LIVRE BLANC

L'hameçonnage ne se limite plus aux e-mails : il s'étend aux réseaux sociaux

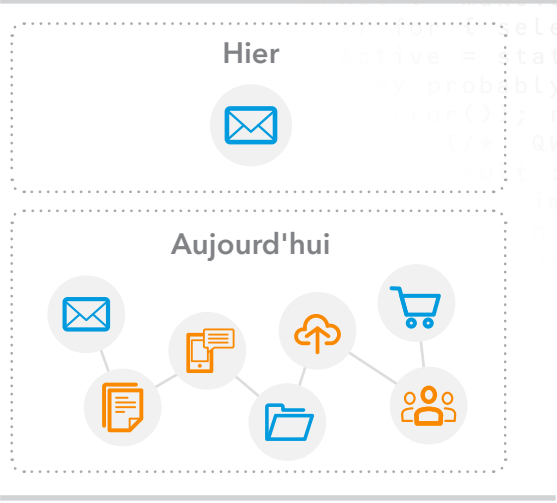
Akamai

Résumé

Malgré des années de publicité et des millions de dollars investis dans la formation des employés, l'hameçonnage demeure la plus grande menace pour les entreprises[1]. Jusqu'à 93 % des violations de sécurité informatique sont le résultat direct d'une forme d'hameçonnage[2] et 34 % de toutes les attaques d'hameçonnage ciblent explicitement les entreprises[3]. Chaque jour, les employés donnent sans le savoir des informations personnelles et professionnelles à des personnes malveillantes.

Et aujourd'hui, les pirates élargissent leurs filets.

Les criminels ne se limitent plus à la messagerie électronique : ils exploitent les réseaux sociaux, les applications de messagerie instantanée et les services de partage de fichiers en ligne les plus répandus. Facebook, Slack, Microsoft Teams, Dropbox, Google Docs et d'autres plateformes populaires servent de porte d'entrée aux criminels pour infiltrer l'entreprise. Ces canaux sont beaucoup plus personnels ; ils invitent au partage et à la diffusion à grande échelle, si bien que l'hameçonnage peut se propager de manière exponentielle.



Un seul ensemble d'identifiants volés suffit à un criminel pour accéder au réseau de l'entreprise, où il peut ensuite se déplacer latéralement pour trouver et extraire les joyaux de la couronne d'une entreprise.

Les contrôles de sécurité traditionnels de l'entreprise ont une capacité limitée à atténuer ces risques. Les employés sont mobiles et dispersés. Ils peuvent accéder à leurs comptes de messagerie et de réseaux sociaux personnels à partir de leurs terminaux professionnels, avec une surveillance minime par les services informatiques. Et lorsqu'ils accèdent à des applications sociales sur des terminaux mobiles, ils se trouvent en dehors de la sphère de gouvernance de l'entreprise.

Malheureusement, une simple vigilance ne peut pas faire grand-chose. Dès que les professionnels de la sécurité déjouent un type d'attaque d'hameçonnage, un autre se présente. C'est un jeu du chat et de la souris, où les criminels sont avertis, patients et précis. Ils recherchent constamment des moyens de déjouer les défenses de sécurité existantes des entreprises.

Pire encore, les personnes malveillantes peuvent facilement acheter des kits d'hameçonnage prêts à l'emploi sur des sites clandestins. Ces kits d'outils offrent aux escrocs tout ce dont ils ont besoin pour créer rapidement de fausses pages Web et lancer des campagnes malveillantes par e-mail et via les réseaux sociaux, le tout dans une optique d'infiltration des entreprises.

De plus en plus d'e-mails d'hameçonnage passent aussi par les systèmes de sécurité des messageries d'entreprise[4]. Bien que la plupart des entreprises actuelles disposent probablement de protections en place, ces passerelles et ces filtres sont loin d'être parfaits. Quelle que soit leur efficacité, il n'est pas recommandé de se fier à une seule couche de défense contre de telles attaques.

Face à ces défis, les entreprises d'aujourd'hui ont besoin d'une nouvelle approche de la sécurité d'entreprise. À savoir, une mentalité Zero Trust : ne se fier à rien, vérifier tout, maintenir des contrôles constants. Chaque demande d'accès doit être authentifiée et autorisée, puis accordée uniquement de façon temporaire.

Une protection avancée, basée sur le cloud et en temps réel contre les menaces est essentielle à cette transformation de la sécurité. Elle permettra à l'entreprise de suivre le rythme de l'évolution de l'écosystème actuel des menaces, y compris les phénomènes d'hameçonnage social que nous explorons dans ce livre blanc.

L'impact de l'hameçonnage sur les entreprises

Partout dans le monde, des entreprises signalent que les stratagèmes d'hameçonnage constituent la principale source de violations de sécurité des entreprises. Jusqu'à 93 % sont le résultat direct d'une forme d'hameçonnage[5].

La présence et l'efficacité de l'hameçonnage sont stupéfiantes :

- *Un e-mail sur 99 est une attaque d'hameçonnage, utilisant des pièces jointes et des liens malveillants comme vecteur principal[6]*
- *52 % des attaques par e-mail réussies parviennent à faire cliquer leurs victimes en moins d'une heure, et 30 % en moins de 10 minutes[7]*
- *Près de 1,5 million de nouveaux sites d'hameçonnage sont créés chaque mois[8]*
- *83 % des professionnels de la sécurité de l'information ont été victimes d'attaques d'hameçonnage en 2018[9]*

Cela ne devrait surprendre personne. Il est beaucoup plus facile pour un cybercriminel de se connecter au réseau d'une entreprise avec les informations volées d'un employé que de la pirater. Il suffit d'un seul ensemble d'identifiants compromis pour qu'un pirate puisse entrer et s'implanter. Cette infiltration initiale entraîne rapidement un mouvement latéral, l'identification des ressources les plus précieuses et l'exfiltration finale.

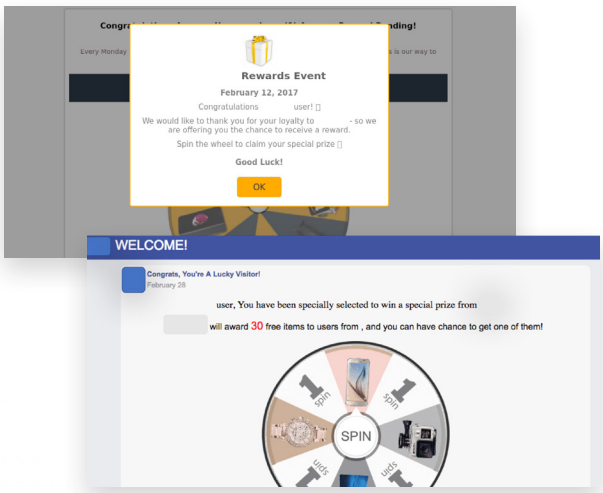
Et l'impact est considérable :

- *Le coût moyen d'une attaque d'hameçonnage pour une entreprise de taille moyenne est de 1,6 million de dollars[10]*
- *1 client sur 3 cessera de faire affaire avec une entreprise qui subit une atteinte à la cybersécurité[11]*

Hameçonnage social : lancement d'un filet plus large

Les réseaux sociaux, les applications de messagerie et les services de partage de fichiers dépendent tous d'un certain niveau de confiance. Cela fait des réseaux sociaux des vecteurs d'attaque idéaux. Les personnes malveillantes tirent parti de la communauté et de la confiance perçue de ces plateformes, incitant les utilisateurs à diffuser du contenu malveillant. Le nombre d'escroqueries par hameçonnage sur les réseaux sociaux a augmenté de plus de 70 % au cours du premier trimestre 2019[12].

Une pratique courante dans le cycle de vie d'une escroquerie par hameçonnage consiste à inclure une étape où la victime doit partager un lien (l'URL du site Web frauduleux ou compromis) sur ses réseaux sociaux. Comme le lien vient d'un contact connu ou de bonne réputation, les relations sociales de la victime deviennent rapidement des proies de l'opération. Et la confiance mal placée dans une cyberdestination dangereuse se propage.



Les faux concours et prix sont des leurres courants.

Dans son livre blanc intitulé « A New Era in Phishing: Games, Social, and Prizes », Or Katz, security researcher chez Akamai, a étudié la manière dont les campagnes d'hameçonnage social tirent parti des concours et des récompenses pour diffuser des liens malveillants[13]. De fausses récompenses et promotions déguisées en occasions légitimes incitent davantage à la diffusion, créant des environnements qui poussent les victimes à divulguer des informations personnelles et professionnelles.

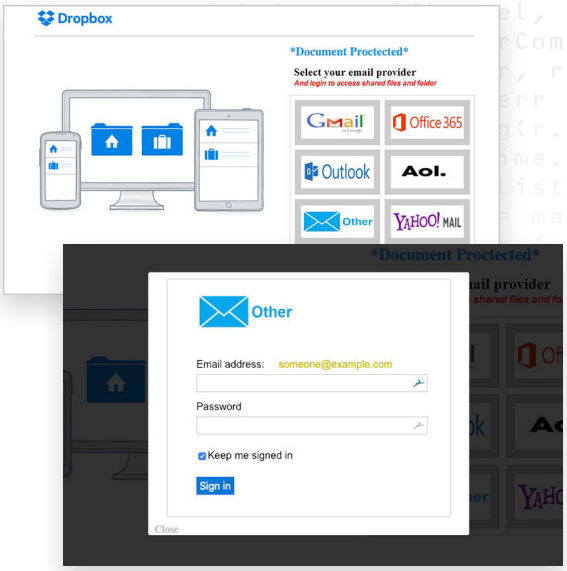
Avec l'augmentation du nombre et de la popularité des comptes de réseaux sociaux, les cybercriminels ont de plus en plus de moyens d'atteindre les victimes.

Forbes signale que les criminels utilisent désormais des services de messagerie instantanée tels que Slack, Skype, Microsoft Teams et Facebook Messenger pour cibler de nouvelles victimes et intensifier leurs campagnes[14]. Ces stratagèmes axés sur les réseaux sociaux utilisent de nombreuses méthodes semblables à l'hameçonnage par e-mail : usurpation d'identité, exploitation de la confiance implicite et liens malveillants. La différence, c'est qu'ils sont transmis par l'entremise de ces plateformes de communication de nouvelle génération.

Selon CSO, les personnes malveillantes organisent de plus en plus d'attaques d'hameçonnage via des outils de partage de fichiers et de collaboration en ligne, tels que Microsoft OneDrive, Google Docs, SharePoint, WeTransfer, Dropbox et ShareFile[15]. Parfois, les fichiers contiennent un programme malveillant. Parfois, ils font partie d'un plan d'hameçonnage plus vaste visant à transporter et à héberger des images, des documents et autres ressources qui pourraient contribuer à légitimer le stratagème auprès de ses cibles et des analyses de messagerie d'entreprise.

Les utilisateurs fictifs des réseaux sociaux ajoutent un autre élément à ces attaques. Ils apparaissent sur un site Web sous la forme d'un plug-in intégré pour les réseaux sociaux, fournissant souvent des témoignages. La cible est en fait en train de visionner du code JavaScript intégré sur un site d'hameçonnage usurpé qui présente des comptes de réseaux sociaux générés préalablement. Ces fausses personnes deviennent la preuve que d'autres ont gagné des prix (inexistants). Cela encourage la participation et permet de promouvoir le stratagème.

Les campagnes d'hameçonnage social lancées spécifiquement via des terminaux mobiles sont particulièrement difficiles à contrer. En plus des failles de sécurité reconnues des terminaux mobiles, l'interface utilisateur mobile n'est pas suffisamment détaillée pour identifier les attaques d'hameçonnage. Par exemple, elle n'inclut pas le survol d'hyperliens pour indiquer la destination. Par conséquent, les utilisateurs mobiles sont trois fois plus susceptibles de tomber dans le piège de l'hameçonnage[16].



Les outils commerciaux légitimes sont de plus en plus exploités.

Les pirates continuent d'améliorer les tactiques d'hameçonnage

Les criminels d'aujourd'hui sont persévérants et utilisent des activités variées et ciblées pour contourner les défenses de sécurité des entreprises. Se protéger contre leurs campagnes d'hameçonnage est une course aux armements en constante évolution. Dès que les agents de sécurité déjouent une agression, les pirates adaptent leur technique.

Voici un exemple récent : des pirates ont trouvé une vulnérabilité qui leur a permis de contourner les protocoles de sécurité de messagerie existants de Microsoft Office 365. Ils ont masqué l'URL d'hameçonnage en y intégrant des caractères sans chasse. Les e-mails compromis ont ainsi pu échapper à la vérification de la réputation des URL de Microsoft et à la protection des URL des liens sécurisés[17]. Les utilisateurs ont reçu l'e-mail avec le lien d'hameçonnage intact, au lieu du lien hébergé par Microsoft qui aurait dû le remplacer.

Dans son récent rapport *Phishing Activity Trends*, l'Anti-Phishing Working Group (Groupe de travail antihameçonnage) a noté une augmentation de l'utilisation de la redirection d'URL. Les pirates placent des redirecteurs à la fois avant la page d'accueil du site d'hameçonnage et après la soumission des identifiants. Cela permet de masquer l'URL d'hameçonnage afin qu'elle ne soit pas détectée via la surveillance du champ référent du journal du serveur Web[18].

Voici d'autres exemples d'hameçonnage évolué et inventif :

- L'industrialisation de l'hameçonnage grâce à la popularité croissante des kits d'hameçonnage prêts à l'emploi
- L'utilisation de Google Translate pour brouiller une URL liée à un faux site de récupération des identifiants Google[19]
- L'utilisation du chiffrement SSL sur une page Web d'hameçonnage pour renforcer la crédibilité d'un e-mail d'hameçonnage[20]

La compromission d'e-mails professionnels, ou BEC (Business Email Compromise), est également en hausse. Les criminels envoient des e-mails d'hameçonnage à partir de comptes de bonne réputation compromis, souvent des comptes Microsoft Office 365. Parce que les expéditeurs sont réels, les filtres ne bloquent pas ces communications. Ces escroqueries ont augmenté de 476 % entre le quatrième trimestre de 2017 et le quatrième trimestre de 2018[21], entraînant des pertes de 1,2 milliard de dollars en 2018[22].

Kits d'hameçonnage : l'industrialisation de l'hameçonnage

Les kits d'hameçonnage modélisés et produits en masse facilitent plus que jamais la création et le lancement rapides de campagnes malveillantes. Vendus sur l'Internet clandestin, ces kits fournissent généralement aux escrocs tout ce dont ils ont besoin pour monter des attaques nuisibles : outils de conception Web et graphiques, contenu d'espaces réservés, envoi massif d'e-mails ou autres logiciels de diffusion.

Steve Ragan, security researcher chez Akamai, décrit ces kits d'outils dans son article pour CSO :

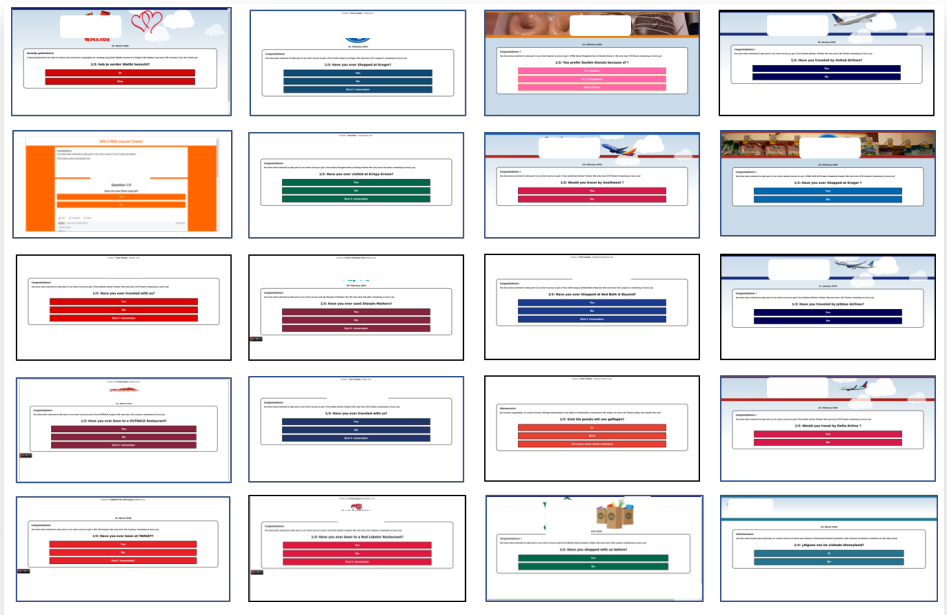
> *« Les kits sont le composant Web, ou le système dorsal d'une attaque d'hameçonnage. C'est l'étape finale dans la plupart des cas, lorsque le criminel a reproduit une marque ou une organisation connue. Une fois chargé, le kit est conçu pour refléter les sites Web légitimes, tels que ceux gérés par Microsoft, Apple ou Google[23]. »*

Des dizaines de milliers de ces kits sont actuellement disponibles. Les criminels les développent à l'aide d'un mélange de HTML et de PHP de base, et les stockent sur des serveurs Web compromis. Les programmes ne durent généralement que 36 heures avant d'être détectés et supprimés.

À l'origine, les cybercriminels vendaient les kits d'hameçonnage, mais ils sont de plus en plus proposés gratuitement. Cependant, ces kits d'hameçonnage « gratuits » masquent souvent les auteurs des kits comme des destinataires implicites, ce qui signifie que les informations volées sont non seulement capturées par l'acheteur du kit, mais également par le créateur original[24]. Comme le dit l'adage, il n'y a pas d'honneur parmi les voleurs.

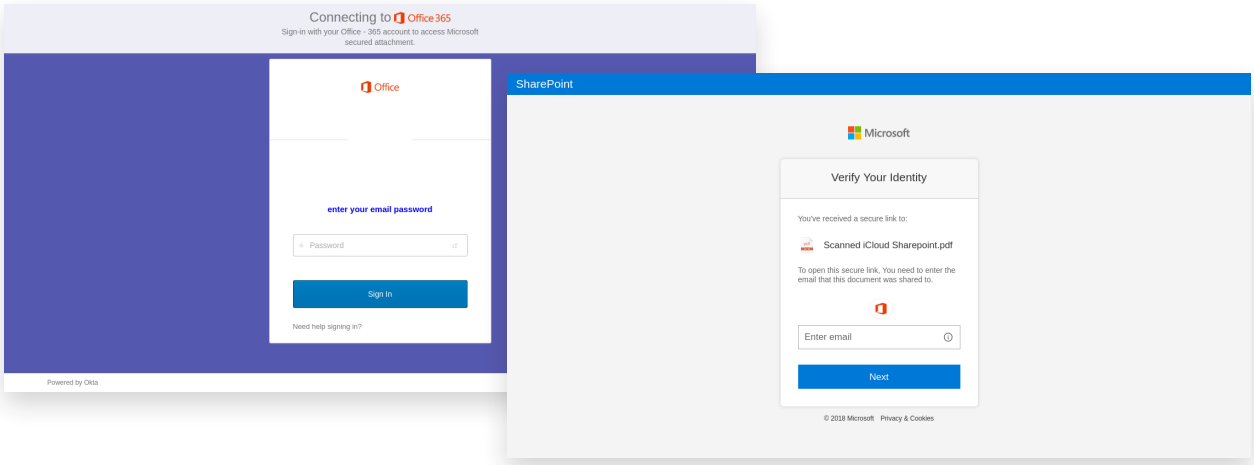
Les chercheurs d'Akamai ont récemment suivi l'activité de plus de 300 campagnes d'hameçonnage utilisant le même kit pour pirater plus de 40 marques commerciales[25]. Chaque escroquerie commence par un questionnaire en trois questions portant sur une marque reconnue. Quelle que soit la réponse sélectionnée, la victime « gagne » toujours.

Comme ces campagnes d'hameçonnage sont basées sur le même kit, elles partagent des fonctionnalités, comme illustrées à droite.



Ces campagnes basées sur des kits tirent parti de la réputation de confiance des marques connues. Bien qu'ils aient des origines et des caractéristiques similaires, chacun d'eux a été facilement personnalisé pour contenir différentes questions de quiz dans différentes langues. Bon nombre des marques victimes étaient des compagnies aériennes, mais les abus sont répandus. Les criminels usurpent aussi couramment les marques de commerce de détail, de décoration intérieure, de parcs d'attractions, de restauration rapide, de restaurants et de cafés.

Un grand nombre de ces fausses pages produites par un kit d'hameçonnage ciblent les internautes qui, par inadvertance, transportent ensuite la compromission sur leur réseau d'entreprise. Et les kits qui ciblent explicitement les utilisateurs d'entreprise sont également largement disponibles. Ces kits ont été utilisés pour créer ces pages de connexion imitant Microsoft Office 365 et SharePoint :



Qu'en est-il des passerelles et des filtres de messagerie ?

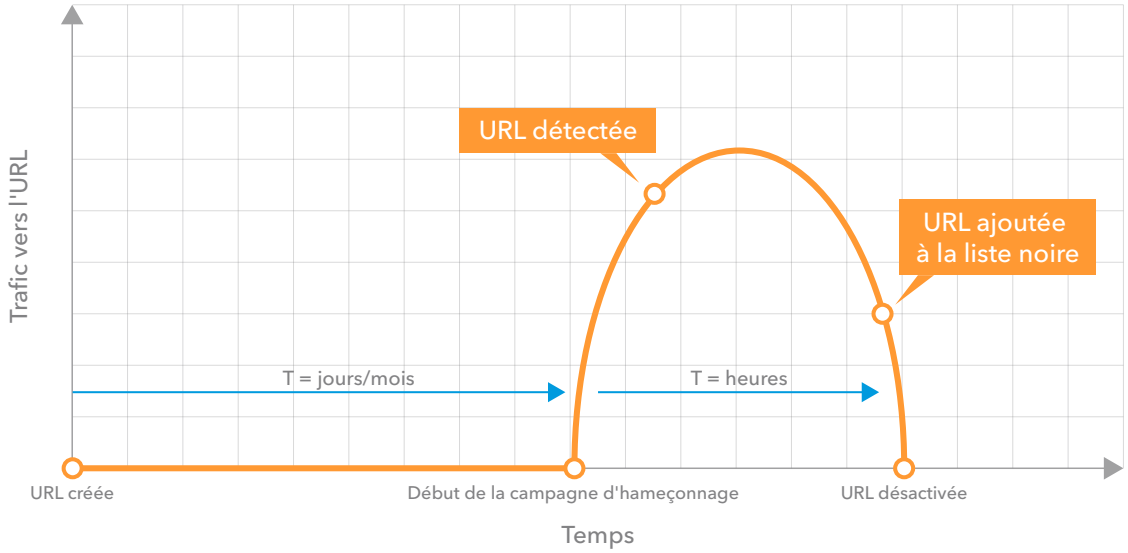
Les entreprises disposent généralement d'une certaine forme de filtrage des e-mails, soit en tant que service dédié, soit en complément de Microsoft Office 365 ou de Google G Suite. Ces produits offrent une protection correcte pour les utilisateurs contre le spam, l'hameçonnage et les e-mails malveillants traditionnels. Mais ils sont loin d'être parfaits.

Dans son dernier rapport *Email Security Risk Assessment*, la société de gestion des e-mails Mimecast signale que les communications compromises passent de plus en plus par les systèmes de sécurité de messagerie actuels. Ils ont détecté 463 546 URL malveillantes contenues dans 28 407 664 e-mails envoyés. En d'autres termes, un e-mail d'hameçonnage sur 61 atteint le destinataire visé[26].

La simplicité et la rentabilité des kits d'hameçonnage ainsi que la prolifération des réseaux sociaux permettent aux cybercriminels de créer et de diffuser des campagnes d'hameçonnage de courte durée avec un succès remarquable. L'équipe de recherche sur les menaces d'Akamai a déterminé que ces attaques de courte durée posent un ensemble unique de défis.

Le trafic doit atteindre le domaine d'hameçonnage et montrer un changement de comportement pour être repéré. Lorsque les équipes de sécurité observent ce trafic malveillant, analysent l'URL, ajoutent l'URL à une liste de menaces et envoient la liste de menaces mise à jour aux clients, la campagne d'hameçonnage est terminée. Elle a fini son œuvre et l'URL malveillante a été désactivée, probablement par les criminels ou peut-être par le propriétaire légitime du site qui a hébergé l'URL compromise.

Cet écart de détection représente une menace importante pour les entreprises.



L'ère de l'itinérance des terminaux d'entreprise et du BYOD (Bring Your Own Device) crée une nouvelle faille. Avec un personnel dispersé et mobile, les mécanismes de sécurité traditionnels des entreprises sont de plus en plus insuffisants. Les terminaux personnels qui entrent et sortent du périmètre de l'entreprise peuvent accéder à des comptes de messagerie privés non protégés par les passerelles et les filtres de messagerie de l'entreprise. Alors que la frontière entre les terminaux professionnels et personnels et l'accès continue de s'estomper, cette menace ne fera qu'empirer.

Les employés qui tombent dans le piège de l'hameçonnage ou d'autres arnaques constituent la menace d'initié la plus dangereuse[27].

42 %

d'employés innocents ont été dupés

26 %

d'employés combinant utilisation professionnelle et personnelle

L'hameçonnage ne se limite plus aux e-mails : il s'étend aux réseaux sociaux

Comme nous l'avons vu précédemment, l'e-mail n'est pas le seul moyen de lancer une attaque d'hameçonnage et de diffuser des liens malveillants.

Pour détecter, bloquer et atténuer ces attaques d'hameçonnage évoluées, les entreprises ont besoin d'une couche de défense supplémentaire, qui analyse l'ensemble du trafic provenant de tous les terminaux du réseau.

Conclusion

Le paysage de l'hameçonnage a évolué. Les kits d'hameçonnage industrialisés, ainsi que l'utilisation des réseaux sociaux et d'autres canaux de diffusion autres que la messagerie électronique sont la nouvelle norme. Cette tendance alarmante est aggravée par l'itinérance des terminaux. Les utilisateurs accèdent généralement aux applications de réseau social et de messagerie via des terminaux mobiles, qui constituent généralement le maillon le plus faible de la structure de sécurité de l'entreprise.

Pour réussir à riposter, les entreprises d'aujourd'hui doivent adopter un modèle Zero Trust. La devise de la sécurité des entreprises devrait être : ne se fier à rien, vérifier tout, maintenir des contrôles constants. Les entreprises doivent authentifier et autoriser chaque demande d'accès, puis accorder l'accès uniquement de façon temporaire.

Les solutions de sécurité basées sur le cloud sont idéalement positionnées pour mettre en œuvre une structure Zero Trust, car elles peuvent surveiller l'ensemble de l'activité du réseau de l'entreprise, quel que soit le type de terminal ou l'origine d'une demande. Elles disposent d'une visibilité globale : elles regroupent un trafic disparate et de portée limitée et créent une vision globale et en temps réel. Ces solutions utilisent des modèles à l'échelle d'Internet pour une sensibilisation plus complète aux menaces.

En observant l'impact des campagnes d'hameçonnage sur plusieurs entreprises, la protection basée sur le cloud peut identifier les tendances qui ne peuvent être détectées par une seule entreprise.

Akamai Enterprise Threat Protector

Enterprise Threat Protector d'Akamai identifie, bloque et atténue de manière proactive les menaces ciblées provenant des campagnes d'hameçonnage, des kits d'hameçonnage, des programmes malveillants, des ransomware, de vol de données DNS et d'attaques zero-day avancées. Enterprise Threat Protector est une plateforme Secure Internet Gateway qui permet aux équipes de sécurité de s'assurer que les utilisateurs et les terminaux peuvent se connecter en toute sécurité à Internet quel que soit l'endroit d'où ils se connectent, sans la complexité associée aux approches de sécurité héritées.

Pour plus d'informations sur Enterprise Threat Protector et un essai gratuit, rendez-vous sur le site akamai.com/etp.

En savoir plus

SOURCES

1) https://nakedsecurity.sophos.com/2018/10/23/phishing-is-still-the-most-commonly-used-attack-on-organizations-survey-says/
2) Data Breach Investigations Report 2018, https://enterprise.verizon.com/resources/reports/dbir/
3) Recherche Akamai interne
4) « Email Security Risk Assessment », rapport trimestriel, Mimecast, mars 2019. https://www.mimecast.com/globalassets/documents/whitepapers/esra-white-paper-march-2019-v3.pdf
5) Data Breach Investigations Report 2018, https://enterprise.verizon.com/resources/reports/dbir/
6) Global Phish Report 2019 d'Avanan, https://www.avanan.com/global-phish-report
7) Rapport The Human Factor 2018, https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-wp-human-factor-report-2018-180425.pdf
8) https://www.webroot.com/us/en/about/press-room/releases/nearly-15-million-new-phishing-sites
9) State of the Phish Report 2019, https://info.wombatsecurity.com/hubfs/Wombat_Proofpoint_2019%20State%20of%20the%20Phish%20Report_Final.pdf
10) Enterprise Phishing Resiliency and Defense Report, https://cofense.com/wp-content/uploads/2017/11/Enterprise-Phishing-Resiliency-and-Defense-Report-2017.pdf
11) https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/consumer-business/deloitte-uk-consumer-review-nov-2015.pdf
12) https://betanews.com/2019/05/02/social-media-phishing/
13) « A New Era in Phishing – Games, Social, and Prizes » par Or Katz, Akamai. https://www.akamai.com/us/en/multimedia/documents/report/a-new-era-in-phishing-research-paper.pdf
14) « Four Phishing Attack Trends To Look Out For In 2019 » par Michael Landewe, Avanan. https://www.forbes.com/sites/forbestechcouncil/2019/01/10/four-phishing-attack-trends-to-look-out-for-in-2019/#6a9fd5034ec2
15) « Cybercriminals Impersonate Popular File Sharing Services to Take Over Email Accounts » par Asaf Cidon, CSO. https://www.csoonline.com/article/3274546/cybercriminals-impersonate-popular-file-sharing-services-to-take-over-email-accounts.html
16) Mobile Phishing Report 2018, https://info.lookout.com/rs/051-ESQ-475/images/Lookout-Phishing-wp-us.pdf
17) « Z-WASP Vulnerability Used to Phish Office 365 and ATP » par Yoav Nathaniel, Avanan. https://www.avanan.com/resources/zwasp-microsoft-office-365-phishing-vulnerability
18) « Phishing Activity Trends Report » par l'Anti-Phishing Working Group. http://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf
19) « Phishing Attacks Against Facebook / Google via Google Translate » par Larry Cashdollar. https://blogs.akamai.com/sitr/2019/02/phishing-attacks-against-facebook-google-via-google-translate.html
20) « Phishing Activity Trends Reports » par l'Anti-Phishing Working Group. http://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf
21) https://www.bleepingcomputer.com/news/security/business-email-compromise-attacks-see-almost-500-percent-increase/
22) « 2018 Internet Crime Report » par le Federal Bureau of Investigation, International Crime Compliant Center. https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf
23) « What Are Phishing Kits? Web Components of Phishing Attacks Explained » par Steve Ragan, CSO. https://www.csoonline.com/article/3290417/csos-guide-to-phishing-and-phishing-kits.html
24) Recherche Akamai interne
25) « Quiz Phishing: One Scam, 78 Variations » par Or Katz, Akamai. https://blogs.akamai.com/sitr/2018/12/quiz-phishing-one-scam-78-variations.html
26) « Email Security Risk Assessment », rapport trimestriel, Mimecast, mars 2019. https://www.mimecast.com/globalassets/documents/whitepapers/esra-white-paper-march-2019-v3.pdf
27) https://www.idg.com/tools-for-marketers/2018-u-s-state-of-cybercrime/

Akamai sécurise et fournit des expériences digitales pour les plus grandes entreprises du monde. La plateforme de périphérie intelligente d'Akamai englobe tout, de l'entreprise au cloud, afin d'offrir rapidité, agilité et sécurité à ses clients et à leurs entreprises. Les plus grandes marques mondiales comptent sur Akamai pour les aider à concrétiser leur avantage concurrentiel grâce à des solutions agiles qui développent la puissance de leurs architectures multi-cloud. Akamai place les décisions, les applications et les expériences au plus près des utilisateurs, et au plus loin des attaques et des menaces. Les solutions de sécurité en périphérie, de performances Web et mobiles, d'accès professionnel et de diffusion vidéo du portefeuille d'Akamai s'appuient également sur un service client exceptionnel, des analyses et une surveillance 24 h/24 et 7 j/7, 365 jours par an. Pour savoir pourquoi les plus grandes marques internationales font confiance à Akamai, visitez akamai.com, blogs.akamai.com ou @Akamai sur Twitter. Vous trouverez nos coordonnées dans le monde entier à l'adresse akamai.com/locations. Publication : 08/19.