

PRÉSENTATION

Scam : pourquoi la messagerie est le premier vecteur de menaces

Aujourd'hui, la plupart des fuites meurtrières commencent encore par un simple e-mail.

Résumé

Le phishing, ce n'est pas seulement vous amener à cliquer sur un lien pour lancer un logiciel malveillant. Cette pratique bien plus insidieuse cherche en réalité à vous dérober les identifiants de super utilisateurs. Cela permet aux agresseurs d'accéder à la messagerie, d'envoyer des e-mails, d'effectuer des requêtes financières et de diffuser du code malveillant partout où l'identité de l'utilisateur possède une autorisation.

La messagerie reste un vecteur de choix pour les menaces. Les entreprises doivent donc rester vigilantes pour protéger leurs collaborateurs contre les attaques avancées de phishing et les logiciels malveillants, notamment de type BEC (Business Email Compromise), les usurpations d'identité et la fraude.

Introduction

Près de 320 milliards d'e-mails sont envoyés chaque jour. La messagerie reste le principal outil de partage d'informations, et par là-même de menaces. Le COVID-19 et le développement du télétravail ont contribué au fait que la messagerie constitue le canal le plus fréquenté pour toutes les formes d'attaques de phishing et par ransomware.

Suite aux précédentes fuites de données majeures, nous avons compris que les attaques avancées employaient souvent de multiples tactiques, techniques et procédures pour compromettre les données de l'utilisateur. Habituellement, la messagerie constitue le point de départ des attaques d'ingénierie sociale, par exemple les attaques de type BEC ou le phishing ciblant les identifiants.

Par exemple, le 2020 Data Breach Report de Verizon indique que 22 % des fuites impliquent l'ingénierie sociale, dont 96 % ont été véhiculées par e-mail. Dans le même rapport, toujours 22 % des fuites résultent d'une défaillance humaine, à savoir l'envoi involontaire de données sensibles au mauvais destinataire.

Une autre étude menée par 451 Research a révélé que 87 % des entreprises ont déjà déployé un produit de sécurisation de messagerie mais que 46 % d'entre elles admettent que les e-mails représentent encore le risque le plus important. Parmi ces entreprises, 46 % indiquent que la messagerie est leur élément de vulnérabilité le plus marqué, près de cinq fois plus que les autres éléments d'inquiétude majeurs.

Microsoft et Google dominent le marché mondial de la messagerie cloud, avec des offres étendues de suite bureautique. Microsot et Google se partagent les parts du marché mondial des technologies de suite bureautique. Dans le monde, Gmail est la plateforrme de messagerie la plus populaire avec plus de 1,8 milliards d'utilisateurs. Fin 2020, Microsoft Office 365 était utilisé par plus d'1 million d'entreprises dans le monde, dont plus de 650 000 aux États-Unis seulement.

Attirés par tant de victimes potentielles, les agresseurs investissent constamment dans de nouvelles cibles de scam, à savoir les utilisateurs de ces services de messagerie cloud. La messagerie cloud est ainsi l'un des vecteurs d'attaque les plus alléchants et les plus lucratifs pour les pirates opportunistes.



Efficacité persistante du phishing et des e-mails frauduleux

La manière dont sont élaborés les e-mails de phishing pour ressembler à de véritables e-mails envoyés à partir de fausses identités ou d'identités dérobées et connues peut duper tous les utilisateurs, même les plus aguerris et les plus avertis en matière de sécurité. Malgré les efforts d'éducation en matière de sécurité, les attaques de phishing sont encore souvent citées comme étant le maillon faible dans ce domaine. D'après les leaders de la sécurité avec lesquels nous nous sommes entretenus, certains utilisateurs cliquent encore sur des e-mails de phishing ciblés et basés sur des thèmes ou des événements, qui ont été personnalisés pour imiter des e-mails légitimes. Ils sont nombreux à ne pas savoir distinguer e-mails légitimes ou faux e-mails, reconnaître les liens suspects ou prendre des mesures de précaution, notamment

authentifier l'URL, l'identité de l'expéditeur et le site Web de l'entreprise.

S'y ajoute le fait que le phénomène de propagation n'échappe pas à la nature humaine. Les e-mails et les pièces jointes échangés entre collaborateurs, partenaires et clients, voire avec la famille et les amis, font partie du quotidien d'un personnel qui travaille aujourd'hui en collaboration et à distance. Nous les acceptons parce qu'il s'agit d'identités auxquelles nous faisons confiance et parce que nous avons besoin d'accéder à leurs contenus pour mener à bien notre travail collectif.

Business Email Compromise

Les attaques de type BEC se trouvent en tête de liste des attaques par usurpation d'identité et des fraudes. Elles impliquent généralement l'utilisation d'un compte de messagerie compromis appartenant au PDG ou à un autre dirigeant. Les escrocs utilisent le compte compromis pour envoyer des demandes frauduleuses d'ordre financier, par exemple le paiement d'une fausse facture ou le transfert d'argent pour clôturer une affaire douteuse.

Dans la plupart des cas, des attaques d'ingénierie sociale ou le whaling sont à l'origine du piratage de comptes de cadres supérieurs. L'IC3 (Internet Crime Complaint Center du FBI) indique que la cybercriminalité a dépassé 4,1 milliards de dollars US en 2020, les attaques BEC, vecteur de menace unique représentant 1,8 milliards, étant à l'origine des dommages financiers les plus importants.

Lorsque vous vous rendez compte que les identifiants d'un responsable ont été compromis, il est déjà trop tard. Il suffit d'un seul compte compromis pour enclencher une réaction virale d'un utilisateur à un autre, d'un appareil à un autre et d'une d'application à une autre. Il ne sera peut-être pas possible de contenir cette réaction avant la survenue des dommages.

La sécurité cloud native ne suffit pas

Les développeurs de solutions de sécurité de messagerie ont créé des outils permettant de protéger les utilisateurs contre les liens malveillants qui contournent les filtres de pré-livraison et parviennent jusqu'à la boîte de réception, notamment la protection via l'heure du clic, le retrait après livraison et les filtres de navigateur Web. Les attaquants sont toutefois tout aussi déterminés à trouver les moyens d'atteindre la boîte de réception.

Selon le récent rapport 2020 sur Microsoft ATP, plus d'un e-mail de phishing ciblé sur dix peut atteindre la boîte de réception de l'utilisateur. Chaque attaque unique exploite diverses combinaisons de méthodes d'obscurcissement conçues explicitement pour contourner les mesures EOP (Exchange Online Protection) et ATP (Advanced Threat Protection) de Microsoft.

Certaines attaques étendues exploitant les e-mails contournent très aisément les filtres de sécurité. Il peut s'agir par exemple d'un e-mail de phishing ciblé, peu volumineux et de qualité, qui semble provenir d'Office 365 ou de Gmail. Son apparence est correcte, il est personnalisé et envoyé à un ensemble spécifique d'utilisateurs plutôt que via une campagne classique de masse. Ces attaques sont sophistiquées tant du côté de la technique permettant d'atteindre la boîte de réception que de l'expérience utilisateur en back-end. Chaque lien comprend généralement l'adresse e-mail de l'utilisateur ; la page de connexion ressemble donc à la deuxième page du compte visé lorsque vous essayez d'aller sur une page d'administration lors de la connexion. Il sait qui vous êtes et nourrit des analyses en backside.

La courbe d'innovation du phishing se manifeste désormais après la livraison. Autrement dit, au lieu de placer l'URL malveillante dans l'e-mail, les phishers renvoient vers un serveur de redirection qui agit comme une passerelle et envoie les requêtes d'une société de sécurité vers un site inoffensif. En revanche, les requêtes des victimes visées sont dirigées vers le serveur de phishing.

Même si Microsoft ATP applique quatre moteurs de stratégie principaux pour l'anti-phishing, les renseignements sur l'usurpation d'identité, les liens approuvés (Safe Links) et les pièces jointes approuvées (Safe Attachments), il s'agit toujours d'une technologie de sécurité basée sur des règles. L'analyse de sécurité repose uniquement sur un filtrage statique basé sur la réputation, que les pirates peuvent soumettre à rétro-ingénierie jusqu'à ce qu'ils trouvent des moyens de contourner ces filtres. En raison de cette faiblesse de la couche de sécurité, les entreprises subissent des risques permanents : la probabilité plane qu'un collaborateur ouvre le mauvais fichier, clique sur la mauvaise URL ou saisisse un mot de passe au mauvais endroit.

La grande majorité des utilisateurs de messagerie cloud étant visible et accessible, ils constituent des cibles faciles pour tous les pirates. Ils n'ont jamais donné autant de comptes utilisateurs et de boîtes aux lettres avec des règles de sécurité identiques. Pour diffuser des logiciels malveillants ou dérober des données, les pirates profitent également du fait que ces comptes cloud sont des sources d'authentification pour d'autres applications SaaS d'entreprise. C'est là que réside actuellement le réel danger de la monoculture de la sécurité cloud. Celui qui parvient à contourner une fois, contournera mille fois.

SiteCloak constitue un bon exemple de cette technique actuellement utilisée pour contourner les liens approuvés ATP de Microsoft 365, également connue sous le nom de protection via l'heure du clic. Cette technique fait passer l'obscurcissement du phishing au niveau supérieur par le biais de diverses tactiques et techniques permettant de masquer la véritable intention de la page cible, qui est souvent une page de recueil d'identifiants.

Les victimes de SiteCloak n'ont pas besoin de saisir leur adresse e-mail. Elles sont directement dirigées vers la page de saisie du mot de passe, où la page de recueil des identifiants utilise la technique « Zero Font » pour contourner les analyseurs de messagerie Microsoft. Il place entre les caractères de la page des caractères aléatoires, d'une taille de police égale à zéro, de sorte que les filtres de langage naturel de Microsoft voient le texte aléatoire tandis que l'œil humain voit ce que les attaquants veulent qu'ils voient. Autrement dit, Safe Links pense qu'il s'agit d'une page inoffensive alors que la victime voit une page de recueil d'identifiants parfaitement crédible. Les attaquants activent le contenu malveillant seulement lorsque l'e-mail a atteint la boîte de réception.

Conclusions

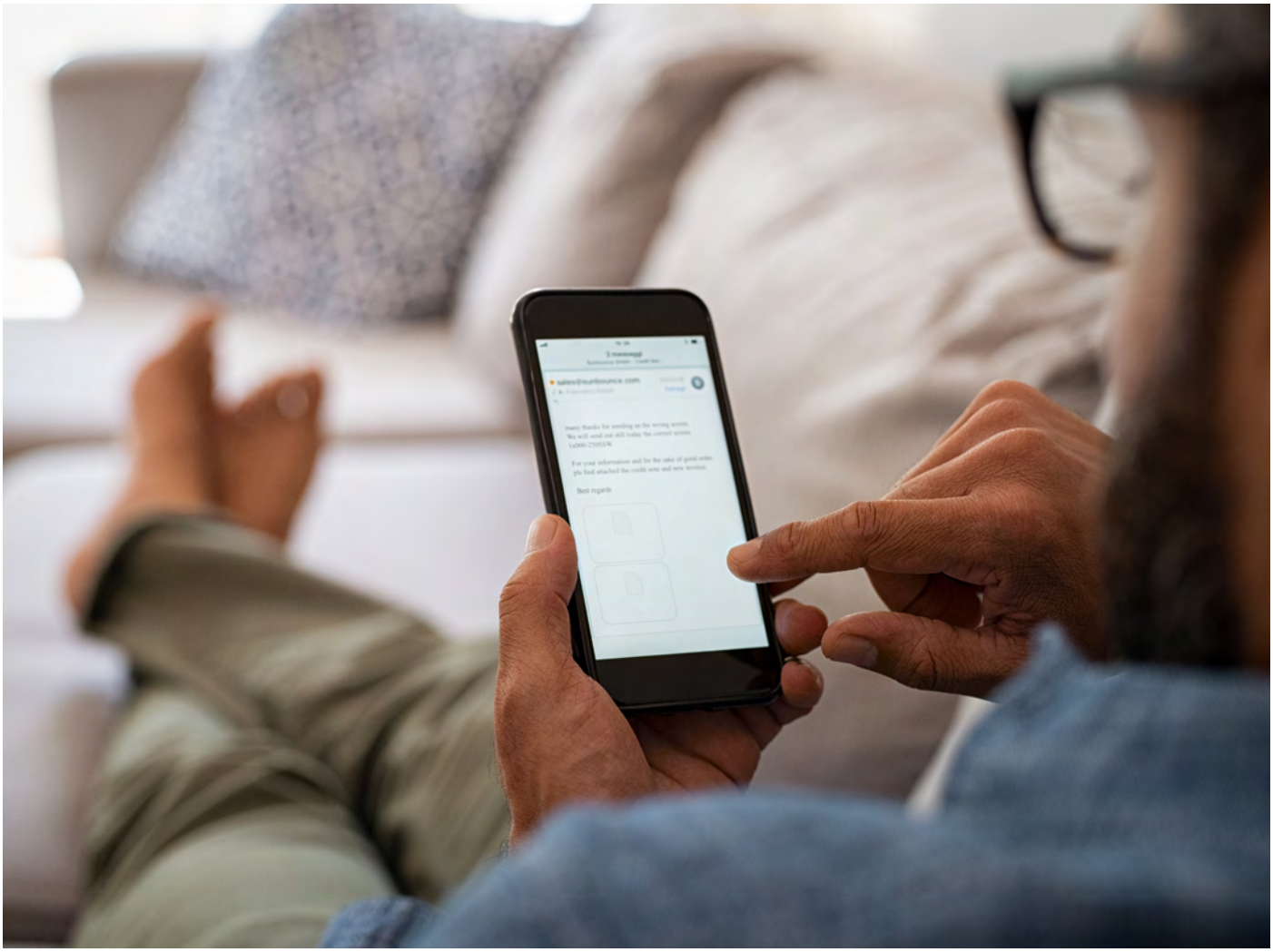
SiteCloak et d'autres formes de fraude par messagerie montrent que les pirates peuvent échapper à toute détection par le biais d'attaques de phishing personnalisées très bien conçues et parfaitement préparées. Elles ne seront pas les dernières à échapper aux filtres de sécurité des fournisseurs de services cloud. Les entreprises ont besoin de niveaux de protection supplémentaires, supérieurs aux niveaux de sécurité intégrés au système bureautique cloud.

SonicWall Email Security peut être déployée sous forme d'appliance virtuelle robuste, d'application logicielle, de service hébergé ou d'appliance physique renforcée, ce qui est idéal pour les entreprises à la recherche d'une solution dédiée sur site. La solution multicouche de SonicWall offre une protection complète des messages entrants et sortants. Elle protège contre les menaces avancées véhiculées par la messagerie, notamment les ransomwares, les menaces de type « zero-day », le spear phishing et les attaques de type BEC (Business Email Compromise).

Plus d'infos sur www.sonicwall.com/email-security.

À propos de SonicWall

SonicWall offre une solution de cybersécurité sans limites pour l'ère de l'hyper-distribution dans une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. En connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant de véritables économies, SonicWall comble le fossé commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour plus d'informations, rendez-vous sur www.sonicwall.com.



SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

© 2021 SonicWall Inc. TOUS DROITS RÉSERVÉS.

SonicWall est une marque commerciale ou déposée de SonicWall Inc. et/ou de ses filiales aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales et déposées sont la propriété de leurs sociétés respectives. Les informations contenues dans ce document sont fournies en relation avec les produits de SonicWall et/ou ses filiales. Aucune licence, expresse ou implicite, par estoppel ou un autre moyen, quant à un quelconque droit de propriété intellectuelle n'est accordée par le présent document ou en lien avec la vente de produits SonicWall. SAUF DISPOSITION CONTRAIRE DANS LES CONDITIONS DU CONTRAT DE LICENCE, LA SOCIÉTÉ SONICWALL ET/OU SES FILIALES DÉCLINENT TOUTE RESPONSABILITÉ QUELLE QU'ELLE SOIT ET REJETTENT TOUTE GARANTIE EXPRESSE, IMPLICITE OU STATUTAIRE CONCERNANT LEURS PRODUITS, Y COMPRIS ET SANS S'Y LIMITER, LES GARANTIES IMPLICITES DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER OU DE NON-CONTREFAÇON. EN AUCUN CAS, SONICWALL OU SES FILIALES NE SERONT RESPONSABLES DES DOMMAGES DIRECTS, INDIRECTS, CONSÉCUTIFS, PUNITIFS, SPÉCIAUX OU FORTUITS (Y COMPRIS, SANS LIMITATION, LES DOMMAGES POUR PERTE DE PROFITS, INTERRUPTION DE L'ACTIVITÉ OU PERTE D'INFORMATIONS) PROVENANT DE L'UTILISATION OU L'IMPOSSIBILITÉ D'UTILISER CE DOCUMENT, MÊME SI SONICWALL ET/OU SES FILIALES ONT ÉTÉ INFORMÉS DE L'ÉVENTUALITÉ DE TELS DOMMAGES. SonicWall et/ou ses filiales ne font aucune déclaration ou ne donnent aucune garantie en ce qui concerne l'exactitude ou l'exhaustivité du contenu de ce document et se réservent le droit d'effectuer des changements quant aux spécifications et descriptions des produits à tout moment sans préavis. SonicWall Inc. et/ou ses filiales ne s'engagent en aucune mesure à mettre à jour les informations contenues dans le présent document.

ExecBrief-EmailThreatVector-A4-COG-5264