu'elle envoie un paiement de 189 dollars à une boîte postale au Panama. Des CD appâts ont ensuite été distribués lors de la conférence sur le sida de l'Organisation mondiale de la santé. Le paiement et l'expédition des CD étaient problématiques et coûteux.
2006	Les cybercriminels ont commencé à utiliser une forme plus efficace de chiffrement à clé publique RSA 660 pour chiffrer les fichiers plus rapidement. Les principaux acteurs de cette époque étaient le cheval de Troie Archiveus et le GPcode qui utilisaient le courrier électronique d'hameçonnage comme point d'entrée.
2008-2009	De nouveaux logiciels antivirus chargés de logiciels malveillants de type rançongiciel sont apparus, et des logiciels de sécurité malveillants ont utilisé FileFix Pro pour extorquer de l'argent en échange du déchiffrement.
2010	Le bitcoin a tout changé. Dix mille variantes de rançongiciel ont été détectées, et le rançongiciel de verrouillage d'écran a fait sa première apparition.
2013	Un quart de million d'échantillons de rançongiciel existaient, et Cryptolocker et Bitcoin sont rapidement devenus le principal mode de paiement. Les rançongiciels utilisaient un chiffrement RSA 2048 bits pour augmenter les demandes, ce qui s'est avéré lucratif pour les gangs.
2015	Le cheval de Troie du rançongiciel Teslacrypt est apparu; il existe désormais 4 millions de variantes de rançongiciels et le service de rançongiciel-service (RaaS) a été introduit.
2016	JavaScript et Locky ransomware étaient populaires, Locky infectant 90 000 victimes par jour. Les attaquants ont ciblé les grandes organisations, comme les hôpitaux et les institutions académiques. Les rançongiciels ont atteint plus d'un milliard de dollars de bénéfices. Le logiciel malveillant Petya a causé des pertes financières de plus de 10 milliards de dollars.
2017	Le crypto-ver WannaCry est apparu cette année, évoluant chaque jour en plusieurs variantes et se propageant rapidement sur 300 000 ordinateurs dans le monde grâce à un exploit de Microsoft.
2018	Katsuya a été lancé. SamSam a provoqué l'arrêt de nombreux services municipaux dans la ville d'Atlanta.

2019	REvil, un gang privé de RaaS, a vu le jour en Russie. Ryuk, une variante de rançongiciel sophistiquée et coûteuse qui s'insère dans des pièces jointes malveillantes et des courriels d'hameçonnage, a exigé des paiements plus élevés par rapport à des attaques similaires et a effectivement mis hors service tous les grands journaux des États-Unis.
2020	Darkside, Egregor et Sodinokibi sont devenus des acteurs majeurs. Ryuk est passé d'un cas par jour à 19,9 millions en septembre, soit l'équivalent de huit cas par seconde.
2021	Les malfaiteurs de REvil/Sodinokibi, Conti et Lockbit ont durement touché les soins de santé. CryptoLocker a soutiré 40 millions de dollars à un grand assureur, CNA Financial, dans le cadre de l'un des plus importants paiements de rançongiciel à ce jour. Le DarkSide a réussi à attaquer la Colonial Pipeline Company, marquant ainsi le plus grand piratage d'infrastructures critiques américaines rendu public.



Le périmètre s'élargit

Comment les rançongiciels sont-ils devenus si répandus? Auparavant, le périmètre était un mur d'enceinte qui gérait les données et les applications centralisées par le biais de pare-feu de réseau privé virtuel (VPN) et de solutions de gestion des appareils mobiles (MDM), comme des douves entourant le château du réseau. Aujourd'hui, le travail se fait de n'importe où et sur n'importe quel appareil (y compris les appareils mobiles personnels), et les données doivent être accessibles à partir d'applications tierces dans le nuage informatique. Il n'y a pas de douves, mais plutôt de nombreuses entrées au château. L'essor du télétravail pendant la pandémie a transformé le périmètre traditionnel en «périmètre défini par logiciel». Dans la hâte de continuer à faire travailler les employés, la sécurité a été laissée de côté pour bon nombre d'entre eux, ce qui a créé des occasions de rançongiciels pour les malfaiteurs.

Accès à distance

Le Gartner principales tendances en matière de sécurité et de risque pour 2021 (Gartner Top Security and Risk Trends for 2021) indique que 64 % des employés sont désormais en mesure de travailler à domicile et que deux cinquièmes de la population active travaillent à domicile. Pendant la pandémie, la majorité des travailleurs ont dû travailler à distance à 100 % et devaient pouvoir travailler sur leurs propres appareils tout en accédant aux applications de logiciel-service (SaaS) dans le nuage informatique et sur site. De nombreuses entreprises ne disposaient pas de l'infrastructure nécessaire pour accompagner ce changement. Aujourd'hui, l'accès à distance est la nouvelle réalité de la main-d'œuvre. À mesure que les organisations s'adaptent à cette norme

de fonctionnement, on prévoit que la main-d'œuvre adoptera un modèle hybride composé de travailleurs à distance et de personnes retournant au bureau.

Peter Firstbrook, vice-président analyste chez Gartner, a déclaré dans un billet de blogue : « Alors que la nouvelle normalité prend forme, toutes les organisations auront besoin d'une posture défensive toujours connectée, et de clarifier quels risques commerciaux les utilisateurs distants augmentent pour rester en sécurité. »

Les entreprises qui n'ont pas renforcé leur dispositif de sécurité en prévision de ce changement ou qui n'ont pas renforcé leur formation interne en matière de sécurité offrent une porte d'entrée facile aux attaquants. Selon Gartner, 57 % des violations sont liées à la négligence d'un employé ou d'un tiers. Selon ZDNet, le protocole de bureau à distance (RDP) est le premier moyen utilisé par les acteurs de la menace pour accéder aux ordinateurs Windows et installer des rançongiciels et d'autres logiciels malveillants, suivi par le hameçonnage par courriel et les exploits de bogues de VPN.

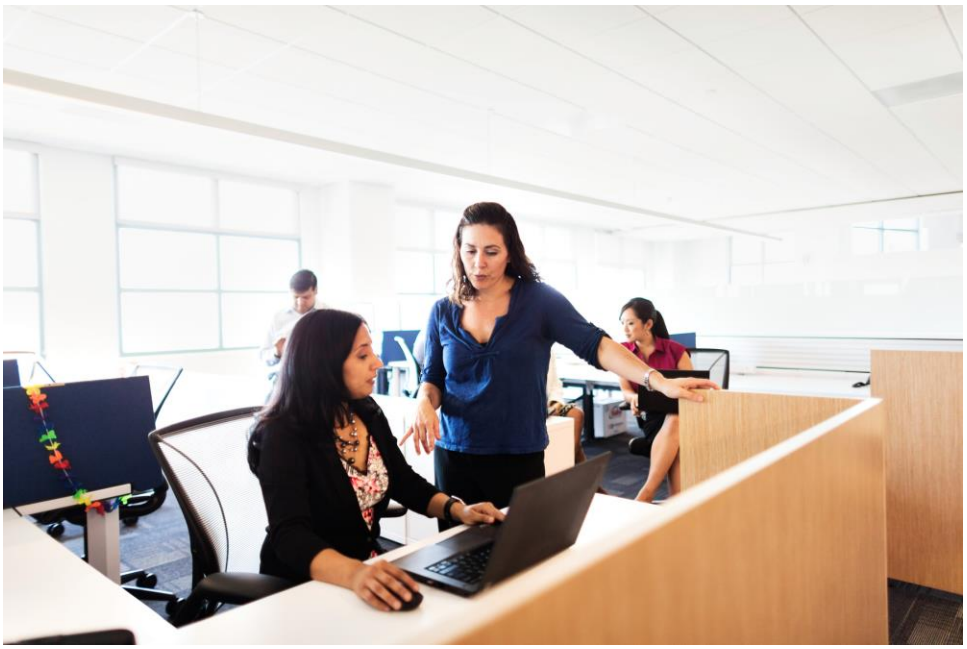
Contraintes VPN

Le piratage des exploits dans les VPN est la troisième méthode d'entrée la plus populaire pour les pirates de rançongiciel. Le piratage qui a entraîné la fermeture de la Colonial Pipeline Company était le résultat d'un mot de passe compromis provenant d'un VPN non utilisé. Alors que les VPN peuvent limiter l'accès aux applications sur site, l'accès aux applications dans le nuage informatique est incohérent, ce qui peut entraîner des vulnérabilités. Une fois compromis, les VPN peuvent conduire à un accès par une porte dérobée au réseau où les pirates peuvent installer des logiciels malveillants sur les systèmes internes.

Selon une étude de Google, un réseau privé virtuel (VPN) à vérification systématique et un pare-feu assortis de l'authentification multifactorielle permettent d'éviter 100 % des attaques par robot automatisé, 99 % des attaques par hameçonnage et 90 % des attaques ciblées.

Terminaux non protégés

Comme de plus en plus de dispositifs se connectent aux réseaux d'entreprise, le nombre de dispositifs personnels et de dispositifs fantômes a augmenté. Comme ces dispositifs ne sont pas nécessairement surveillés ou mis à jour, ils peuvent potentiellement entraîner des violations au niveau des terminaux clés sans être détectés. Alors que les pirates cherchent méticuleusement un moyen d'entrer, les points d'extrémité non protégés et le manque d'informations sur les personnes et les objets qui se connectent à votre réseau et sur l'état de santé des appareils peuvent conduire à une violation.



Hameçonnage, attaques ciblées et vulnérabilités

Quelles sont les techniques utilisées dans les attaques par rançongiciel? Il s'agit d'un processus en plusieurs étapes qui peut être relativement court ou s'étaler sur plusieurs mois pour accéder aux données les plus précieuses et les crypter, et qui causera le plus de dommages si elles sont prises en otage. Selon CSOonline.com, 94 % des logiciels malveillants sont diffusés par courrier électronique et les attaques par hameçonnage sont responsables de plus de 80 % des incidents de sécurité. Les autres points d'entrée sont les mises à jour non corrigées et les vulnérabilités de type « zero day ». Presque toutes commencent par le vol d'informations d'identification.

Techniques de rançongiciel

Le « Spray and Pray », ou le hameçonnage à grande échelle

Les agents de menace acquièrent des listes d'adresses électroniques sur le marché noir, puis analysent les informations d'identification et distribuent des courriels d'hameçonnage. Seules quelques références sont nécessaires pour réussir, souvent acquises par le biais d'un courriel avec des pièces jointes malveillantes, de sites Web frauduleux qui semblent légitimes, ou d'une fausse identité ciblant des employés de grande valeur.

Hameçonnage ciblé

Cette attaque coordonnée et ciblée sur un groupe spécifique d'utilisateurs est menée par l'envoi de messages personnalisés et socialement élaborés qui suscitent la curiosité, la peur ou la récompense d'une source légitime. Les courriels et le site Web contiennent des logiciels malveillants utilisés pour voler des informations d'identification. Les logiciels malveillants peuvent également être diffusés par les médias sociaux et les applications de messagerie instantanée.

Force brute

Selon un sondage de LastPass, 91 % des personnes interrogées ont reconnu qu'elles réutilisaient les mots de passe. Les pirates informatiques le savent bien et récupèrent les mots de passe dans les décharges d'informations d'identification ou sur le dark web. Ils se servent ensuite d'outils automatisés pour tester les mots de passe sur différents sites, ce que l'on appelle le remplissage de justificatifs ou la force brute. Une fois entré, l'attaque peut commencer.

Exploitation des vulnérabilités connues

En plus de savoir quels appareils se connectent à votre réseau, il est important de connaître l'état de santé des appareils et de savoir si les correctifs et les mises à jour sont à jour pour maintenir un profil de sécurité élevé. Selon Security Boulevard, « les composants open source obsolètes et 'abandonnés' sont omniprésents. Et 91 % des bases de code contenaient des composants qui avaient soit plus de quatre ans de retard, soit aucune activité de développement au cours des deux dernières années.»

Guide étape par étape d'une attaque par rançongiciel

Chiffrement des rançongiciels

Le plus souvent, les attaques par rançongiciels chiffrent les données sur les systèmes cibles, les rendant inaccessibles jusqu'à ce qu'une rançon soit payée pour le déchiffrement. La dernière tactique en date est le double chiffrement, dans lequel les pirates cryptent un système deux fois, ou deux gangs différents ciblent la même victime. Avec cette approche, les attaquants ont la possibilité de collecter deux rançons en recevant le paiement de la première couche de chiffrement, puis en surprenant les victimes avec une autre couche après avoir reçu le paiement de la première. Le chiffrement le plus courant est asymétrique ou symétrique.

Coordonner l'attaque

À ce stade, les pirates de rançongiciel font leurs devoirs sur les entreprises spécifiques qu'ils ciblent. Ils peuvent acheter des listes d'adresses électroniques sur le dark web, identifier les dirigeants importants, se renseigner sur les finances de l'entreprise, rechercher les profils des médias sociaux et dresser une liste des principales parties prenantes telles que les entrepreneurs, les vendeurs et les partenaires. Quelles sont les tactiques utilisées par les pirates pour s'infiltrer? Les trois principales attaques en 2020 provenaient de terminaux RDP mal sécurisés, d'attaques de hameçonnage par courriel et de l'exploitation de vulnérabilités VPN de type «zero day». Les informations d'identification compromises constituent le principal moyen d'accès des acteurs malveillants.

Mouvement vertical

Dans la phase d'infiltration et d'infection, on parle de mouvement vertical lorsque les acteurs de la menace passent d'une position externe à une position interne. Une fois à l'intérieur, ils analysent les fichiers et exécutent un code malveillant sur les terminaux et les périphériques réseau. Le logiciel malveillant se déplace dans le système infecté, désactivant les pare-feu et les logiciels antivirus. À ce stade, les attaquants ont pris le contrôle des données, mais elles ne sont pas encore cryptées. Les points d'entrée courants pour le mouvement vertical comprennent les boîtes de courriel hameçonnées, les serveurs Web de bas niveau et les terminaux mal protégés.

Prise de pied latérale

Les menaces persistantes avancées (APT) ont gagné en succès grâce aux mouvements latéraux. Pour s'implanter, les criminels doivent chiffrer les ordinateurs et diffuser le rançongiciel à un maximum de systèmes. Une fois l'accès obtenu, la chasse aux pirates peut commencer. Ils commencent à se déplacer latéralement, sans être détectés, pendant des semaines ou des mois à travers le réseau pour identifier des cibles clés comme le centre de commande et de contrôle (C2), les clés asymétriques et les fichiers de sauvegarde. Parallèlement, ils élèvent leur accès et leurs autorisations en infectant d'autres systèmes et comptes d'utilisateurs et préparent une présence malveillante persistante pour détourner

Exfiltrer les données

Une fois l'évaluation de l'inventaire terminée, le chiffrement commence. Les sauvegardes du système sont supprimées, les fichiers et dossiers locaux sont corrompus, des lecteurs réseau non mappés sont connectés aux systèmes infectés et une communication avec le centre de commande et de contrôle est établie pour générer les clés cryptographiques utilisées sur le système local. Les données du réseau sont copiées localement, chiffrées puis téléchargées, remplaçant les données d'origine. Les données exfiltrées peuvent être utilisées pour une double extorsion. Dans ce cas, une rançon est demandée pour déchiffrer les données cryptées, puis une deuxième rançon est exigée

Paiement et déverrouillage

Les attaquants activent ensuite le logiciel malveillant, bloquent les données et annoncent leur demande de rançon sur les sites compromis, avec des instructions spécifiques sur la manière d'effectuer le paiement, généralement en bitcoins. Un rançonlogiciel crée un problème de temps d'arrêt très coûteux et extrêmement difficile à résoudre. Des menaces sont proférées, et le compte à rebours commence. Les entreprises doivent décider si elles veulent prendre le risque de payer, essayer de restaurer leurs fichiers par elles-mêmes ou faire appel à leur assurance cybersécurité, qui ne récupère qu'une partie de la rançon. Le choix est difficile, ce qui explique pourquoi il est impératif que

Prise de pied latérale	**Exfiltrer les données**	**Paiement et déverrouillage**
les données. Parmi les exemples de mouvements latéraux, citons l'exploitation de services à distance, le hameçonnage par harponnage interne (spear phishing) et l'utilisation de mots de passe volés, également connue sous le nom de «pass the hash».	pour ne pas divulguer les données volées.	les organisations mettent en œuvre une architecture à vérification systématique et adoptent des pratiques de sécurité renforcées pour éviter cette situation.

Secteurs d'activité vulnérables

Les soins de santé, les municipalités et les gouvernements, ainsi que le commerce de détail, l'éducation et la finance, sont les secteurs les plus touchés par les attaques de rançongiciel. Ces secteurs disposent de solutions patrimoniales complexes et ne peuvent pas toujours tirer parti d'une sécurité infonuagique robuste. Les secteurs de la santé, de l'éducation et de l'administration tardent à adapter leur posture de sécurité aux mises à jour et aux nouvelles technologies, ce qui en fait des cibles lucratives et faciles.

Arrêter la compromission par les rançongiciels avant qu'elle ne commence

Dans une attaque par rançongiciel, les attaquants doivent d'abord obtenir un accès. Ils peuvent le faire en obtenant des informations d'identification compromises, comme dans le cas de la fuite de Colonial Pipeline.

L'authentification multifactorielle (MFA) Duo peut contribuer à empêcher les rançongiciels d'obtenir un accès en premier lieu. Duo MFA exige qu'un utilisateur présente une combinaison de deux ou plusieurs justificatifs d'identité pour vérifier son identité lors de la connexion. Par exemple, en plus d'un nom d'utilisateur et d'un mot de passe, la MFA demande un élément que vous possédez, comme un dispositif de confiance ou un jeton logiciel ou matériel, avant d'accorder l'accès aux ressources. Grâce à cette exigence supplémentaire, la MFA rend beaucoup plus difficile pour les rançongiciels de prendre pied.

Les rançongiciels utilisent aussi volontiers des services à distance, tels que des RDP et VPN, pour accéder à un réseau. Darkside, l'auteur présumé de l'attaque de Colonial Pipeline, est soupçonné d'avoir utilisé un accès VPN d'entreprise pour s'introduire dans l'environnement de la victime. Plus qu'une simple MFA, Duo MFA, Duo Device Trust, Duo Network Gateway (DNG) et Duo Trust Monitor se combinent en une seule solution d'accès sécurisé et peuvent aider à sécuriser l'accès à distance à l'infrastructure sur site et à empêcher les ransomwares d'y accéder.

Duo MFA exige plus qu'un nom d'utilisateur et un mot de passe pour s'authentifier. DNG permet aux utilisateurs d'accéder à des sites web, des applications web, des serveurs SSH et RDP sur site sans avoir à se soucier des identifiants VPN. Duo Device Trust garantit que l'appareil accédant à distance aux ressources est un ordinateur de confiance et non le dispositif d'un attaquant. Enfin, Duo Trust Monitor prête attention aux demandes d'authentification qui semblent suspectes, comme celles provenant de pays où les acteurs de ransomware sont connus pour être actifs, et de pays où une organisation n'a pas d'employés.

L'utilisation de logiciels malveillants est également une technique d'infection populaire des rançongiciels. Cisco propose d'autres solutions complémentaires, telles que Cisco Secure Endpoint et Email Gateway, qui permettent d'inspecter, de détecter et de bloquer les rançongiciels avant qu'ils n'infectent les terminaux.

Comment Duo aide à se protéger contre les rançongiciels

Selon Gartner, 90 % des rançongiciels peuvent être évités. Duo est particulièrement bien placé pour aider les organisations sur trois fronts :

1. Empêcher les rançongiciels de s'implanter dans un environnement
2. Empêcher ou ralentir la propagation des rançongiciels s'ils parviennent à s'infiltrer dans une organisation
3. Protéger les actifs et les parties critiques de l'organisation pendant que l'attaquant est encore présent dans l'environnement et jusqu'à ce qu'il soit complètement remédié à la situation.

Lutter contre la propagation

Les rançongiciels qui touchent un petit nombre de systèmes ont un effet limité et il est peu probable qu'une organisation s'arrête de fonctionner et veuille payer une rançon. La propagation des rançongiciels est donc cruciale pour faire tomber une partie importante d'une organisation et l'obliger à payer la rançon pour reprendre rapidement ses activités. En 2017, WannaCry et NotPetya ont utilisé l'exploit External Blue pour tirer parti d'une vulnérabilité de Microsoft et la propager sans intervention de l'utilisateur.

L'application Device Health de Duo permet de maintenir les appareils à jour, ce qui rend la propagation automatique des rançongiciels plus difficile. En outre, il offre une visibilité en vérifiant l'état d'intégrité de l'appareil, y compris son degré de mise à jour, à chaque tentative de connexion. Et grâce à la fonction d'autoréparation de Duo, les utilisateurs peuvent facilement maintenir leurs appareils à jour sans l'aide du service informatique.

Remédier à la situation en toute sécurité

Se remettre d'une attaque par rançongiciel et rétablir les systèmes en ligne ne signifie pas nécessairement que l'attaquant a quitté l'environnement. Ils ont peut-être essayé d'établir une persistance pour revenir plus tard. Une technique courante consiste à compromettre des comptes existants ou à créer de nouveaux comptes, souvent en accédant à Active Directory ou à d'autres répertoires contenant des comptes d'utilisateurs. Duo MFA peut apporter la tranquillité d'esprit qu'un attaquant qui est toujours sur le réseau ne peut pas facilement pivoter et se déplacer latéralement en utilisant des informations d'identification compromises. Elle peut également permettre de gagner du temps et d'empêcher l'attaquant de commettre d'autres dommages pendant que l'attaque est entièrement corrigée, en supprimant toute trace de persistance.

Mise en œuvre d'un modèle de sécurité à vérification systématique

Fondée sur le principe «ne jamais faire confiance, toujours vérifier», la vérification systématique est un modèle de sécurité qui peut aider les organisations à mettre en œuvre de manière proactive les meilleures pratiques connues pour protéger contre les cyberattaques, notamment les rançongiciels.

La vérification systématique est si importante que la Maison-Blanche a publié un ordre exécutif imposant spécifiquement la vérification systématique et l'authentification multifactorielle.

Duo fournit une MFA facile à utiliser et à mettre en œuvre. Elle permet également aux organisations de n'accorder l'accès que si un utilisateur et son appareil peuvent être vérifiés et mis en confiance. Cette capacité à contrôler et à gérer les accès est l'un des piliers fondamentaux de la vérification systématique, et Duo MFA est l'une des premières étapes de la mise en œuvre d'un cadre à vérification systématique.

Conclusion

Les rançongiciels seront plus fréquents et les entreprises doivent être plus vigilantes. L'ingénierie sociale et le hameçonnage par harponnage réussissent parce qu'ils exploitent l'élément humain de la sécurité d'une organisation. L'adoption et la mise en œuvre d'une philosophie de sécurité à vérification systématique, qui commence par une MFA fort et une plateforme d'accès de confiance, sont importantes pour garder une longueur d'avance sur les attaques rançongiciels.

Mettez à jour votre défense au-delà de MFA avec Duo

Les organisations peuvent se défendre contre l'impact des rançongiciels par le biais d'attaques sociales et d'hameçonnage ciblé en mettant en œuvre des politiques d'accès conditionnel qui exploitent les facteurs contextuels, tels que la localisation et la posture de l'appareil, afin de susciter la confiance des utilisateurs et de leurs appareils.

Duo est une plateforme de sécurité infonuagique qui protège l'accès à toutes les applications, quel que soit l'utilisateur, l'appareil et l'emplacement. Nous avons simplifié l'accès sécurisé pour faire face aux risques liés aux identités et aux appareils grâce à six fonctionnalités essentielles :

1. Vérifiez l'identité des utilisateurs grâce à des méthodes d'authentification multifactorielle sûres et flexibles.
2. Offrez une expérience de connexion cohérente avec L'authentification unique Duo (Duo Single Sign-On), qui fournit un accès centralisé aux applications sur site et infonuagiques.
3. Obtenez une visibilité sur chaque appareil et tenez un inventaire détaillé de tous les appareils qui accèdent aux applications de l'entreprise.
4. Établissez la confiance des appareils par des contrôles de santé et de posture pour les appareils gérés ou non gérés avant d'accorder l'accès aux applications.
5. Appliquez des politiques d'accès granulaires pour limiter l'accès aux utilisateurs et aux appareils qui répondent aux niveaux de tolérance au risque de l'organisation.
6. Surveillez et détectez les comportements de connexion à risque à l'aide de Duo Trust Monitor, ou exportez les connexions vers votre SIEM, afin de remédier aux événements suspects tels que l'inscription d'un nouveau dispositif pour l'authentification ou la connexion à partir d'un emplacement inattendu.

Pourquoi choisir Duo?

Sécurisation rapide

Duo fournit les éléments constitutifs de la vérification systématique en une seule solution qui est rapide et facile à déployer auprès des utilisateurs. En fonction de leur cas d'utilisation spécifique, certains clients peuvent être opérationnels en quelques minutes.

Convivialité

Les utilisateurs peuvent s'inscrire eux-mêmes en téléchargeant simplement une application depuis le magasin d'applications et en se connectant. Les contrôles de la maintenance et des politiques sont faciles à gérer pour les administrateurs et offrent une visibilité claire.

S'intègre avec toutes les applications

Notre produit est conçu pour être agnostique et fonctionner avec les systèmes existants. Quels que soient les fournisseurs de services informatiques et de sécurité que vous utilisez, avec Duo, vous pouvez toujours sécuriser l'accès à toutes les applications de travail, pour tous les utilisateurs, de partout.

Coût total d'acquisition (TCO) moins élevé

Parce que Duo est facile à mettre en œuvre et n'exige pas le remplacement des systèmes, il nécessite beaucoup moins de ressources en temps et en coût, vous permettant d'être rapidement opérationnel et de commencer le voyage vers un modèle de sécurité à vérification systématique.

Références

The Pandemic-hit World Witnessed a 150% Growth of Ransomware, https://cisomag.eccouncil.org/growth-of-ransomware-2020/, CISO Magazine, 5 mars 2021

Exclusive: U.S. to give ransomware hacks similar priority as terrorism, https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/, Reuters, 3 juin 2021

NIST Announces Tech Collaborators on NCCoE Zero Trust Project, https://www.hstoday.us/industry/emerging-innovation/nist-announces-tech-collaborators-on-nccoe-zero-trust-project/, Homeland Security Today, 24 septembre 2021

FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware, https://www.whitehouse.gov/briefingroom/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware, The White House, 13 octobre 2021

Types of Encryption: Symmetric or Asymmetric? RSA or AES?, https://preyproject.com/blog/en/types-ofencryption-symmetric-or-asymmetric-rsa-or-aes/, Prey Project, 15 juin 2021

What We Know About DarkSide, the Russian Hacker Group That Just Wreaked Havoc on the East Coast, https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hackergroup-just-wreaked-havoc, The Heritage Foundation, 20 mai 2021

What We Can Learn From Ransomware Actor "Security Reports," https://www.coveware.com/blog/2021/6/24/what-we-can-learn-from-ransomware-actor-security-reports, Coveware, 24 juin 2021

The State of Ransomware 2021, https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx, Sophos, 2021

Data Mining Process: The Difference Between Data Mining & Data Harvesting, https://www.import.io/post/the-difference-between-data-mining-data-harvesting, Import.io, 23 avril 2019

Ransomware: Enemy at The Gate, https://ussignal.com/blog/ransomware-enemy-at-the-gate, US Signal, 3 septembre 2021

2020 Data Breach Investigations Report, https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf, Verizon, 2020

Malware is down, but IoT and ransomware attacks are up, https://www.techrepublic.com/article/malwareis-down-but-iot-and-ransomware-attacks-are-up/, Tech Republic, 23 juin 2020

One Ransomware Victim Every 10 Seconds in 2020, https://www.infosecurity-magazine.com/news/one-ransomware-victim-every-10/, Infosecurity Magazine, 25 février 2021

Terrifying Statistics: 1 in 5 Americans Victim of Ransomware, https://sensorstechforum.com/1-5-americans-victim-ransomware/, Sensors Tech Forum, 19 août 2019

Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021, https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem, Gartner, 17 mai 2021

1 in 5 SMBs have fallen victim to a Ransomware attack, https://www.helpnetsecurity.com/2019/10/17/smbs-ransomware-attack/, Help Net Security, 17 octobre 2019

Ransomware – how to stop this growing, major cause of downtime, https://polyverse.com/blog/ransomware-how-to-stop-this-growing-major-cause-of-downtime, Polyverse.com

The strange history of ransomware, https://theworld.org/stories/2017-05-17/strange-history-ransomware, PRI The World, 17 mai 2017

Ransomware Timeline, https://www.tcdi.com/ransomware-timeline, tcdi.com, 27 décembre 2017

A History of Ransomware Attacks: The Biggest and Worst rançongiciel Attacks of All Time, https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time, Digital Guardian, 2 décembre 2020

One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack, https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5, Business Insider, 22 mai 2021

Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare, https://www.wired.com/story/atlantaspent-26m-recover-from-ransomware-scare, Wired.com, 23 avril 2018

Cyber-attack: US and UK blame North Korea for WannaCry, https://www.bbc.com/news/world-uscanada-42407488, BBC.com, 19 septembre 2017

Ransomware: Now a Billion Dollar a Year Crime and Growing, https://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646, NBCNews.com, 9 janvier 2017

The Untold Story of NotPetya, the Most Devastating Cyber Attack in History, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world, Wired.com, 22 août 2018

Ransomware in Healthcare Facilities: The Future is Now, https://mds.marshall.edu/cgi/viewcontent.cgi?article=1185&context=mgmt_faculty, Marshall University Digital Scholar, automne 2017

New ransomware holds Windows files hostage, demands $50, https://www.networkworld.com/article/2265963/new-ransomware-holds-windows-files-hostage--demands--50.html, NetworkWorld.com, 26 mars 2009

Preventing Digital Extortion, https://subscription.packtpub.com/book/networking_and_servers/9781787120365/4/ch04lvl1sec24/the-advancement-of-locker-ransomware-winlock, PackIt, mai 2017

The Irreversible Effects of Ransomware Attack, https://www.crowdstrike.com/blog/irreversible-effectsransomware-attack, CrowdStrike, 20 juillet 2016

New Era of Remote Working Calls for Modern Security Mindset, Finds Thales Global Survey of IT Leaders, https://www.businesswire.com/news/home/20210914005014/en/New-Era-of-Remote-Working-Calls-for-Modern-Security-Mindset-Finds-Thales-Global-Survey-of-IT-Leaders, Business Wire, 14 septembre 2021

FBI sees spike in cyber crime reports during coronavirus pandemic, https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic, The Hill, 16 avril 2020

Symantec Security Summary - September 2021, https://symantec-enterprise-blogs.security.com/blogs/featurestories/symantec-security-summary-september-2021, Symantec Security, 27 septembre 2021

INTERPOL report shows alarming rate of cyberattacks during COVID-19, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19, Interpol, 4 août 2020

Gartner Top Security and Risk Trends for 2021, https://www.gartner.com/smarterwithgartner/gartner-topsecurity-and-risk-trends-for-2021, Gartner, 5 avril 2021

Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time, https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time, Gartner, 14 juillet 2020

Gartner Highlights Identity-First Security as a Top Security Trend for 2021, https://www.attivonetworks.com/blogs/gartner-identity-first-security-in-2021, Attivo, 27 avril 2021.

2021 SonicWall Cyber threat Report, https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyberthreat-report.pdf, SonicWall, 2021

Top exploits used by ransomware gangs are VPN bugs, but RDP still reigns supreme, https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme, ZDNet.com, 23 août 2020

VPN exploitation rose in 2020, organizations slow to patch critical flaws, https://www.cybersecuritydive.com/news/trustwave-network-security-remote-access/602044/, Cybersecurity Dive, 18 juin 2021

New research: How effective is basic account hygiene at preventing hijacking, https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html, Google Blog, 17 mai 2019

Top cybersecurity statistics, trends, and facts, https://www.csoonline.com/article/3634869/top-cybersecuritystatistics-trends-and-facts.html, CSOonline.com, 7 octobre 2021

Protecting Companies From Cyberattacks, https://www.inc.com/knowbe4/protecting-companies-fromcyberattacks.html, Inc.com, 20 septembre 2021

ThreatList: People Know Reusing Passwords Is Dumb, But Still Do It, https://threatpost.com/threatlistpeople-know-reusing-passwords-is-dumb-but-still-do-it/155996/, Threatpost, 25 mai 2020

Synopsys Study Shows 91% of Commercial Applications Contain Outdated or Abandoned Open Source Components, https://www.securitymagazine.com/articles/92368-synopsys-study-shows-91-ofcommercial-applications-contain-outdated-or-abandoned-open-source-components, Security Magazine, 12 mai 2020

Ransomware's Dangerous New Trick Is Double-Encrypting Your Data, https://www.wired.com/story/rançongiciel-double-encryption/, Wired.com, 17 mai 2021

Combating Lateral Movement and the Rise of Ransomware, https://www.msspalert.com/cybersecurityguests/combating-lateral-movement-and-the-rise-of-ransomware, MSSP Alert, 24 juin 2021

Lateral Movement, https://attack.mitre.org/tactics/TA0008/, MITRE| ATT&CK, 17 octobre 2019

Industries Impacted by Ransomware, https://airgap.io/blog/industries-impacted-by-ransomware, AirGap.com

Defend Against and Respond to Ransomware Attacks, https://www.gartner.com/en/documents/3978727/defend-against-and-respond-to-ransomware-attacks, Gartner Research, 26 décembre 2019

Executive Order on Improving the Nation's Cybersecurity, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, The White House, 12 mai 2021

Siège social aux États-Unis
Cisco Systems, Inc.
San Jose. CA

Siège social en Asie-Pacifique
Cisco Systems (USA) Pad Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam,
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et numéros de télécopieur sont répertoriés sur le site Web de Cisco, à l'adresse **www.cisco.com/go/offices**.

Imprimé aux États-Unis C11-3233828-00 10/22