proofpoint.

EBOOK

La sensibilisation : un pare-feu efficace contre les cyberattaques ?

Ce que les utilisateurs ignorent à propos des cybermenaces — et pourquoi cela peut leur porter préjudice

Introduction

D'après un vieil adage, ce que l'on ignore ne peut pas nous faire de mal. Rien n'est moins vrai en ce qui concerne les cybermenaces.

Le manque de connaissances peut porter préjudice à vos utilisateurs, mais aussi à l'entreprise tout entière. Les collaborateurs sont une cible privilégiée des cyberattaques. Les erreurs dues à leur manque de connaissances peuvent entraîner des perturbations des activités et des fuites de données, de même qu'avoir des conséquences négatives à long terme.

Cet eBook se penche sur des attaques réelles qui mettent en lumière le double rôle des utilisateurs en tant que principales cibles des cybercriminels et première ligne de défense des entreprises.

Sont abordées cinq grandes catégories de cyberattaques qui commencent par — ou reposent sur — la compromission d'utilisateurs :

- Phishing
- Piratage de la messagerie en entreprise (BEC, Business Email Compromise)
- Ransomwares
- Attaques cloud
- Attaques via la messagerie Web

Nous vous présenterons également certaines conclusions de notre rapport State of the Phish 2022 pour mettre en avant les connaissances, les vulnérabilités et la résilience des utilisateurs dans ces domaines. Ces données pourront éclairer les responsables de la sécurité cherchant à protéger leurs utilisateurs, leurs données et leurs marques. Elles montrent également pourquoi les collaborateurs constituent le nouveau périmètre — et doivent donc être au cœur de vos initiatives de cybersécurité.

SECTION 1

Phishing

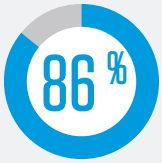
Le phishing est un type d'ingénierie sociale.

Distribués par email ou par SMS, les messages de phishing ont recours à un éventail croissant de techniques pour exploiter la psychologie humaine. Les cybercriminels trompent la confiance des utilisateurs pour mettre la main sur des informations financières, des identifiants système et d'autres données sensibles.

Tendances

Année après année, le phishing gagne en popularité auprès des cybercriminels. D'après le *rapport 2021 sur la cybercriminalité* du FBI, le phishing et les attaques similaires représentaient plus de 38 % des activités cybercriminelles potentielles signalées aux États-Unis l'année dernière. Près de 323 000 tentatives de phishing ont été rapportées en 2021, soit près de 83 000 plaintes de plus qu'en 2020 et 209 000 de plus qu'en 2019[1].

Les recherches que nous avons menées pour les besoins du rapport *State of the Phish 2022* révèlent à quel point les attaques de phishing sont répandues et efficaces. En effet, en 2021 :



des entreprises ont été victimes d'attaques de phishing en masse[2]

1 utilisateur sur 5

a ouvert une pièce jointe dans le cadre d'une simulation d'attaque de phishing

1 utilisateur sur 10

a cliqué sur un lien dans le cadre d'une simulation d'attaque de phishing

Exemple concret : mise hors service du réseau électrique ukrainien

En décembre 2015, le réseau électrique ukrainien a été piraté, ce qui a entraîné des coupures de courant allant jusqu'à six heures pour environ 225 000 consommateurs. Il s'agit de la première cyberattaque publiquement reconnue ayant entraîné des coupures de courant[3].

Les cybercriminels à l'origine de l'attaque ont passé plusieurs mois à préparer leur stratégie et à collecter des informations de threat intelligence. Parmi les techniques employées pour mener leur plan à bien, on retrouve le spear phishing. Les cibles étaient des membres de l'équipe informatique et des administrateurs système de trois sociétés ukrainiennes de distribution d'énergie (ou *oblenergos*)[4].

1 FBI IC3, « Internet Crime Report 2021 » (Rapport 2021 sur la cybercriminalité), mars 2022. Disponible sur : https://www.ic3.gov/Home/AnnualReports.

2 Proofpoint définit le phishing en masse comme des attaques classiques lancées au hasard dans le cadre desquelles le même email est envoyé à de nombreux collaborateurs d'une entreprise.

3 SANS ICS (Industrial Control Systems) et E-ISAC (Electricity Information Sharing and Analysis Center), « Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case » (Analyse de la cyberattaque contre le réseau électrique ukrainien : enseignements en matière de défense), 18 mars 2016.

4 ICS et E-ISAC.

Déroulement de l'attaque

Pour compromettre ces utilisateurs, les cybercriminels ont envoyé une pièce jointe malveillante au format Microsoft Word dans un email qui semblait provenir d'une source de confiance. Une fois ouvert, le document affichait une fenêtre contextuelle invitant l'utilisateur à activer les macros. Si l'utilisateur s'exécutait, un malware appelé BlackEnergy3 infectait la machine et installait une porte dérobée (backdoor) pour les cybercriminels[5].

Ces attaques de spear phishing ont offert aux cybercriminels un accès au réseau de la société de distribution d'énergie. Les cyberpirates ont ensuite passé plusieurs mois à s'infiltrer dans les systèmes de contrôle et d'acquisition de données en temps réel (SCADA) des sociétés pour préparer leur attaque. Ils ont employé diverses techniques, y compris l'établissement d'un accès aux contrôleurs de domaine Microsoft Windows pour collecter encore plus d'identifiants de connexion des utilisateurs[6].

Résultat

Les coupures de courant ont été de courte durée. Pourtant, il a fallu plusieurs mois pour que les centres de contrôle des oblenergos concernés redeviennent pleinement opérationnels. Et comme le souligne un rapport sur l'attaque, l'incident a établi un précédent fâcheux pour la sécurité des réseaux électriques du monde entier[7].

Conséquences potentielles du phishing

Prise de contrôle de comptes | Pertes financières | Fuite de données | Atteinte à la réputation

Comment la sensibilisation des utilisateurs aurait pu aider

Comme la plupart des cyberattaques, la mise hors service du réseau électrique ukrainien en 2015 a commencé par un email de phishing. Après avoir incité un collaborateur à ouvrir une pièce jointe infectée, les cybercriminels ont passé plusieurs mois à collecter des informations de threat intelligence et à s'infiltrer plus profondément dans l'environnement.

Des formations de sensibilisation à la sécurité informatique auraient pu aider à neutraliser l'attaque avant même qu'elle ne soit lancée. Le collaborateur aurait su qu'il ne fallait pas ouvrir la pièce jointe ni interagir avec elle, ce qui aurait empêché les cybercriminels d'obtenir un accès aux systèmes.

5 Kim Zetter *(Wired)*, « Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid » (Dans les coulisses du piratage sans précédent du réseau électrique ukrainien), 3 mars 2016.
6 Ibid.
7 Ibid.

SECTION 2

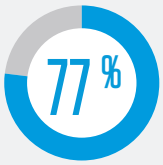
Piratage de la messagerie en entreprise (BEC)

Le piratage de la messagerie en entreprise (BEC, Business Email Compromise) cible des entreprises de toutes tailles et de tous les secteurs.

Les cybercriminels spécialisés dans les attaques BEC se font passer pour une personne ou une entité en qui le destinataire est susceptible d'avoir confiance, comme le PDG de l'entreprise ou un fournisseur. Le destinataire est ensuite invité à transférer des fonds, à détourner des salaires, à modifier des informations bancaires en vue de l'exécution ultérieure de paiements ou à effectuer d'autres actions. Au moment où la victime se rend compte de l'erreur commise, il est souvent trop tard pour récupérer l'argent.

Tendances

Les campagnes BEC peuvent rapporter gros. D'après le *rapport 2021 sur la cybercriminalité* du FBI, les attaques BEC ont entraîné des pertes ajustées de 2,4 milliards de dollars l'année dernière rien qu'aux États-Unis[8]. Étant donné les gains potentiels, il n'est pas surprenant que les recherches que nous avons menées pour les besoins du rapport *State of the Phish 2022* aient révélé que 77 % des entreprises du monde entier ont été victimes d'attaques BEC en 2021.



des entreprises à travers le monde ont été visées par des attaques BEC en 2021

Les attaques BEC sont souvent très sophistiquées, bien financées et soutenues par une planification et des recherches minutieuses[9]. De nombreux cybercriminels concentrent leurs efforts sur la fraude aux factures fournisseurs en raison des importantes transactions B2B qu'ils peuvent pirater. La fraude aux factures est une tactique courante. Lors de ces attaques, le cyberescroc se fait passer pour un fournisseur et détourne des paiements destinés à de véritables fournisseurs.

Exemple concret : Ubiquiti victime d'une fraude aux fournisseurs à 46,7 millions de dollars

La fraude au PDG constitue une stratégie BEC bien connue mais néanmoins efficace, dans le cadre de laquelle les cybercriminels se font passer pour le PDG ou un autre cadre supérieur d'une entreprise. En général, ils envoient un email à un collaborateur du département financier pour demander un transfert de fonds. L'argent est souvent viré sur un compte international contrôlé par les cyberpirates.

Ubiquiti Inc. a été victime de ce type d'escroquerie BEC. Les cybercriminels sont parvenus à extorquer 46,7 millions de dollars à la société technologique avant que quelqu'un ne se rende compte de la supercherie. Les utilisateurs ayant le pouvoir de transférer des fonds ne pensent pas forcément à remettre en question les demandes à caractère financier émanant de cadres supérieurs — même si celles-ci leur semblent inhabituelles.

Déroulement de l'attaque

Quelques semaines seulement après avoir rejoint l'entreprise à la mi-mai 2015, le nouveau directeur financier d'Ubiquiti a reçu des emails qu'il pensait provenir du PDG de la société et d'un avocat basé à Londres. Le cyberescroc se faisant passer pour le PDG a expliqué que l'entreprise s'apprêtait à réaliser une acquisition. L'email demandait au directeur financier de garder cette acquisition secrète et expliquait que plusieurs virements bancaires étaient nécessaires pour conclure la transaction. L'imposteur a ensuite envoyé des emails contenant de fausses instructions et informations bancaires, et autorisant les paiements[10].

8 FBI IC3.

9 Proofpoint, « Gare aux fraudes par email ! Tour d'horizon des attaques BEC les plus dévastatrices », avril 2022.

10 Nathan Vardi *(Forbes)*, « How a Tech Billionaire's Company Misplaced $46.7 Million and Didn't Know It » (Comment l'entreprise d'un milliardaire de la Silicon Valley a égaré 46,7 millions de dollars sans même s'en rendre compte), février 2016.

Résultat

En 17 jours, le directeur financier a effectué 14 virements bancaires, pour un total de 46,7 millions de dollars, vers des comptes chinois, hongrois, russes et polonais. Début juin, le véritable PDG de l'entreprise a été contacté par un agent du FBI, qui l'a informé qu'une grosse somme d'argent avait peut-être été dérobée sur le compte de la division d'Ubiquiti à Hong Kong[11]. Jusqu'alors, le PDG n'avait même pas connaissance des virements bancaires.

En août 2015, Ubiquiti a révélé dans un rapport financier trimestriel déposé auprès de la SEC (Securities and Exchange Commission) qu'une fraude avait été découverte en juin. L'incident y était décrit comme « une usurpation de l'identité d'un collaborateur et des demandes frauduleuses émanant d'une entité extérieure ».

Ubiquiti n'a pu récupérer qu'une partie du montant subtilisé et la réputation de l'entreprise en est ressortie entachée. Son directeur financier a démissionné juste avant que l'entreprise n'annonce publiquement l'attaque BEC. Une enquête interne a mis en lumière l'inefficacité des contrôles internes appliqués aux activités financières, lesquels contrôles ont par la suite été consolidés par l'entreprise[12].

Conséquences potentielles des attaques BEC

Pertes financières directes

Fuite de données

Comment la sensibilisation des utilisateurs aurait pu aider

Les fraudes aux fournisseurs et autres menaces BEC sont des attaques qui, par nature, sont centrées sur les personnes. Elles ne parviennent à leurs fins que si les destinataires pensent avoir affaire à quelqu'un en qui ils ont confiance. S'il avait suivi une formation efficace de sensibilisation à la sécurité informatique, le directeur financier aurait peut-être su reconnaître les signes indiquant que les emails provenaient d'un imposteur, et non du PDG et des avocats de l'entreprise.

Combinée à des contrôles financiers solides, une telle formation peut apprendre à vos collaborateurs à détecter instinctivement les domaines similaires ou sans rapport, les URL dangereuses et les techniques d'ingénierie sociale susceptibles de tromper les utilisateurs moins bien informés.

11 Ibid.

12 KrebsonSecurity. « Tech Firm Ubiquiti Suffers $46M Cyberheist »
(Un cyberhold-up à 46 millions de dollars pour la société technologique Ubiquiti), août 2015.

SECTION 3

Ransomwares

Fondamentalement, un ransomware est un outil d'extorsion. Il s'agit d'un malware qui prend en otage les données et les systèmes informatiques des victimes jusqu'au versement d'une rançon.

En général, le cybercriminel exige un paiement en cryptomonnaie (p. ex., en bitcoins), car l'argent est ainsi transféré plus rapidement et plus difficile à tracer. La demande de rançon est souvent assortie d'une échéance : si les victimes ne paient pas à temps, elles perdront leurs données pour de bon ou devront s'acquitter d'une rançon plus élevée pour les récupérer. Pour augmenter la pression sur les victimes, les cybercriminels les menacent souvent de publier les données. Il arrive aussi que les victimes paient la rançon sans pour autant récupérer leurs données.

Les chiffreurs et les verrouilleurs d'écran sont les principaux types de malwares utilisés dans les attaques de ransomwares. Les chiffreurs, comme leur nom l'indique, chiffrent les données présentes sur un système, de sorte que le contenu est inutilisable sans clé de déchiffrement. Les verrouilleurs d'écran utilisent un écran « de verrouillage » pour empêcher les utilisateurs d'accéder au système compromis.

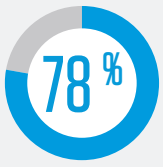
Les attaques de ransomwares existent depuis plusieurs décennies. Elles ont beaucoup attiré l'attention des médias ces dernières années, car elles entraînent des perturbations majeures, exigent le versement de sommes astronomiques et ciblent des infrastructures critiques, en particulier dans les secteurs de la santé et de l'énergie.

Elles ont par ailleurs évolué au fil du temps. Les opérateurs de ransomwares achètent souvent un accès auprès de groupes cybercriminels indépendants qui infiltrent des cibles de choix, puis vendent cet accès à d'autres cyberpirates en échange d'une part des gains mal acquis. Des groupes cybercriminels distribuant déjà des malwares bancaires ou autres chevaux de Troie peuvent également intégrer un réseau affilié d'organisations de ransomwares. Se constitue ainsi un écosystème criminel solide et lucratif dans lequel des individus et des organisations se sont spécialisés dans l'optimisation des profits de toutes les parties concernées — à l'exception, bien entendu, des victimes.

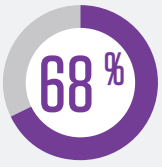
Tendances

Les attaques de ransomwares sont elles aussi en plein essor. D'après le *rapport d'enquête 2022 sur les compromissions de données* de Verizon, les attaques de ransomwares ont augmenté de 13 % entre 2020 et 2021, ce qui équivaut à la hausse enregistrée au cours des cinq dernières années combinées[13].

Voici quelques conclusions du rapport *State of the Phish 2022* concernant les ransomwares :



des entreprises ont été victimes d'attaques de ransomwares par email en 2021



des entreprises ont été infectées par des ransomwares

des entreprises infectées ont payé une rançon

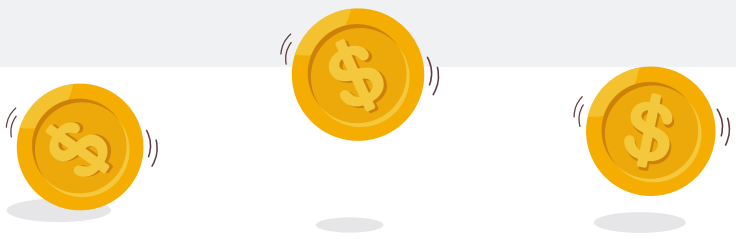
13 Verizon, « Data Breach Investigations Report » (Rapport d'enquête sur les compromissions de données), mai 2022.

Exemple concret : attaques de ransomwares consécutives contre le gouvernement costaricain

Une attaque de ransomware de grande ampleur a frappé le gouvernement costaricain en avril 2022. Elle a ciblé une trentaine d'organismes, dont le ministère des Finances, la caisse de sécurité sociale et même l'institut météorologique national. Le gang de ransomware Conti a revendiqué cette campagne et a demandé une rançon de 10 millions de dollars américains, faute de quoi il divulguerait les informations sensibles subtilisées sur les serveurs du ministère des Finances avant l'attaque[14].

Lorsque le gouvernement a refusé de payer, Conti a augmenté la demande de rançon à 20 millions de dollars. Peu après, le groupe a commencé à charger les fichiers volés sur son site Web. Dans une tentative vaine et désespérée pour obtenir un paiement, le groupe Conti a réduit la demande de rançon à 15 millions de dollars[15]. Les cybercriminels ont également menacé de renverser le gouvernement[16].

Fin mai, alors que le gouvernement costaricain ne s'était toujours pas complètement remis de l'attaque du groupe Conti, le système de santé national (CCSS) a été victime d'une attaque de ransomware lancée par un groupe connu sous le nom de Hive. L'organisme a pris conscience de l'attaque lorsque ses imprimantes ont commencé à sortir des copies du message de rançon de Hive, qui ne faisait état d'aucun montant[17]. La demande est arrivée plus tard, lorsque Hive a exigé le versement d'une rançon de 5 millions de dollars en bitcoins, sans quoi il divulguerait des informations sensibles[18].



14 Carly Page *(TechCrunch)*, « Fears Grow for Smaller Nations After Ransomware Attack on Costa Rica Escalates » (L'inquiétude des petits pays grandit après l'escalade de l'attaque de ransomware contre le Costa Rica), 20 mai 2022.

15 Carla Rosch *(Rest of World)*, « A Massive Cyberattack in Costa Rica Leaves Citizens Hurting » (Une cyberattaque de grande ampleur sème le chaos au Costa Rica), 1er juin 2022.

16 Matt Burgess *(Wired)*, « Conti's Attack Against Costa Rica Sparks a New Ransomware Era » (L'attaque du groupe Conti contre le Costa Rica marque le début d'une nouvelle ère pour les ransomwares), 12 juin 2022.

17 KrebsonSecurity, « Costa Rica May Be Pawn in Conti Ransomware Group's Bid to Rebrand, Evade Sanctions » (Le Costa Rica pourrait être un pion dans la tentative du gang de ransomware Conti pour changer de marque et échapper aux sanctions), 31 mai 2022.

18 Alonso Martinez *(Delfino)*, « Cybercriminals Request $5 million in Bitcoins from the CCSS » (Les cybercriminels réclament 5 millions de dollars en bitcoins au système de santé national costaricain), 2 juin 2022.

Déroulement de l'attaque

Selon des chercheurs spécialisés en menaces, un membre du groupe Conti connu sous le nom de « MemberX » a utilisé des identifiants de connexion compromis pour établir un accès via une connexion VPN à un système appartenant au ministère des Finances du Costa Rica[19]. Moins de 24 heures après la première attaque lancée par Conti, les cybercriminels avaient chiffré les fichiers du ministère des Finances et mis à l'arrêt deux systèmes critiques : le système de collecte des impôts en ligne et le système informatique de contrôle des douanes[20].

Certains prétendent que Conti aurait reçu l'aide de personnes travaillant pour le gouvernement costaricain. En effet, le groupe a publié un message sur le Dark Web après l'attaque, indiquant que « des personnes travaillant pour le gouvernement [costaricain] » lui avaient apporté leur aide, des affiliés identifiés comme « UNC1756 »[21].

Le groupe Hive, quant à lui, s'appuie sur un modèle RaaS (Ransomware-as-a-Service) pour ses attaques. Le groupe et ses affiliés envoient des emails de phishing contenant des pièces jointes malveillantes, cherchent à mettre la main sur des identifiants de connexion VPN et utilisent des serveurs RDP (Remote Desktop Protocol) vulnérables pour se déplacer latéralement au sein du réseau compromis. Selon un comité consultatif du FBI sur Hive, le groupe exfiltre généralement des données et chiffre les fichiers présents sur le réseau. Il laisse ensuite un message de rançon dans chaque répertoire affecté du système de la victime. Le message donne les instructions à suivre pour acheter le logiciel de déchiffrement et menace de publier les données de la victime sur le site Tor « HiveLeaks »[22].

Certains experts en cybersécurité pensent que les mêmes cybercriminels étaient impliqués dans les deux attaques de ransomwares survenues au printemps. Selon eux, Hive pourrait s'être servi de sa campagne pour aider Conti à « changer de marque » afin d'échapper aux lois internationales interdisant de payer les cybercriminels qui opèrent dans des pays connus pour tolérer (si ce n'est soutenir) cette activité[23]. Hive a déclaré sur son site Web qu'il n'était pas affilié à Conti[24].

Résultat

Après la première attaque de ransomware survenue à la mi-avril, l'économie costaricaine perdait près de 30 millions de dollars par jour. Le gouvernement a été contraint de mettre à l'arrêt de nombreux systèmes critiques pendant la phase de correction. Les pertes subies par la Chambre costaricaine de commerce extérieur sont estimées à plus de 125 millions de dollars rien que pour les deux premiers jours suivant l'attaque[25].

19 Ionut Ilascu *(BleepingComputer),* « How Conti Ransomware Hacked and Encrypted the Costa Rican Government » (Comment le gang de ransomware Conti a piraté et chiffré les fichiers du gouvernement costaricain), 21 juillet 2022.

20 Matt Burgess *(Wired),* « Conti's Attack Against Costa Rica Sparks a New Ransomware Era » (L'attaque du groupe Conti contre le Costa Rica marque le début d'une nouvelle ère pour les ransomwares), 12 juin 2022.

21 Claudia Glover *(Tech Monitor),* « 'We will overthrow the government' – Does Conti have help inside Costa Rica? » ("Nous allons renverser le gouvernement" – Le groupe Conti reçoit-il de l'aide de personnes travaillant pour le gouvernement costaricain ?), 17 mai 2022.

22 Rapport FLASH du FBI, « Indicators of Compromise Associated with Hive Ransomware » (Indicateurs de compromission associés au ransomware Hive), 25 août 2021.

23 KrebsonSecurity, « Costa Rica May Be Pawn in Conti Ransomware Group's Bid to Rebrand, Evade Sanctions » (Le Costa Rica pourrait être un pion dans la tentative du gang de ransomware Conti pour changer de marque et échapper aux sanctions), 31 mai 2022.

24 Ibid.

25 Carla Rosch *(Rest of World),* « A Massive Cyberattack in Costa Rica Leaves Citizens Hurting » (Une cyberattaque de grande ampleur sème le chaos au Costa Rica), 1er juin 2022.

Le gouvernement a également dû mettre hors ligne les pages Web des organismes ciblés. Il a sollicité l'aide technique d'autres gouvernements, dont les États-Unis, et de sociétés technologiques telles que Microsoft. Les États-Unis ont même proposé jusqu'à 5 millions de dollars de récompense en échange d'informations qui pourraient conduire à l'arrestation ou à la condamnation de toute personne impliquée dans une attaque de ransomware lancée par Conti[26].

Début mai, le nouveau président du Costa Rica, Rodrigo Chaves Robles, a déclaré l'état d'urgence nationale, qualifiant l'attaque du groupe Conti d'acte de terrorisme. Quelques semaines plus tard, Hive a lancé son attaque.

Le gouvernement costaricain a mis des semaines à s'en remettre. À la mi-juin, certains organismes ont enfin pu reprendre leurs activités.

Conséquences potentielles des ransomwares

Perturbation des activités

Pertes financières
(dues au paiement de la rançon et aux mesures de correction après l'attaque)

Fuite de données
(si les cybercriminels mettent leurs menaces à exécution et divulguent des données en l'absence de paiement de la rançon)

Comment la sensibilisation des utilisateurs aurait pu aider

Selon certaines sources, l'attaque de ransomware contre le Costa Rica aurait pu bénéficier de l'aide de personnes malintentionnées travaillant pour le gouvernement. Toutefois, de nombreuses infections de ransomwares découlent d'attaques antérieures véhiculées par email. Les cybercriminels emploient des techniques telles que le phishing pour dérober des identifiants de connexion qui leur permettront d'accéder à des systèmes critiques.

Apprendre aux utilisateurs à repérer et à signaler les emails suspects peut réduire considérablement le risque de ransomwares et autres malwares, en particulier si vous effectuez également des analyses automatisées en boucle fermée.

Les utilisateurs doivent instinctivement se méfier des pièces jointes et des URL, surtout dans les emails qui jouent sur des sentiments humains comme le profit personnel, la curiosité, la peur, l'indignation et même la serviabilité. Ils doivent également connaître les signes indiquant que l'expéditeur pourrait ne pas être celui qu'il prétend être.

26 Elizabeth Montalbano *(Threatpost)*, « Conti Ransomware Attack Spurs State of Emergency in Costa Rica » (L'état d'urgence déclaré au Costa Rica suite à l'attaque du gang de ransomware Conti), 10 mai 2022.

SECTION 4

Attaques cloud et prise de contrôle de comptes

Les cybercriminels suivent les utilisateurs comme leur ombre. La migration vers le cloud ne fait pas exception à la règle. La pandémie de COVID-19 a accéléré la migration vers le cloud, ce qui s'est traduit par une multiplication des attaques cloud. Comme l'explique notre *rapport Le facteur humain 2022*, les compromissions de comptes cloud occupent aujourd'hui une place importante et permanente dans le paysage des cybermenaces, au même titre que le phishing et les malwares.

La compromission de compte consiste à prendre le contrôle du compte cloud d'un service de messagerie ou de collaboration d'un utilisateur légitime afin d'accéder à un large éventail de données, contacts, événements de calendrier, emails et autres outils système. En exploitant l'authentification unique, les cyberpirates sont libres de se déplacer dans différents systèmes au sein de l'environnement et de causer des dommages considérables.

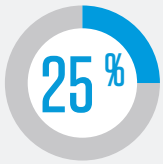
Voici des outils auxquels les cybercriminels ont souvent recours pour compromettre des comptes cloud et en prendre le contrôle :

- Attaques par force brute qui automatisent la recherche systématique d'identifiants de connexion
- Attaques de phishing, notamment phishing de jetons OAuth
- Recyclage d'identifiants de connexion, également appelé « credential stuffing », qui utilise des combinaisons de nom d'utilisateur et de mot de passe volées précédemment
- Malwares, tels que les enregistreurs de frappe et les voleurs d'identifiants de connexion

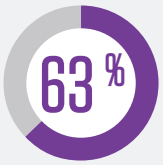
La persistance semble également faire partie des ingrédients indispensables d'une compromission de comptes cloud.

Tendances

D'après le rapport *Le facteur humain 2022*, plus de 90 % des locataires cloud surveillés ont été ciblés par des cybercriminels chaque mois. Près d'un quart (25 %) ont été victimes d'une attaque réussie. Le pourcentage total de locataires compromis en 2021 atteint 63 %[27].



des attaques contre les locataires cloud surveillés ont été fructueuses



des locataires cloud ont été compromis en 2021

Les prises de contrôle de comptes cloud sont souvent difficiles à détecter, complexes à neutraliser et dommageables pour vos résultats financiers. Selon une étude récente, les pertes financières moyennes dues à la compromission de comptes cloud s'élèvent à 6,2 millions de dollars par an pour les entreprises. En moyenne, les entreprises subissent également 138 heures d'interruption des applications imputables à cette activité[28].

Applications cloud malveillantes

Les applications non approuvées (Shadow IT) participent au problème des applications cloud malveillantes. Une application cloud tierce est une application qui s'intègre avec un service cloud, mais qui est fournie par un fournisseur autre que celui dudit service cloud. Les applications tierces utilisent OAuth, un protocole d'autorisation grâce auquel elles peuvent obtenir un accès limité à un service cloud. OAuth permet également à des applications tierces d'utiliser les informations ou les données d'un compte utilisateur sans exposer les identifiants de connexion de ce dernier[29].

À première vue, ce processus semble très pratique et sûr. Malheureusement, les applications tierces peuvent facilement être exploitées. Lorsque les utilisateurs les installent, ils cliquent souvent sur Accepter sans prêter attention à l'étendue des autorisations. Une fois que les cybercriminels disposent d'un accès OAuth, ils peuvent compromettre et pirater des comptes cloud. Pire encore, ils bénéficient d'un accès persistant aux comptes et données des utilisateurs jusqu'à ce que le jeton OAuth soit explicitement révoqué.

27 Proofpoint, « Le facteur humain 2022 », mai 2022.

28 Ponemon Institute, « 2021 Ponemon Report: The Cost of Cloud Compromise and Shadow IT » (Rapport 2021 du Ponemon Institute : le coût de la compromission de comptes cloud et du Shadow IT), avril 2021.

29 Proofpoint, « Ce que tout professionnel de la sécurité doit savoir sur les applications OAuth tierces », mai 2022.

Fichiers malveillants stockés dans le cloud

Une fois qu'un cybercriminel a pris le contrôle d'un compte cloud, il peut charger des fichiers malveillants afin de préparer le terrain pour d'autres méfaits, comme un vol de données ou une fraude aux virements bancaires. Par exemple, au cours d'une attaque de phishing exploitant Microsoft SharePoint, un cyberpirate charge un fichier malveillant sur un compte cloud compromis. Il définit les autorisations de partage du fichier sur Public afin que le nouveau lien anonyme puisse être partagé avec tout le monde. Il envoie ensuite le lien par email ou le communique aux contacts de l'utilisateur compromis ou à d'autres cibles. Une fois que ces destinataires ont ouvert le fichier et cliqué sur le lien malveillant, le cybercriminel a le champ libre[30].

Nos chercheurs spécialisés en menaces ont récemment découvert une nouvelle variante des attaques cloud : les cyberpirates ciblent désormais des données cloud et lancent des attaques de type ransomware à l'aide de l'infrastructure cloud. Ils compromettent par la même occasion des applications cloud d'entreprise populaires, comme SharePoint Online et OneDrive dans la suite Microsoft 365[31].

Malgré le danger bien réel que peuvent représenter les fichiers compromis dans le cloud, le rapport *State of the Phish 2022* révèle que seulement 37 % des utilisateurs savent que les fichiers stockés dans le cloud peuvent être malveillants.

Exemple concret : campagne OiVaVoii

Le cloud facilite la collaboration et le partage de données. Il s'agit d'un environnement de menaces complexe qui évolue rapidement dans un contexte de transformation numérique et de généralisation du travail à distance et hybride.

Une campagne récente ciblant des utilisateurs de grande valeur, dont des membres de l'équipe de direction, montre pourquoi les collaborateurs à tous les échelons de la hiérarchie doivent faire preuve de prudence lorsqu'ils accordent des autorisations à des applications cloud, même si celles-ci paraissent inoffensives et semblent provenir d'expéditeurs légitimes.

30 Itir Clarke, Eilon Bendet et Doyle Groves, *(Proofpoint),* « Comment se protéger contre le phishing sur OneDrive et SharePoint ? », octobre 2020.

31 Or Safran, David Krispin, Assaf Friedman et Saikrishna Chavali *(Proofpoint),* « Proofpoint Discovers Potentially Dangerous Microsoft Office 365 Functionality that can Ransom Files Stored on SharePoint and OneDrive » (Découverte par Proofpoint d'une fonctionnalité de Microsoft 365 potentiellement dangereuse capable de prendre en otage des fichiers stockés sur SharePoint et OneDrive), juin 2022.

Déroulement de l'attaque

En janvier 2022, nos chercheurs ont détecté pour la première fois une campagne de cloud hybride malveillante, OiVaVoii, et ont découvert cinq applications OAuth malveillantes associées à la campagne[32].

Au moins trois des applications tierces malveillantes ont été créées par deux « éditeurs vérifiés » différents. Ces éditeurs sont probablement des comptes administrateur compromis de locataires Microsoft 365 légitimes. Sur les deux applications restantes, au moins une a été créée par un éditeur non vérifié. Cela suggère que les cybercriminels utilisaient un environnement cloud piraté tiers ou un locataire Microsoft 365 malveillant dédié.

Résultat

Une fois les applications créées, les cybercriminels ont envoyé des demandes d'autorisation par email à de nombreux utilisateurs ciblés, dont des cadres dirigeants. Bon nombre de ces utilisateurs ont autorisé les applications. Cette simple action a permis aux cybercriminels de générer des jetons OAuth au nom de l'utilisateur ciblé et de finalement prendre le contrôle de comptes. Toutes les applications associées à la campagne OiVaVoii ont demandé des autorisations similaires aux utilisateurs, principalement pour l'accès aux boîtes email (lecture et écriture). Une fois les demandes acceptées par les utilisateurs, les cybercriminels étaient libres d'envoyer des emails malveillants tant au niveau interne qu'externe, de voler de précieuses informations et bien plus encore.

Attaques cloud : conséquences potentielles

Prise de contrôle de comptes

Fuite de données (due à l'intrusion de malwares dans l'environnement ou à l'exfiltration directe de données par des applications malveillantes)

Perturbation des activités (due aux ransomwares et autres malwares s'introduisant dans l'environnement)

Comment la sensibilisation des utilisateurs aurait pu aider

Comme la plupart des attaques véhiculées par email, les attaques cloud nécessitent une interaction humaine pour parvenir à leurs fins. C'est pourquoi elles incitent les utilisateurs à divulguer leurs identifiants de connexion, à installer des applications malveillantes et à cliquer sur des URL pointant vers des sites de partage de fichiers de confiance utilisés pour héberger des fichiers malveillants, le tout à leur insu.

Dans le cadre de votre programme de sensibilisation à la sécurité informatique, il est essentiel que vous appreniez à vos collaborateurs à utiliser les services cloud en toute sécurité et à se méfier des demandes d'autorisation provenant d'applications inconnues.

32 Eilon Bendet, Assaf Friedman et David Krispin *(Proofpoint)*, « OiVaVoii – An Active Malicious Hybrid Cloud Threats Campaign » (OiVaVoii, une campagne de cloud hybride malveillante active), janvier 2022.

Pourquoi l'authentification multifacteur n'est pas une solution miracle

De nombreuses entreprises sensibilisées à la sécurité informatique apprennent à leurs utilisateurs à se servir de l'authentification multifacteur comme outil pour protéger leurs comptes, et à juste titre. L'authentification multifacteur permet de protéger les comptes lorsqu'un cybercriminel tente de se connecter avec des identifiants volés. Lorsqu'un utilisateur se connecte, celui-ci est invité à saisir non seulement son nom d'utilisateur et son mot de passe, mais aussi un code envoyé sur son numéro de téléphone, son badge ou sa clé de sécurité physique. L'authentification multifacteur réduit considérablement le risque que les cybercriminels compromettent des comptes à l'aide d'identifiants volés uniquement et doit être intégrée à chaque programme de sécurité.

Cependant, elle n'est pas infaillible. Des kits de phishing simples d'utilisation permettent aux cybercriminels de contourner facilement ces mécanismes de protection. D'après Microsoft, 10 000 entreprises ont été victimes d'attaques contournant l'authentification multifacteur depuis septembre 2021. Après avoir obtenu un accès, les cyberpirates utilisaient des comptes compromis pour lancer des attaques BEC[33].

Ces attaques commencent généralement par un email de phishing. Il est donc primordial d'apprendre aux utilisateurs à repérer et à signaler les messages suspects. Dans le cas de l'attaque Microsoft, les emails de phishing contenaient une pièce jointe au format HTML. Une fois ouvert, le fichier redirigeait vers un serveur proxy qui interceptait le trafic entre les utilisateurs et l'écran de connexion.

Les collaborateurs doivent également apprendre à ne jamais ouvrir une pièce jointe provenant d'un expéditeur inconnu, surtout s'il s'agit d'un type de fichier qui n'est généralement pas envoyé par email.

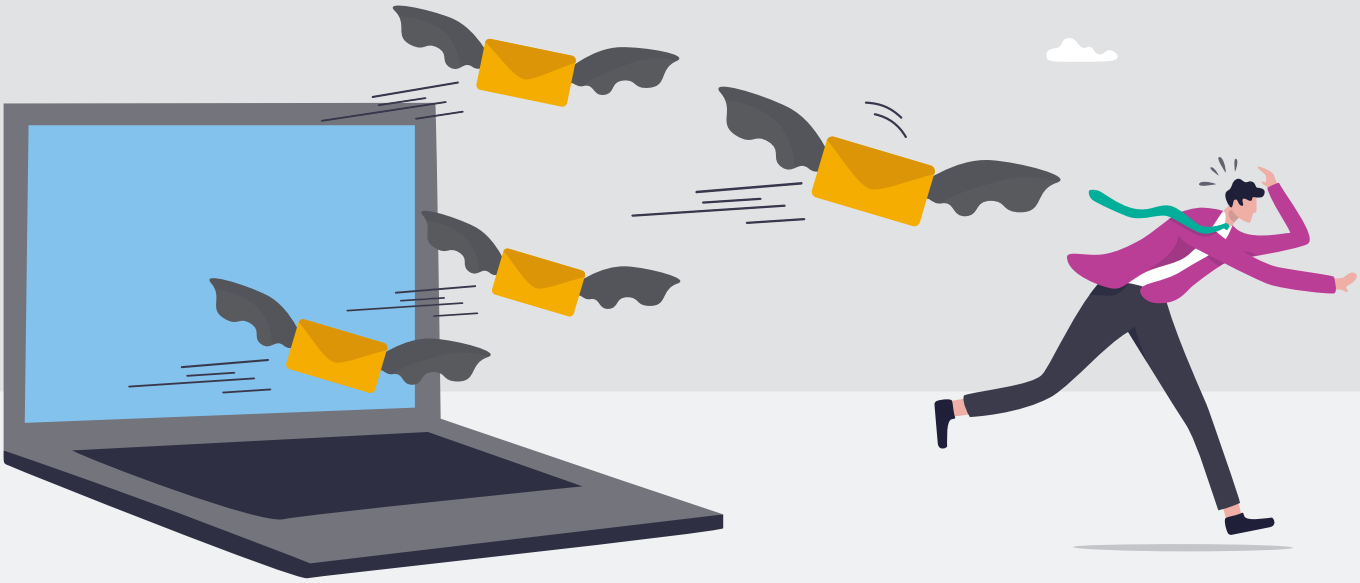
33 Microsoft, « From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud » (Du vol de cookies aux attaques BEC : les cybercriminels utilisent des sites de phishing AiTM comme point d'entrée pour d'autres fraudes financières), juillet 2022.

SECTION 5

Attaques via la messagerie Web

L'essor du télétravail offre aux cybercriminels encore plus d'opportunités d'infiltrer les systèmes d'entreprise. La plupart des collaborateurs ont recours à un réseau privé virtuel (VPN) pour accéder au réseau de leur entreprise lorsqu'ils travaillent à l'extérieur. Par ailleurs, ils utilisent leurs propres terminaux pour se connecter aux ressources d'entreprise, ceux-là mêmes dont ils se servent pour accéder à leur messagerie Web personnelle. À l'inverse, bon nombre de collaborateurs utilisent leurs terminaux d'entreprise pour accéder à leurs comptes personnels.

Si des cybercriminels compromettent les comptes personnels d'un utilisateur, ils peuvent mettre la main sur des identifiants de connexion à des applications, des données et des systèmes d'entreprise. Ils peuvent également profiter du fait que de nombreux collaborateurs utilisent leurs comptes de messagerie ou leurs numéros de téléphone mobile personnels pour l'authentification à deux facteurs ou les réinitialisations de mots de passe. Ces informations sont suffisantes pour permettre aux cybercriminels d'infiltrer les réseaux d'entreprise.

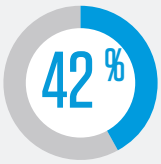


Tendances

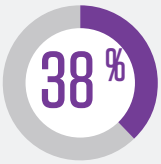
D'après le rapport *State of the Phish 2022*, de nombreux utilisateurs sont susceptibles d'être victimes d'attaques via la messagerie Web qui pourraient mettre en péril leur entreprise.

En outre, il semble que bon nombre d'entre eux partent du principe que leur fournisseur de messagerie Web les protégera contre ces attaques.

Voici les conclusions de nos recherches :



des utilisateurs consultent leur messagerie personnelle sur leurs terminaux d'entreprise



des utilisateurs savent que leur fournisseur de messagerie personnelle ne peut pas bloquer tous les email dangereux

Exemple concret : LAPSUS$

Il arrive que des cybercriminels tiennent tout autant, si ce n'est plus, à créer des perturbations et à faire parler d'eux qu'à engendrer des profits. C'est le cas de LAPSUS$, un groupe cybercriminel spécialisé dans le vol et l'extorsion de données apparu fin 2021. Il se peut que le groupe soit toujours actif, même si plusieurs de ses membres, tous âgés de 16 à 21 ans, ont été arrêtés par la police britannique en mars[34].

Déroulement de l'attaque

En seulement quelques mois, le groupe LAPSUS$ a essayé d'extorquer des données au ministère brésilien de la Santé et a publié des captures d'écran d'outils internes associés à NVIDIA, Samsung et Vodafone[35]. Son approche peu conventionnelle de l'extorsion n'est pas passée inaperçue. Il a subtilisé des données sensibles, puis a menacé de les publier en ligne si la victime ne payait pas. Fondamentalement, il s'agissait d'une attaque de ransomware sans ransomware.

Résultat

Comble de l'audace, le groupe publiait des sondages dans l'application Telegram afin que les utilisateurs votent pour les données de la victime qui seraient publiées en ligne en premier[36]. Pour accéder aux réseaux d'entreprise qu'il souhaitait compromettre, le groupe LAPSUS$ ciblait souvent les comptes de messagerie personnels de collaborateurs pour obtenir des identifiants de connexion afin d'établir un accès à distance[37].

34 Scott Ikeda *(CPO Magazine)*, « Suspected Lapsus$ Hackers Arrested; London Group Between the Ages of 16 and 21 » (Sept suspects âgés de 16 à 21 ans arrêtés pour leurs liens avec le groupe londonien LAPSUS$), mars 2022.

35 KrebsonSecurity, « A Closer Look at the LAPSUS$ Data Extortion Group » (Focus sur le groupe LAPSUS$, spécialisé dans l'extorsion de données), mars 2022.

36 Lily May Newman *(Wired)*, « The Lapsus$ Hacking Group Is Off to a Chaotic Start » (Le groupe de piratage LAPSUS$ déjà dans la tourmente), mars 2022.

37 Microsoft, « DEV-0537 criminal actor targeting organizations for data exfiltration and destruction » (Le groupe cybercriminel DEV-0537 cible des entreprises en vue d'exfiltrer et de détruire leurs données), mars 2022.

Les équipes Microsoft Security nomme le gang LAPSUS$ « DEV-0537 ».

« Contrairement à la plupart des groupes cybercriminels qui font profil bas, DEV-0537 ne semble pas chercher à dissimuler ses activités », explique le géant de l'informatique. « Il va jusqu'à annoncer ses attaques sur les réseaux sociaux et fait part de son intention d'acheter des identifiants de connexion aux collaborateurs des entreprises qu'il a en ligne de mire[38]. »

La campagne de publicité du groupe incluait des messages Telegram, dans lesquels LAPSUS$ essayait de recruter des collaborateurs et autres utilisateurs internes travaillant pour des opérateurs de télécommunications, des géants de l'informatique et du jeu, des opérateurs de centres d'appels et des hébergeurs de serveurs. Son objectif : soudoyer des collaborateurs pour obtenir des identifiants de connexion VPN ou tout autre type d'accès à distance. LAPSUS$ proposait également de l'argent à des utilisateurs internes en l'échange d'informations. Une publicité précisait qu'il était possible de gagner 20 000 dollars au minimum par semaine[39].

Microsoft Security a également signalé que LAPSUS$ avait obtenu un accès initial aux victimes par d'autres moyens, dont l'achat d'identifiants de connexion et de jetons de session sur des forums clandestins et la recherche d'identifiants exposés dans les référentiels de code publics.

Conséquences potentielles des attaques via la messagerie Web

Fuite de données | Perturbation des activités | Pertes financières | Atteinte à la réputation

Comment la sensibilisation des utilisateurs aurait pu aider

Le groupe LAPSUS$ employait plusieurs tactiques, dont les suivantes :

- Compromission de messageries Web et de méthodes d'accès à distance
- Recrutement de collaborateurs, de fournisseurs ou de partenaires commerciaux des entreprises ciblées
- Vol de données sensibles et de propriété intellectuelle
- Demandes de rançon

Montrer aux utilisateurs comment protéger leurs identifiants de connexion, consulter leur messagerie personnelle en toute sécurité et signaler les demandes de rançon aurait grandement aidé à éviter les attaques.

38 Ibid.

39 KrebsonSecurity, « A Closer Look at the LAPSUS$ Data Extortion Group » (Focus sur le groupe LAPSUS$, spécialisé dans l'extorsion de données), mars 2022.

SECTION 6

Conclusions et recommandations

Déterminer le meilleur moyen de former vos utilisateurs au paysage des menaces en constante évolution et de les tenir informés représente un défi de taille. Au bout du compte, votre objectif est de les motiver à être aussi vigilants que vos équipes de sécurité à l'égard des cybermenaces. Ils pourront ainsi devenir des défenseurs proactifs.

Pour que les formations de sensibilisation à la sécurité informatique soient efficaces, vos utilisateurs doivent comprendre les enjeux. Pourquoi doivent-ils se préoccuper des cybermenaces ? Pourquoi la défense de l'entreprise relève-t-elle en partie de leur responsabilité ? Pour faire court, c'est parce qu'ils constituent le nouveau périmètre. Et pour que l'entreprise ait une réelle chance de tenir les cybercriminels modernes à distance, elle doit adopter une approche de la sécurité centrée sur les personnes.

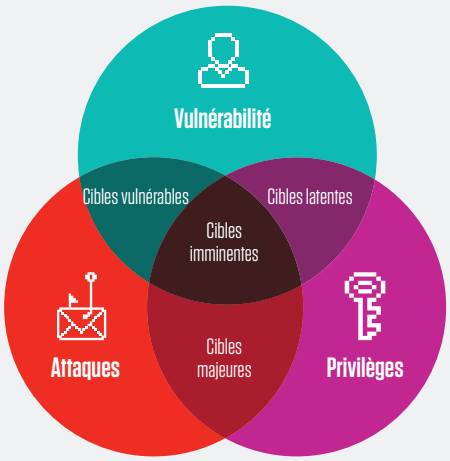
Les cinq types de cybermenaces et les exemples d'attaques abordés dans cet eBook ont un point commun : ils ciblent des personnes. Les cybercriminels se servent des utilisateurs, de leur plein gré ou non, pour faire progresser leurs campagnes et atteindre leurs objectifs.

Ces menaces et incidents prouvent que les collaborateurs constituent le facteur de risque le plus critique dans le paysage des menaces actuel. C'est pourquoi vous devez intégrer des formations de sensibilisation à la sécurité informatique à votre stratégie de cybersécurité.

Donnez la priorité aux thèmes les plus pertinents

Tout collaborateur susceptible d'influencer le niveau de sécurité de votre entreprise doit être formé aux bonnes pratiques de cybersécurité. Vous devez adopter une approche délibérée et stratégique de l'évaluation et de la formation de votre personnel.

Veillez également à aborder en priorité les thèmes que vous savez pertinents pour votre secteur d'activité et votre entreprise — et vos collaborateurs. N'hésitez pas à utiliser les exemples concrets évoqués dans cet eBook afin qu'ils trouvent écho auprès des utilisateurs. Ceux-ci seront forcément confrontés à des attaques similaires en raison de la nature de leur travail, de leur fonction, de leur emplacement et de leurs méthodes de travail, ainsi que d'autres facteurs.



Tirez parti de la threat intelligence

La threat intelligence peut également vous aider à déterminer quand proposer des formations données à des collaborateurs spécifiques. Pour tirer parti des informations sur les menaces connues et émergentes, il est essentiel d'identifier les utilisateurs suivants :

Utilisateurs hautement vulnérables – en fonction de leur comportement, de leur tendance à cliquer sur les emails lors de simulations d'attaques de phishing et de leur participation aux formations

Utilisateurs les plus exposés – utilisateurs qui sont confrontés à des volumes élevés d'attaques, à des menaces particulièrement sophistiquées, à des attaques extrêmement ciblées ou aux trois à la fois

Utilisateurs aux privilèges les plus élevés – utilisateurs qui ont accès aux données, systèmes et autres ressources stratégiques que l'entreprise doit protéger

En résumé, une approche de la sécurité centrée sur les personnes nécessite d'identifier les collaborateurs et les départements de votre entreprise qui sont attaqués et ciblés à un moment donné, ainsi que les méthodes employées par les cybercriminels pour tenter de compromettre vos utilisateurs et votre environnement.

Analysez constamment les indicateurs clés de sensibilisation à la sécurité informatique pour évaluer l'efficacité de vos programmes

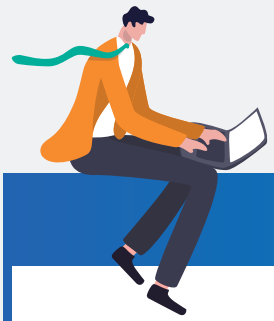
Évitez de vous focaliser sur une seule mesure, comme le taux d'échec aux tests de phishing. Pour évaluer l'efficacité de vos programmes, vous devez vous appuyer sur plusieurs mesures et prendre en compte différents facteurs.

Envisagez d'utiliser les indicateurs suivants :

- Échecs aux simulations d'attaques de phishing
- Signalement des simulations d'attaques de phishing
- Évaluations des connaissances
- Précision des emails signalés
- Participation aux formations

Dernier conseil : n'oubliez pas de maintenir à jour vos formations de sensibilisation à la sécurité informatique dans un paysage des menaces en constante évolution. Sachant que votre entreprise évolue également, assurez-vous que vos conseils sont pertinents pour vos utilisateurs. Les indicateurs mentionnés ci-dessus peuvent vous aider à évaluer en continu l'efficacité de vos programmes et à les ajuster si nécessaire.

Pour en savoir plus sur ces stratégies d'amélioration de vos programmes de formation et de sensibilisation à la sécurité informatique, téléchargez le rapport *State of the Phish 2022* de Proofpoint.



EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.
