Livre blanc
Document public

The bridge to possible

Protection contre les ransomwares

Une sécurité Zero Trust pour des modes de travail modernes

Sommaire

The bridge to possible

La fin des ransomwares n'a pas encore sonné

Les ransomwares ont évolué rapidement pour devenir des attaques stratégiques. Autrefois considérés comme une reprise de parc hostile visant des ordinateurs isolés, les enjeux sont aujourd'hui beaucoup plus importants. Les hackers s'en prennent de plus en plus à des cibles géopolitiques, des systèmes d'entreprise essentiels et des infrastructures (par exemple, avec la tactique de la chasse au gros gibier), des actions qui peuvent causer des dommages inédits. Aujourd'hui, les ransomwares représentent l'une des plus grandes menaces en matière de cybersécurité, enregistrant une augmentation de 150 % en 2020 en raison de l'essor du travail à distance.

Les ransomwares sont désormais considérés comme du cyberterrorisme. Par ailleurs, le décret présidentiel récent du président américain, Joe Biden, confirme qu'il est indispensable d'agir pour protéger les systèmes. Une approche Zero Trust est la solution la plus efficace pour se protéger contre les ransomwares. Selon le National Institute of Standards and Technology (NIST), « implémenter une architecture Zero Trust est devenu une obligation de cybersécurité et un impératif professionnel ».

Une fiche d'informations émise par la Maison-Blanche énonce, « Les incidents récents comme ceux qui ont touché SolarWinds, Microsoft Exchange et le Colonial Pipeline nous rappellent tristement que les entités des secteurs public et privé américains font de plus en plus face à une cyberactivité malveillante émanant de hackers et de cybercriminels nationaux. »

> **« Les incidents récents qui ont touché SolarWinds, Microsoft Exchange et Colonial Pipeline nous rappellent tristement que les entités des secteurs public et privé américains font de plus en plus face à une cyberactivité malveillante émanant de cybercriminels et d'états étrangers. »**

Fiche d'informations de la Maison-Blanche, États-Unis d'Amérique.

Qu'est-ce qu'un ransomware ?

Pour faire simple, les ransomwares utilisent diverses tactiques pour cibler des utilisateurs principalement en les infectant avec un malware. On peut citer par exemple les e-mails de phishing, le vol de mots de passe ou les attaques par force brute. Une attaque par ransomware chiffre des fichiers ou des dossiers, empêche l'accès au disque dur et manipule le dossier de démarrage principal pour interrompre le démarrage du système. Lorsque le malware est installé et s'est diffusé, les hackers ont accès à des données sensibles et aux données de sauvegarde, qu'ils chiffrent pour les prendre en otage. Les hackers peuvent agir rapidement ou passer des mois sans être détectés afin d'étudier l'infrastructure de réseau avant de lancer leur attaque.

Le piratage doit créer un sentiment de peur et d'urgence chez les victimes. Celles-ci perdent l'accès à leurs données jusqu'à payer une rançon (principalement en Bitcoins). Même après le paiement, les entreprises n'ont aucune garantie de récupérer toutes leurs données. Il existe de très nombreux variants de ransomwares, mais les cryptoransomwares dominent le marché. En raison de leur polymorphisme (un malware qui change constamment), de nombreux variants parviennent à éviter les systèmes de détection.

Les cryptoransomwares qui verrouillent les données évoluent rapidement. En 2006, les ransomwares utilisaient 56 bits de chiffrement « fait maison ». Aujourd'hui, les versions sophistiquées des ransomwares utilisent des algorithmes symétriques AES et le chiffrement à clés publiques RSA ou ECC pour bloquer les données.

Les ransomwares gagnent en maturité et les hackers s'organisent en entreprises

À mesure que les ransomwares continuent de profiter d'une certaine dynamique, ils gagnent en maturité. Certaines organisations criminelles deviennent de véritables entreprises (principalement situées en Chine, en Russie, en Corée du Nord et en Europe de l'Est) dont l'objectif est d'identifier et de perturber des cibles à haute valeur ajoutée et de soustraire de l'argent en échange des données. Pour plus d'efficacité, ces organisations sont allées jusqu'à mettre en place des centres d'appel pour permettre aux victimes d'acheter des Bitcoins et de payer les rançons. Certaines obtiennent même de bonnes notes pour leurs services clients de la part de leurs victimes.

Pour inciter au paiement, les hackers fournissent un « rapport de sécurité » qui précise de manière détaillée comment ils ont exécuté leur attaque après le versement de la rançon. Même s'ils ont tout intérêt à déchiffrer les fichiers corrompus après avoir reçu l'argent pour inciter leurs prochaines victimes à payer, certains ne le font pas. Selon le rapport Sophos sur l'état des ransomwares en 2021, seuls 8 % des victimes récupèrent leurs données et 29 % n'en récupèrent que la moitié. Les données sont parfois collectées et vendues à d'autres hackers ou conservées pour plus tard.

Ces dernières années, les hackers ont développé le ransomware en tant que service (RaaS), une solution totalement intégrée et prête à l'emploi qui permet à quiconque de déployer une attaque par ransomware sans savoir coder. Tout comme les produits SaaS (logiciels utilisés comme un service), le RaaS offre un accès simple et économique à ces types de programmes malveillants pour un coût inférieur à celui nécessaire pour créer un malware. Les fournisseurs de solutions RaaS réclament généralement 20 à 30 % de la rançon obtenue. Il existe aussi des modèles d'abonnement et de société affiliée pour lancer ce type d'attaque avec succès. Le groupe de hackers REvil avait développé un modèle de société affiliée dans le cadre duquel les bénéfices seraient partagés avec toute personne qui aurait contribué à une attaque fructueuse par ransomware. Ce modèle a généré une hausse considérable du nombre d'attaques par ransomware.

D'abord attribuée au groupe Maze, la double extorsion est une autre tendance en vogue. Les hackers récupèrent des données et menacent de les publier sur le dark web et/ou sur Internet si leurs demandes ne sont pas exaucées. Ils disposent d'une infrastructure intégrée pour gérer ces images de données, d'après le rapport Verizon 2020 sur les analyses des violations de données. La tactique « désigner et blâmer » est désormais populaire dans la plupart des groupes spécialisés dans le ransomware, tout comme le modèle des « pénalités » où le prix augmente au fil du temps.

Comme les entreprises renforcent leur stratégie de sécurité pour protéger leurs ordinateurs et leurs réseaux contre les attaques par ransomware, les hackers cherchent désormais à exploiter les terminaux mobiles. Ceux-ci ont un écran plus petit et ne présentent pas toutes les informations au premier coup d'œil (les e-mails par exemple), ce qui pousse les victimes à cliquer plus facilement sur des liens malveillants. Les attaques IoT (Internet des objets) connaissent également un certain élan, car les ransomwares et les failles de sécurité transforment les périphériques et les objets en points d'entrée pour les outils d'attaque par ransomware. En 2020, les attaques par ransomware ciblant des objets connectés ont augmenté de 109 % aux États-Unis.

Ces facteurs ainsi que certains pays qui servent de refuges aux hackers ont favorisé l'émergence des attaques criminelles par ransomware. Une attaque par ransomware a été lancée avec succès toutes les 10 secondes en 2020 et d'après l'enquête Anomali Harris Poll, un Américain sur cinq en est victime. De plus, le magazine Infosecurity Magazine affirme que la méthode d'attaque de loin la plus prisée « cible le trafic de botnets (28 %), suivie par le cryptomining (21 %), le vol d'informations (16 %), les terminaux mobiles (15 %) et le secteur bancaire (14 %) ». Pour faire face, les entreprises s'efforcent d'investir dans le domaine de la sécurité (150 milliards de dollars en 2021 d'après Gartner).

Les attaques visant des particuliers diminuent, car les hackers se concentrent sur des cibles plus lucratives. Les fournisseurs de services managés signalent une augmentation de 85 % des attaques visant les PME. Les entreprises ainsi que les infrastructures, le secteur de la santé, le secteur public et les usines sont plus ciblés que jamais avec des rançons qui atteignent plusieurs millions en échange de leurs données. Le montant des rançons a doublé l'an dernier, car les hackers visent de plus grandes entreprises. Les attaques ciblant les fournisseurs, les sous-traitants et les logiciels tiers ont également connu un essor considérable. Les entreprises n'avaient d'autre choix que de faire confiance aux solutions de sécurité de ces tiers qui accèdent à leurs systèmes.

L'essor des ransomwares	La première instance connue de ransomware était stockée sur des disquettes, contenant des enquêtes relatives au SIDA ainsi qu'un malware, qui ont été distribuées dans le monde entier en 1989 par le Dr Joseph Popp. Les disquettes chiffraient le système des victimes et leur y interdisaient l'accès jusqu'à ce qu'elles envoient 189 $ à une boîte postale au Panama. Des CD d'appât étaient ensuite distribués lors de la conférence sur le SIDA de l'Organisation Mondiale de la Santé. Le processus de paiement et l'envoi des CD restaient complexes et onéreux.
2006	Les cybercriminels ont commencé à utiliser une méthode plus efficace qui consistait à exploiter le chiffrement à clé publique RSA 660 pour chiffrer les fichiers plus rapidement. Les grands noms de cette période étaient le cheval de Troie Archiveus et GPcode qui utilisaient un e-mail de phishing comme point d'entrée.
2008-2009	De nouveaux logiciels antivirus intégrant un ransomware ont fait leur apparition et des logiciels de sécurité non autorisés utilisaient FileFix Pro pour extorquer de l'argent en échange du déchiffrement.
2010	Le Bitcoin a tout changé. Des dizaines de milliers de variants de ransomwares ont été détectés et des ransomwares qui bloquent des écrans ont été identifiés pour la première fois.
2013	Il existait un quart de million de ransomwares, et Cryptolocker et le Bitcoin sont rapidement devenus les méthodes de paiement principales. Les ransomwares utilisaient un chiffrement RSA 2 048 bits pour faire face aux demandes grandissantes, ce qui s'est révélé lucratif pour les groupes de hackers.
2015	Le cheval de Troie Teslacrypt est né. À cette époque, il existait 4 millions de variants de ransomwares et l'approche RaaS (ransomware en tant que service) a été lancée.
2016	Les ransomwares JavaScript et Locky ont gagné en popularité, Locky infectant 90 000 victimes chaque jour. Les hackers ciblaient de plus grandes entreprises, comme des hôpitaux et des établissements scolaires. Les ransomwares ont enregistré plus de 1 milliard de dollars de bénéfices. Le malware Petya est à l'origine de plus de 10 milliards de dollars de pertes financières.
2017	Le ver WannaCry est apparu cette année-là et a vu naître de très nombreux variants chaque jour pour se répandre rapidement sur plus de 300 000 ordinateurs dans le monde entier via un exploit Microsoft.
2018	Katsuya a fait son apparition. SamSam a bloqué plusieurs services municipaux de la ville d'Atlanta.

2019	REvil, un groupe RaaS privé, a vu le jour en Russie. Ryuk, un ransomware sophistiqué et coûteux qui était intégré dans des pièces jointes malveillantes et des e-mails de phishing, exigeait des versements plus importants que d'autres attaques similaires et a réussi à bloquer tous les principaux journaux américains.
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 8 infections par seconde.
2021	REvil/Sodinokibi, Conti et Lockbit ont durement touché le secteur de la santé. CryptoLocker a extorqué 40 millions de dollars à la principale compagnie d'assurance CNA Financial, ce qui reste à ce jour l'un des plus gros paiements suite à un ransomware. DarkSide est parvenu à attaquer l'entreprise Colonial Pipeline, ce qui représente la plus grande attaque connue publiquement touchant une infrastructure américaine essentielle.

The bridge to possible

Le périmètre s'étend

Comment les ransomwares ont-ils pris une telle ampleur ? Auparavant, le périmètre était un mur fortifié qui gérait les applications et les données centralisées via les pare-feu du réseau privé virtuel (VPN) et des solutions de gestion des terminaux mobiles, à l'instar des douves autour du château « réseau ». Aujourd'hui, les collaborateurs travaillent partout et sur tout type de périphérique (y compris des terminaux mobiles personnels) et les données doivent être accessibles par des applications tierces dans le cloud. Il n'y a plus de douve et les failles se sont multipliées dans le château. Le travail depuis la maison qui s'est répandu en urgence à cause de la pandémie a transformé le périmètre classique en « périmètre logiciel ». En voulant assurer la continuité de l'activité, la sécurité a été reléguée au second plan, ouvrant une brèche pour les hackers et leurs ransomwares.

L'accès à distance

Selon le rapport sur les principales tendances 2021 en matière de sécurité et de risque de Gartner, 64 % des collaborateurs peuvent désormais travailler depuis la maison et deux cinquièmes des collaborateurs le font. Pendant le confinement imposé par la pandémie, la majorité des collaborateurs ont dû travailler à 100 % à distance, tout en utilisant leurs propres périphériques et en accédant à des applications SaaS dans le cloud et on-premise. De nombreuses entreprises ne disposaient pas de l'infrastructure nécessaire pour prendre en charge un tel changement. Aujourd'hui, l'accès à distance est devenu réalité pour tous les collaborateurs. À mesure que les entreprises s'adaptent à ce nouveau fonctionnement, on observe l'apparition d'un modèle hybride combinant les collaborateurs qui travaillent à distance et ceux qui retournent au bureau.

Peter Firstbrook, vice-président et analyste chez Gartner, a déclaré dans un article de blog, « Une nouvelle norme s'impose. Pour préserver la sécurité, toutes les entreprises devront adopter une posture défensive connectée en permanence, tout en clarifiant les risques générés par le travail à distance ».

Les entreprises qui n'ont pas renforcé leur sécurité pour faire face à ce changement ou qui n'ont pas fortifié leur environnement de sécurité interne donnent carte blanche aux hackers. Selon Gartner, 57 % des failles impliquent une négligence de la part des collaborateurs/de tiers. D'après ZDNet, le protocole RDP (Remote Desktop Protocol) est utilisé en priorité par les hackers pour accéder aux ordinateurs Windows et installer des ransomwares et d'autres malwares, suivi par le phishing par e-mail et l'exploitation des bugs du VPN.

Les contraintes du VPN

Le piratage des VPN est la troisième méthode la plus populaire utilisée par les hackers pour s'infiltrer. L'attaque qui a bloqué l'entreprise Colonial Pipeline Company était liée à la compromission d'un seul mot de passe d'un VPN inutilisé. Les VPN peuvent limiter l'accès aux applications on-premise, mais certains accès incohérents aux applications cloud peuvent également engendrer des vulnérabilités. Une fois compromis, les VPN deviennent des portes dérobées d'accès au réseau via lesquelles les hackers peuvent installer des malwares sur les systèmes internes.

Un pare-feu et un VPN à plusieurs couches Zero Trust avec authentification multifacteur bloquent 100 % des robots automatisés, 99 % des attaques par phishing en masse et 90 % des attaques ciblées, d'après une étude Google.

Des terminaux non protégés

Alors qu'un nombre croissant de périphériques se connectent à des réseaux d'entreprises, les périphériques personnels et « fantômes » se multiplient. Parfois, ces périphériques ne sont ni contrôlés ni mis à jour, ce qui peut engendrer des failles non détectées sur des terminaux clés. Les hackers recherchent minutieusement un moyen de s'infiltrer. Les terminaux non protégés, le manque d'informations sur les utilisateurs et les périphériques qui se connectent à votre réseau ou encore l'intégrité d'un périphérique peuvent être à l'origine d'une faille.

Phishing, attaques ciblées et vulnérabilités

Quelles techniques sont utilisées dans les attaques par ransomware ? C'est un processus en plusieurs étapes qui peut être relativement court ou s'étendre sur plusieurs mois pour accéder et chiffrer les données les plus précieuses afin de causer le plus de dommages possible. Selon CSOonline.com, 94 % des malwares sont distribués par e-mail et les attaques par phishing représentent plus de 80 % des incidents. Les mises à jour non corrigées et les vulnérabilités zero-day constituent d'autres points d'entrée. Presque toutes les attaques commencent par le vol d'informations d'authentification.

Les techniques des ransomwares

Technique « Spray and Pray » ou le phishing généralisé

Des agents obtiennent des listes d'adresses e-mail sur le marché noir, puis analysent les informations d'authentification et envoient des e-mails de phishing. Seules quelques informations d'authentification sont nécessaires pour réussir une telle attaque. Ils les obtiennent souvent en envoyant un e-mail contenant une pièce jointe malveillante, en lançant des sites web frauduleux qui semblent légitimes ou en utilisant une fausse identité pour cibler des collaborateurs à haute valeur ajoutée.

Phishing ciblé

Cette attaque coordonnée et ciblée visant un groupe spécifique d'utilisateurs consiste à envoyer des messages personnalisés reposant sur l'ingénierie sociale qui éveillent la curiosité ou la peur, ou promettent une récompense et qui semblent provenir d'une source légitime. Ces e-mails et ces sites web contiennent des malwares utilisés pour voler des informations d'authentification. Les malwares peuvent aussi être diffusés via les réseaux sociaux et les applications de messagerie instantanée.

Force brute

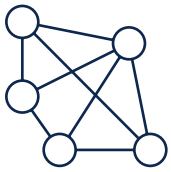
D'après une enquête LastPass, 91 % des personnes interrogées ont confirmé qu'elles réutilisaient des mots de passe. Les hackers en sont conscients et les collectent par le biais du dumping d'informations d'identification ou sur le dark web. Ils se servent ensuite d'outils automatisés pour tester les mots de passe sur différents sites, ce qu'on appelle « credential stuffing » (bourrage d'identifiant) ou force brute. Une fois qu'ils sont infiltrés, l'attaque peut commencer.

Exploitation de vulnérabilités connues

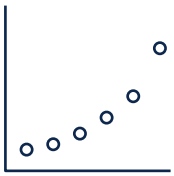
En plus des informations relatives aux périphériques connectés à votre réseau, il est important de connaître l'intégrité du périphérique et le niveau d'application des correctifs et des mises à jour pour assurer une sécurité renforcée. Security Boulevard déclare que « les composants open source obsolètes et abandonnés sont omniprésents. 91 % des bases de code contenaient des composants qui étaient obsolètes depuis plus de quatre ans ou qui n'ont pas été développés au cours des deux dernières années. »

The bridge to possible

Étapes d'une attaque par ransomware



Chiffrement du ransomware	Coordination de l'attaque	Déplacement vertical
En règle générale, les attaques par ransomware chiffrent les données sur les systèmes cibles, vous empêchant d'y accéder jusqu'à ce que vous ayez payé une rançon pour les déchiffrer. La dernière tactique en vogue est le double chiffrement : les hackers chiffrent un système deux fois ou deux groupes différents ciblent la même victime. Cette approche permet aux hackers de collecter deux rançons en exigeant un paiement pour la première couche de chiffrement, puis en surprenant les victimes avec une autre couche une fois la première somme reçue. Le chiffrement le plus fréquent est asymétrique ou symétrique.	À ce stade, les hackers se renseignent sur les entreprises qu'ils ciblent. Ils peuvent acheter des listes d'adresses e-mail sur le dark web, identifier les membres de l'équipe dirigeante, consulter les données financières de l'entreprise, rechercher des profils sur les réseaux sociaux et compiler une liste des principales parties prenantes comme les sous-traitants, les fournisseurs et les partenaires. Quelles sont les tactiques utilisées par les hackers pour s'infiltrer ? Les trois principales attaques en 2020 provenaient de terminaux RDP mal protégés, d'attaques par e-mail de phishing et de l'exploitation de vulnérabilités zero-day du VPN. La compromission des informations d'authentification est la méthode numéro 1 utilisée par les hackers pour s'infiltrer.	Lors de la phase d'infiltration et d'infection, le déplacement vertical correspond au déplacement des cybercriminels depuis un point externe vers un point interne. Une fois infiltrés, ils analysent les fichiers et exécutent du code malveillant sur les terminaux et les périphériques réseau. Le malware se déplace sur tout le système infecté et désactive les pare-feu et les logiciels antivirus. À ce stade, les hackers ont pris le contrôle des données, mais ils ne les ont pas encore chiffrées. Les comptes de messagerie hameçonnés, les serveurs web de niveau inférieur et les terminaux mal protégés sont d'excellents points d'entrée pour des déplacements verticaux.



Infiltration latérale	Exfiltration des données	Paiement et déverrouillage
Les menaces persistantes avancées (APT) se sont largement répandues avec le déplacement latéral. Pour s'infiltrer avec succès, les cybercriminels doivent chiffrer les ordinateurs et répandre le ransomware sur le plus grand nombre de systèmes. Une fois qu'ils ont obtenu un accès, la prospection commence. Ils se déplacent latéralement sur tout le réseau sans être détectés pendant plusieurs semaines ou mois afin d'identifier des cibles clés comme le centre de contrôle-commande, les clés asymétriques et les fichiers de sauvegarde. En parallèle, ils augmentent leurs droits d'accès et leurs autorisations en infectant d'autres systèmes et comptes d'utilisateurs, puis préparent une présence malveillante persistante pour pirater les données. On peut citer les exemples suivants de déplacement latéral : l'exploitation des services distants, le phishing ciblé interne et l'utilisation de mots de passe volés, également connue sous le nom de « pass the hash ».	Au terme de l'inventaire, le chiffrement démarre. Les sauvegardes du système sont effacées, les fichiers et les dossiers locaux sont corrompus, les lecteurs réseau non mappés sont connectés aux systèmes infectés et les communications avec le centre de contrôle-commande visent à générer les clés cryptographiques utilisées sur le système local. Les données du réseau sont copiées localement, chiffrées, puis chargées pour remplacer les données d'origine. Les données exfiltrées peuvent être utilisées pour réaliser une double extorsion. Dans ce cas, une première rançon est exigée pour déchiffrer les données chiffrées, puis une seconde pour ne pas divulguer les données volées.	Les hackers activent ensuite le malware, bloquent les données et envoient leurs demandes de rançon aux sites compromis avec des instructions spécifiques concernant le mode de paiement, généralement à verser en Bitcoins. Un ransomware entraîne des interruptions très coûteuses qui sont extrêmement difficiles à résoudre. Les menaces sont envoyées et le compte à rebours commence. Les entreprises doivent choisir si elles jouent le jeu et paient, si elles essaient de restaurer les fichiers elles-mêmes, ou si elles tirent parti de leur assurance Cybersécurité pour récupérer une partie de la rançon. C'est comme choisir entre la peste et le choléra. C'est pourquoi il est indispensable que les entreprises implémentent une architecture Zero Trust et renforcent leurs bonnes pratiques de sécurité pour éviter de se retrouver dans une telle situation.

Les secteurs vulnérables

La santé, les municipalités et le secteur public, sans oublier le commerce, l'enseignement et le domaine financier, sont les secteurs les plus touchés par les ransomwares. Ces secteurs sont équipés d'anciennes solutions complexes et ne s'appuient pas toujours sur une solution de sécurité cloud robuste. Le secteur public, de la santé et de l'enseignement mettent beaucoup de temps à adapter leur système de sécurité pour y ajouter des mises à jour et de nouvelles technologies, ce qui en fait des cibles faciles et lucratives.

The bridge to possible

Arrêter une attaque par ransomware avant qu'elle démarre

Dans le cadre d'une attaque par ransomware, les hackers doivent d'abord réussir à accéder à votre environnement. Pour ce faire, ils peuvent récupérer des identifiants compromis, comme dans le cas de la faille de Colonial Pipeline.

L'authentification multifacteur (MFA) Duo empêche le ransomware d'accéder à votre système. L'authentification MFA impose à l'utilisateur d'indiquer une combinaison d'au moins deux informations d'authentification pour vérifier son identité avant d'autoriser sa connexion. Par exemple, en plus du nom d'utilisateur et du mot de passe, Duo MFA vous demande quelque chose que vous possédez (comme un périphérique de confiance, un logiciel ou un jeton matériel) avant de vous laisser accéder aux ressources. Grâce à cette exigence supplémentaire de l'authentification MFA, il est beaucoup plus difficile pour le ransomware de s'infiltrer.

Les ransomwares ciblent également les services distants, comme le protocole RDP et les VPN, pour accéder à un réseau. Darkside, l'auteur présumé de l'attaque du Colonial Pipeline, est suspecté d'avoir utilisé l'accès au VPN de l'entreprise pour accéder à l'environnement de la victime. Bien plus qu'une authentification multifacteur, Duo MFA, Duo Device Trust, Duo Network Gateway (DNG) et Duo Trust Monitor forment une solution d'accès fiable qui protège les accès distants à l'infrastructure on-premise et empêche les ransomwares d'accéder à votre environnement.

Duo MFA exige plus qu'un nom d'utilisateur et un mot de passe pour vous authentifier. DNG permet aux utilisateurs d'accéder aux sites web, aux applications web, aux serveurs SSH et à RDP on-premise sans se soucier des informations d'authentification du VPN. Duo Device Trust vérifie que le périphérique qui accède aux ressources à distance est un ordinateur fiable et pas le terminal d'un hacker. Enfin, Duo Trust Monitor attire l'attention sur les demandes d'authentification suspectes, comme celles émanant de pays où les spécialistes du ransomware sont connus pour être actifs et où l'entreprise ne compte aucun collaborateur.

L'utilisation de malwares est aussi une technique populaire d'infection par ransomware. Cisco propose des solutions complémentaires comme Secure Endpoint et Email Gateway, qui inspectent, détectent et bloquent les ransomwares reposant sur un malware avant qu'ils infectent les terminaux.

Comment Duo vous protège-t-il contre les ransomwares ?

Gartner signale que 90 % des ransomwares peuvent être évités. Duo est parfaitement positionné pour aider les entreprises sur trois fronts :

1. Empêcher les ransomwares de s'infiltrer dans un environnement
2. Empêcher ou ralentir la propagation du ransomware s'il parvient à infiltrer une entreprise
3. Protéger les ressources stratégiques et certaines parties de l'entreprise alors que le hacker est toujours présent dans l'environnement jusqu'à remédiation complète

Éviter la propagation

Les ransomwares qui affectent un petit nombre de systèmes ont un impact limité et sont peu susceptibles de paralyser une entreprise et de forcer le paiement d'une rançon. C'est pourquoi la propagation du ransomware est cruciale pour bloquer efficacement une grande partie d'une entreprise et l'obliger à payer pour redémarrer son activité. En 2017, WannaCry et NotPetya ont utilisé l'exploit External Blue pour tirer parti d'une vulnérabilité de Microsoft et se propager sans intervention humaine.

Duo Device Health Application assure l'application de correctifs et de mises à jour sur les périphériques, ce qui complique la propagation automatique des ransomwares. De plus, vous profitez d'une visibilité tout en contrôlant l'intégrité du périphérique, notamment les mises à jour qui lui sont appliquées, à chaque tentative de connexion. Par ailleurs, grâce à la fonctionnalité de remédiation automatique de Duo, les utilisateurs peuvent facilement appliquer des correctifs à leurs périphériques sans l'aide du département IT.

Remédier au problème en toute sécurité

Reprendre l'activité suite à une attaque par ransomware et restaurer les systèmes ne signifie pas nécessairement que le hacker a quitté l'environnement. Il a peut-être essayé de s'établir de manière persistante pour revenir ultérieurement. Pour ce faire, en général les hackers compromettent des comptes existants ou créent de nouveaux comptes, souvent en accédant à Active Directory ou à d'autres répertoires contenant les comptes d'utilisateurs. Avec Duo MFA, ce n'est plus un problème. Si un hacker est toujours présent sur votre réseau, il ne peut pas se déplacer latéralement dans votre environnement à l'aide d'informations d'authentification compromises. Cela vous permet aussi de gagner du temps et d'empêcher un hacker de causer des dommages supplémentaires jusqu'à ce que l'attaque soit totalement éradiquée et que toutes les traces de persistance soient supprimées.

Implémenter un modèle de sécurité Zero Trust

Basé sur le principe suivant « ne jamais faire confiance, toujours vérifier », le modèle Zero Trust aide les entreprises à mettre en œuvre de manière proactive les bonnes pratiques connues pour se protéger contre les cyberattaques, notamment les ransomwares.

Son efficacité est si stratégique que la Maison-Blanche a émis un décret présidentiel imposant spécifiquement une approche Zero Trust et l'authentification MFA.

Duo propose une authentification multifacteur facile à utiliser et à implémenter. Cette solution permet aussi aux entreprises de n'autoriser l'accès que si un utilisateur et son périphérique sont authentifiés et fiables. Cette capacité à contrôler et à gérer les accès est l'un des piliers fondamentaux de l'approche Zero Trust, et Duo MFA est l'une des premières étapes pour implémenter un cadre Zero Trust.

Conclusion

Les ransomwares vont encore prendre de l'ampleur et les entreprises doivent renforcer leur vigilance. L'ingénierie sociale et le phishing ciblé sont efficaces, car ils exploitent la composante humaine du système de sécurité d'une entreprise. Il est important d'adopter et de mettre en œuvre une approche de sécurité Zero Trust qui démarre par une authentification multifacteur forte et une plateforme d'accès fiable pour garder une longueur d'avance sur les attaques par ransomware.

The bridge to possible

Moderniser votre système de défense au-delà de l'authentification multifacteur avec Duo

Les entreprises peuvent se défendre contre l'impact d'un ransomware utilisant l'ingénierie sociale et le phishing ciblé en mettant en œuvre des politiques d'accès conditionnelles qui s'appuient sur des facteurs contextuels, comme l'emplacement et l'état du périphérique, afin de confirmer la fiabilité des utilisateurs et de leurs périphériques.

La plateforme de sécurité cloud Duo protège l'accès à toutes les applications, quels que soient les utilisateurs et les terminaux, et où qu'ils soient. Nous avons simplifié la sécurisation des accès pour gérer les risques liés à l'identité et aux périphériques avec six fonctionnalités essentielles :

1. Vérifier l'identité des utilisateurs avec des méthodes sécurisées et flexibles d'authentification multifacteur.
2. Offrir une expérience de connexion homogène avec l'authentification unique Duo, qui assure un accès centralisé aux applications on-premise et cloud.
3. Assurer une visibilité sur chaque équipement et répertorier en détail tous les appareils qui accèdent aux applications de l'entreprise.
4. Vérifier la fiabilité des périphériques via des contrôles de l'intégrité et de l'état de sécurité des périphériques gérés et non gérés avant d'autoriser un accès aux applications.
5. Mettre en œuvre des politiques d'accès granulaires pour limiter l'accès des utilisateurs et des périphériques qui dépassent les seuils de tolérance au risque de l'entreprise.
6. Surveiller et détecter les connexions risquées avec Duo Trust Monitor ou exporter les journaux d'événements vers votre système SIEM afin de remédier aux événements suspects, comme l'enregistrement d'un nouvel appareil ou une connexion depuis un endroit inattendu.

Pourquoi choisir Duo ?

La rapidité du déploiement de la sécurité

Duo pose les bases d'une approche Zero Trust dans une seule et même solution facile et rapide à déployer pour les utilisateurs. En fonction de l'utilisation spécifique prévue, certains clients peuvent la mettre en place en quelques minutes.

La facilité d'utilisation

Les utilisateurs peuvent s'inscrire eux-mêmes aussi simplement qu'en téléchargeant une application dans l'App Store et en se connectant. Les administrateurs disposent de fonctionnalités de maintenance et de contrôle des politiques simplifiées ainsi que d'une bonne visibilité.

L'intégration avec toutes les applications

Notre produit est conçu pour être indépendant et compatible avec les systèmes déjà en place. Peu importe votre environnement IT et votre fournisseur de solution de sécurité, Duo vous permet de protéger l'accès à toutes les applications professionnelles, quels que soient les utilisateurs et où qu'ils se trouvent.

Un coût total d'acquisition (TCO) réduit

Duo est facile à implémenter et ne vous oblige pas à remplacer vos systèmes ; il exige donc beaucoup moins de ressources en termes de temps et d'argent, ce qui vous permet d'être opérationnel plus rapidement et de commencer votre transition vers un modèle de sécurité Zero Trust.

Références

Le monde a connu une augmentation de 150 % des ransomwares suite à la pandémie, https://cisomag.eccouncil.org/growth-of-ransomware-2020/, CISO Magazine, 5 mars 2021

Exclusif : les États-Unis apparentent les attaques par ransomware à du terrorisme, https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/, Reuters, 3 juin 2021

Le NIST annonce que des collaborateurs technologiques s'attellent à un projet Zero Trust NCCoE, https://www.hstoday.us/industry/emerging-innovation/nist-announces-tech-collaborators-on-nccoe-zero-trust-project/, Homeland Security Today, 24 sept. 2021

FICHE D'INFORMATIONS : des efforts continus du secteur public aux États-Unis pour contrer les ransomwares, https://www.whitehouse.gov/briefingroom/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware, La Maison-Blanche, 13 oct. 2021

Types de chiffrements : symétrique ou asymétrique ? RSA ou AES ?, https://preyproject.com/blog/en/types-ofencryption-symmetric-or-asymmetric-rsa-or-aes/, Prey Project, 15 juin 2021

Ce que nous savons sur DarkSide, le groupe de hackers russes qui a fait des ravages sur la côte Est, https://www.heritage.org/cybersecurity/commentary/what-we-know-about-darkside-the-russian-hackergroup-just-wreaked-havoc, The Heritage Foundation, 20 mai 2021

Ce qu'il faut retenir des « rapports de sécurité » sur les hackers à l'origine des ransomwares, https://www.coveware.com/blog/2021/6/24/what-we-can-learn-from-ransomware-actor-security-reports, Coveware, 24 juin 2021

L'état des ransomwares en 2021, https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx, Sophos, 2021

Le processus de datamining : la différence entre datamining et collecte de données, https://www.import.io/post/the-difference-between-data-mining-data-harvesting, Import.io, 23 avril 2019

Ransomware : un ennemi à votre porte, https://ussignal.com/blog/ransomware-enemy-at-the-gate, US Signal, 3 septembre 2021

Rapport d'enquête sur les violations de données en 2020, https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf, Verizon, 2020

Les malwares reculent, mais les attaques par ransomware et visant les objets connectés sont en hausse, https://www.techrepublic.com/article/malwareis-down-but-iot-and-ransomware-attacks-are-up/, Tech Republic, 23 juin 2020

Une victime d'attaque par ransomware toutes les 10 secondes en 2020, https://www.infosecurity-magazine.com/news/oneransomware-victim-every-10/, Infosecurity Magazine, 25 février 2021

Des statistiques terrifiantes : 1 Américain sur 5 victime d'un ransomware, https://sensorstechforum.com/1-5-americansvictim-ransomware/, Sensors Tech Forum, 19 août 2019

Gartner estime que les dépenses consacrées à la gestion de la sécurité et des risques dans le monde entier devraient dépasser 150 milliards de dollars en 2021, https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem, Gartner, 17 mai 2021

1 PME sur 5 a été victime d'une attaque par ransomware, https://www.helpnetsecurity.com/2019/10/17/smbsransomware-attack/, Help Net Security, 17 octobre 2019

Les ransomwares, principale cause des interruptions : comment arrêter leur essor ?, https://polyverse.com/blog/ransomware-how-to-stop-this-growing-major-cause-of-downtime, Polyverse.com

L'étrange histoire des ransomwares, https://theworld.org/stories/2017-05-17/strange-history-ransomware, PRI The World, 17 mai 2017

La chronologie des ransomwares, https://www.tcdi.com/ransomware-timeline, tcdi.com, 27 décembre 2017

L'histoire d'une attaque par ransomware : la plus importante et la pire attaque par ransomware de tous les temps, https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time, Digital Guardian, 2 décembre 2020

L'une des plus grandes compagnies d'assurance américaines a déclaré avoir payé une rançon de 40 millions de dollars après une cyberattaque, https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5, Business Insider, 22 mai 2021

Atlanta a dépensé 2,6 millions de dollars suite à l'attaque d'un ransomware réclamant 52 000 $, https://www.wired.com/story/atlantaspent-26m-recover-from-ransomware-scare, Wired.com, 23 avril 2018

Cyberattaque : les États-Unis et le Royaume-Uni accusent la Corée du Nord d'être à l'origine du ver WannaCry, https://www.bbc.com/news/world-uscanada-42407488, BBC.com, 19 sept. 2017

Ransomwares : une activité criminelle en plein essor pesant déjà un milliard de dollars par an, https://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646, NBCNews.com, 9 janvier 2017

L'histoire méconnue de NotPetya, la cyberattaque la plus dévastatrice de l'histoire, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world, Wired.com, 22 août 2018

Les ransomwares dans le secteur de la santé : l'avenir, c'est maintenant, https://mds.marshall.edu/cgi/viewcontent.cgi?article=1185&context=mgmt_faculty, Marshall University Digital Scholar, automne 2017

Un nouveau ransomware tient en otage des fichiers Windows et réclame 50 $, https://www.networkworld.com/article/2265963/new-ransomware-holds-windows-files-hostage--demands--50.html, NetworkWorld.com, 26 mars 2009

Empêcher les extorsions numériques, https://subscription.packtpub.com/book/networking_and_servers/9781787120365/4/ch04lvl1sec24/the-advancement-of-locker-ransomware-winlock, PackIt, mai 2017

Les effets irréversibles d'une attaque par ransomware, https://www.crowdstrike.com/blog/irreversible-effectsransomware-attack, CrowdStrike, 20 juillet 2016

La nouvelle ère du travail à distance exige une approche de sécurité moderne, d'après une enquête de Thales menée auprès de responsables IT du monde entier, 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 sept. 2021

Le FBI observe un pic de cybercrimes pendant la pandémie de coronavirus, https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic, The Hill, 16 avril 2020

Synthèse de Symantec Security – Septembre 2021, https://symantec-enterprise-blogs.security.com/blogs/featurestories/symantec-security-summary-september-2021, Symantec Security, 27 sept. 2021

Un rapport d'INTERPOL constate un nombre alarmant de cyberattaques pendant la pandémie de 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

Rapport sur les principales tendances 2021 en matière de sécurité et de risque de Gartner, https://www.gartner.com/smarterwithgartner/gartner-topsecurity-and-risk-trends-for-2021, Gartner, 5 avril 2021

Une enquête de Gartner révèle que 82 % des dirigeants d'entreprises envisagent d'autoriser leurs collaborateurs à travailler partiellement à distance, 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 identifie la sécurité basée en priorité sur les identités comme une tendance de sécurité majeure en 2021, https://www.attivonetworks.com/blogs/gartner-identity-first-security-in-2021, Attivo, 27 avril 2021.

Rapport 2021 de SonicWall sur les cybermenaces, https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyberthreat-report.pdf, SonicWall, 2021

Les principaux exploits utilisés par les groupes spécialisés dans les ransomwares sont les bugs des VPN, mais le protocole RDP règne toujours en maître, https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme, ZDNet.com, 23 août 2020

L'exploitation des VPN a augmenté en 2020, les entreprises corrigent trop lentement les failles majeures, https://www.cybersecuritydive.com/news/trustwave-network-security-remote-access/602044/, Cybersecurity Dive, 18 juin 2021

Nouvelle étude : l'efficacité d'une sécurité basique des comptes pour empêcher le piratage, https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html, Blog Google, 17 mai 2019

Principaux faits, statistiques et tendances concernant la cybersécurité, https://www.csoonline.com/article/3634869/top-cybersecuritystatistics-trends-and-facts.html, CSOonline.com, 7 octobre 2021

Protéger les entreprises contre les cyberattaques, https://www.inc.com/knowbe4/protecting-companies-fromcyberattacks.html, Inc.com, 20 septembre 2021

ThreatList : tout le monde sait qu'il ne faut pas réutiliser des mots de passe, mais tout le monde le fait, https://threatpost.com/threatlistpeople-know-reusing-passwords-is-dumb-but-still-do-it/155996/, Threatpost, 25 mai 2020

Une étude Synopsys révèle que 91 % des applications commerciales contiennent des composants open source obsolètes ou abandonnés, https://www.securitymagazine.com/articles/92368-synopsys-study-shows-91-ofcommercial-applications-contain-outdated-or-abandoned-open-source-components, Security Magazine, 12 mai 2020

Une nouvelle tendance dangereuse en matière de ransomware : le double chiffrement de vos données, https://www.wired.com/story/ransomware-double-encryption/, Wired.com, 17 mai 2021

Éradiquer les déplacements latéraux et lutter contre la hausse des ransomwares, https://www.msspalert.com/cybersecurityguests/combating-lateral-movement-and-the-rise-of-ransomware, MSSP Alert, 24 juin 2021

Les déplacements latéraux, https://attack.mitre.org/tactics/TA0008/, MITRE| ATT&CK, 17 octobre 2019

Les secteurs touchés par les ransomwares, https://airgap.io/blog/industries-impacted-by-ransomware, AirGap.com

Se protéger contre les attaques par ransomware et riposter, https://www.gartner.com/en/documents/3978727/defend-against-and-respond-to-ransomware-attacks, Étude Gartner, 26 décembre 2019

Un décret présidentiel pour améliorer la cybersécurité nationale, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, La Maison-Blanche. 12 mai 2021