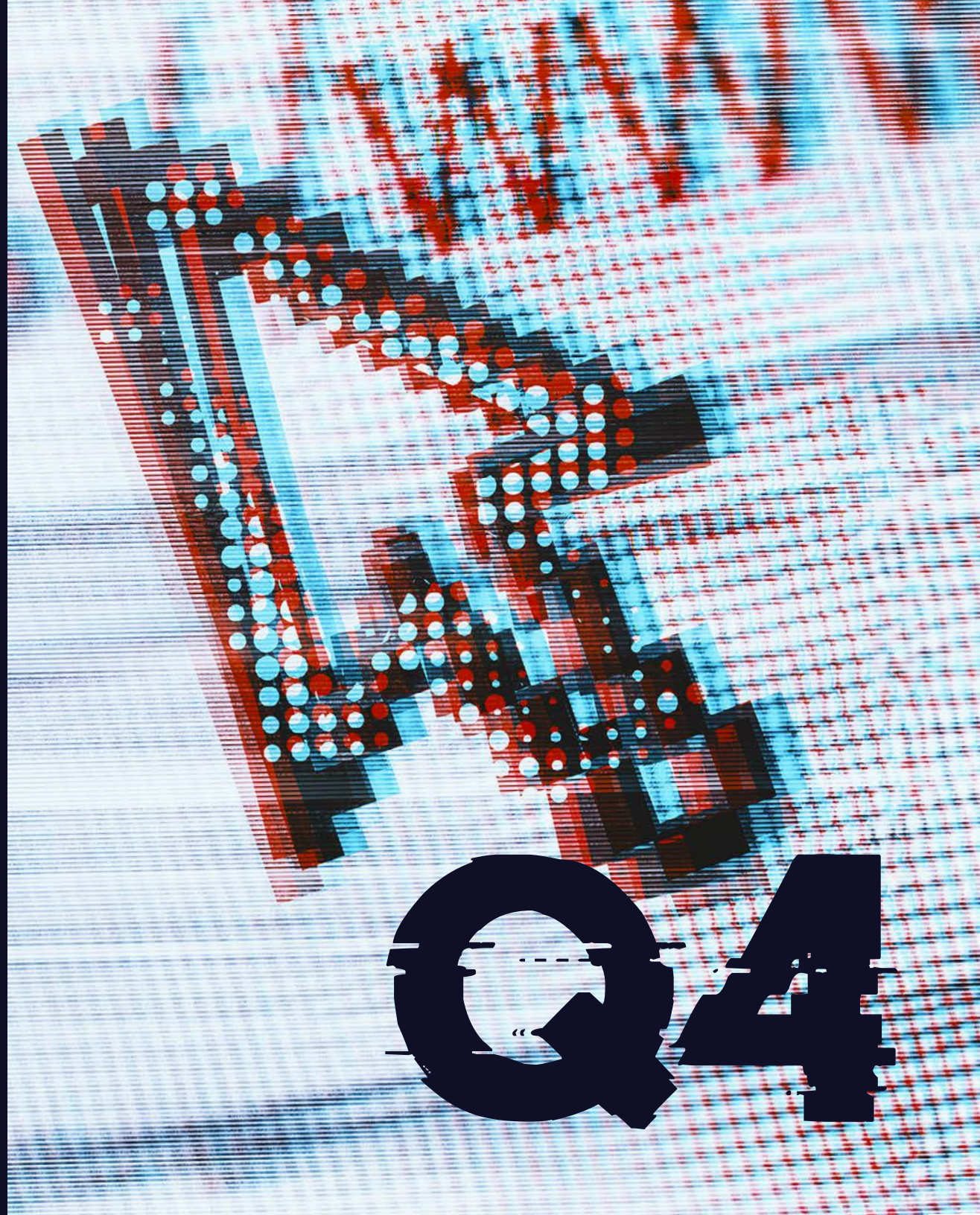
mimecast

Rapport de Renseignement sur les Menaces Mondiales

4ème Trimestre 2023



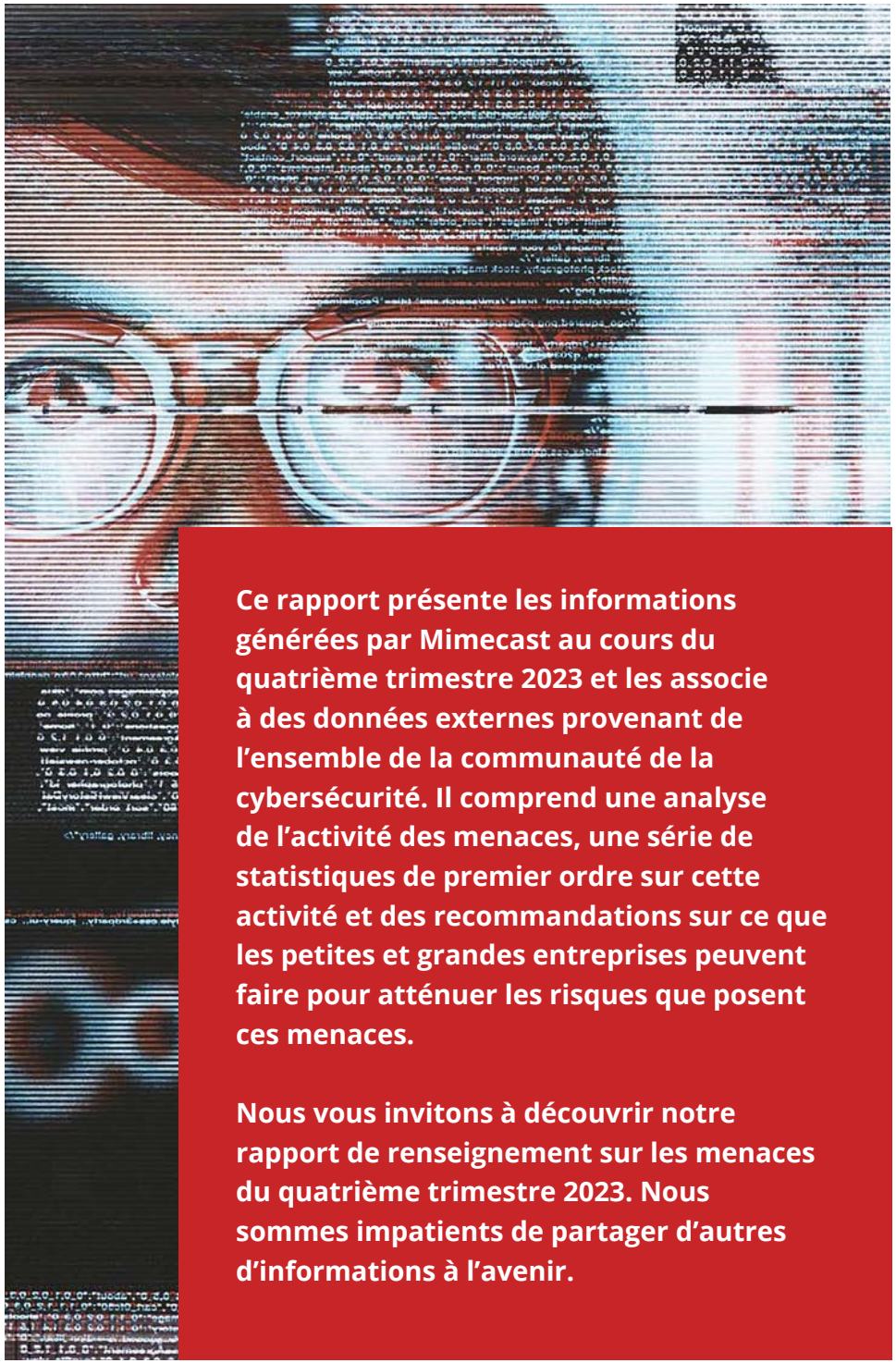
INTRODUCTION

Trop souvent, les organisations reçoivent des renseignements sous forme d'analyses individuelles d'incidents spécifiques, ce qui donne aux équipes de sécurité une vision étroite du paysage des menaces. Dans ce Rapport de renseignement sur les menaces mondiales, Mimecast replace les incidents des trois derniers mois dans leur contexte et fournit aux entreprises les outils dont elles ont besoin pour identifier les cibles des attaquants et les possibilités d'amélioration des défenses.

Mimecast génère des informations sur les menaces en analysant 1,7 milliard d'e-mails par jour pour le compte de plus de 42 000 clients. Le courrier électronique étant le principal vecteur de cyberattaques, Mimecast détecte de nombreuses nouvelles menaces avant qu'elles ne soient largement répandues.

+ 1.7 milliard d'e-mails par jour

42 000 clients



Ce rapport présente les informations générées par Mimecast au cours du quatrième trimestre 2023 et les associe à des données externes provenant de l'ensemble de la communauté de la cybersécurité. Il comprend une analyse de l'activité des menaces, une série de statistiques de premier ordre sur cette activité et des recommandations sur ce que les petites et grandes entreprises peuvent faire pour atténuer les risques que posent ces menaces.

Nous vous invitons à découvrir notre rapport de renseignement sur les menaces du quatrième trimestre 2023. Nous sommes impatients de partager d'autres d'informations à l'avenir.

RÉSUMÉ

Au quatrième trimestre 2023, les attaquants ont continué à modifier leurs méthodes de diffusion en utilisant des liens comme charges utiles initiales, abandonnant progressivement l'envoi de malware sous forme de pièces jointes à des e-mails. En outre, les acteurs malveillants utilisent de plus en plus de codes QR pour contourner les défenses conçues pour bloquer les liens malveillants et masquer leurs attaques.

Après les attaques contre de grands casinos plus tôt dans l'année, les attaquants ont continué à cibler les entreprises de voyage, d'hôtellerie et de restauration au quatrième trimestre 2023, faisant de ce secteur le deuxième le plus ciblé au cours du trimestre, après le secteur bancaire. Bien que les campagnes visant les ressources humaines et les services de recrutement aient quelque peu diminué, ce secteur reste le troisième le plus ciblé.

L'équipe de renseignement sur les menaces de Mimecast

L'équipe de renseignements sur les menaces de Mimecast est composée d'un ensemble d'ingénieurs, de scientifiques, d'analystes et de chercheurs sur les menaces répartis dans le monde entier, qui aident le centre d'opérations de sécurité de Mimecast (MSOC). Les menaces sont surveillées en permanence sur plus de 1,7 milliard d'e-mails par jour. Les experts en cybersécurité de Mimecast procèdent à l'ingénierie inverse des outils d'attaque, enquêtent sur les attaques et testent l'efficacité des indicateurs de compromission afin de générer rapidement des renseignements sur les menaces et des protections pour l'ensemble de nos solutions.

RÉSULTATS CLÉS

Secteurs

Les secteurs qui ont subi le plus d'attaques au quatrième trimestre 2023 sont les institutions financières, le secteur du voyage, l'hôtellerie et la restauration, ainsi que les ressources humaines et les services de recrutement. Ces attaques ont eu lieu sous la forme de ransomware, de vols de données et de compromissions des e-mails professionnels (BEC). De plus, dans tous les secteurs, les utilisateurs moyens des petites et moyennes entreprises ont été confrontés à plus de deux fois plus de menaces que ceux des grandes entreprises.

Liens et pièces

Pour la première fois, l'utilisateur moyen était plus susceptible de rencontrer un lien malveillant qu'une pièce jointe malveillante au quatrième trimestre 2023. Par le passé, les attaquants étaient plus susceptibles d'utiliser des logiciels malveillants connus pour livrer des charges utiles.

Géopolitics

Les tensions géopolitiques se sont accrues, entraînant une augmentation des cyberattaques. En effet, plus de 100 groupes de pirates informatiques ont revendiqué leur participation au seul conflit entre Israël et Gaza. Les États-nations utilisent les cyberopérations pour recueillir des renseignements sur les gouvernements rivaux et attaquer les infrastructures et systèmes d'information critiques.

IA générative

Les attaquants utilisent l'IA générative et des modèles d'apprentissage automatique pour créer des leurres de phishing plus convaincants et traduire les attaques dans d'autres langues. Des indicateurs techniques de la menace, tels que la réputation du domaine, l'isolation du navigateur et l'analyse des malware, seront de plus en plus nécessaires pour bloquer les attaques.

Codes QR

L'utilisation des codes QR pour masquer les liens a continué à se répandre, avec le même objectif que les raccourcissements d'URL, mais avec un avantage supplémentaire pour les attaquants, car les victimes se sont déjà habituées à prendre des photos des codes QR.

LES CAMPAGNES D'EXTORSION SE MULTIPLIENT, LES CYBERATTAQUES SUIVENT LA GÉOPOLITIQUE

Les campagnes de ransomware et de violation avec demande de rançon ont continué de croître au quatrième trimestre 2023. L'un des plus grands groupes de cybercriminels, ALPHV Balckcat, a en effet compromis plus de 1000 victimes avec des ransomwares et des extorsions de données, récoltant plus de 300 millions de dollars de rançons au cours du trimestre.

Les stratégies d'attaque ont évolué, passant des cryptoransomware (les attaquants chiffrent les données et détiennent la clé de déchiffrement) aux campagnes de violation avec demande de rançon (les attaquants volent des données sensibles et menacent de les divulguer à moins d'être payés) et aux stratégies de double et triple extorsion (les attaquants associent plusieurs tactiques pour des conséquences plus directes).

Les groupes de ransomware et de vol de données se sont tournés vers des techniques plus sophistiquées, telles que le vol de jetons et d'identifiants de compte de Google Chrome. Ces stratégies efficaces ont conduit à une consolidation du nombre d'outils de ransomware, avec 43 familles de malware utilisées pour l'extorsion en 2023, contre 95 en 2022. Cela indique que les cybercriminels et leurs affiliés s'installent sur un ensemble connu de plateformes populaires. Quatre groupes (LockBit, Cl0p, ALPHV/BlackCat et Play) ont dominé le paysage des ransomware au cours du trimestre, avec 88% de l'activité totale des ransomware.

Cependant, même si les incidents liés aux ransomware et aux violations de données ont augmenté en 2023, les entreprises résistent aux attaques d'extorsion. Les taux de paiement de rançon ont chuté, atteignant 34% au deuxième trimestre 2023, contre 85% au début de 2019. (Le taux d'acceptation des demandes de rançon par les entreprises a légèrement augmenté au troisième trimestre 2023.) Trois changements au niveau des opérations de sécurité des entreprises et de l'économie des ransomware sont probablement à l'origine de cette évolution : les entreprises font moins confiance à la capacité des cybercriminels à extorquer des données; les organisations ont eu le temps d'améliorer (petit à petit) leur posture de sécurité; et payer des rançons aux auteurs de menaces de certains États-nations constitue désormais une violation des lois fédérales.

Les groupes de ransomware essaient d'inverser la tendance. À partir du 1er octobre, le groupe de ransomware LockBit a mis en place de nouvelles règles concernant les négociations avec les victimes, avertissant ses affiliés qu'il n'est plus acceptable d'offrir des remises importantes sur les frais de rançon.

La situation géopolitique s'est détériorée avec l'attaque terroriste du 7 octobre contre Israël par le groupe militant Hamas. Comme lors d'autres conflits mondiaux, tels que l'invasion de l'Ukraine par la Russie, les cyberattaques se sont multipliées à mesure que les États-nations, les groupes liés à l'un ou l'autre camp et les partisans du hacktivisme ont intensifié leurs attaques contre les sites Web, les infrastructures critiques et les systèmes informatiques. Au moins 90 acteurs malveillants pro-palestiniens et 23 acteurs malveillants pro-israéliens ont mené des attaques au quatrième trimestre 2023.

Certains signes indiquent déjà que les modèles d'apprentissage automatique et l'IA générative modifient également le paysage des menaces. Par exemple, les leurres de phishing deviennent beaucoup plus convaincants et plus faciles à adapter à des zones géographiques spécifiques en raison de l'adoption de l'IA générative par les acteurs malveillants, selon l'équipe de renseignement sur les menaces de Mimecast.

En outre, des chercheurs ont pu charger sur GitHub du code malveillant lié à des composants d'apprentissage automatique, tels que PyTorch, comme des attaques contre d'autres composants de la chaîne d'approvisionnement open-source.

GRAPHIQUES DU QUATRIÈME TRIMESTRE 2023

Les secteurs qui ont subi le plus d'attaques au quatrième trimestre 2023 sont les institutions financières, le secteur du voyage, de l'hôtellerie et de la restauration, ainsi que les services des ressources humaines. Ces attaques ont eu lieu sous la forme de ransomwares, de vols de données et de compromissions des e-mails professionnels (BEC).

De plus, dans tous les secteurs, les utilisateurs moyens des petites et moyennes entreprises ont été confrontés à un plus grand nombre de menaces (deux fois plus en moyenne) que ceux des grandes entreprises.

01. Les PME sont confrontées à deux fois plus de menaces

02. Les liens malveillants se multiplient

03. Le phishing domine et les liens sont le vecteur le plus courant

04. Les attaques augmentent dans tous les secteurs, les attaques ciblant les RH

05. Les principales vulnérabilités au fil du temps

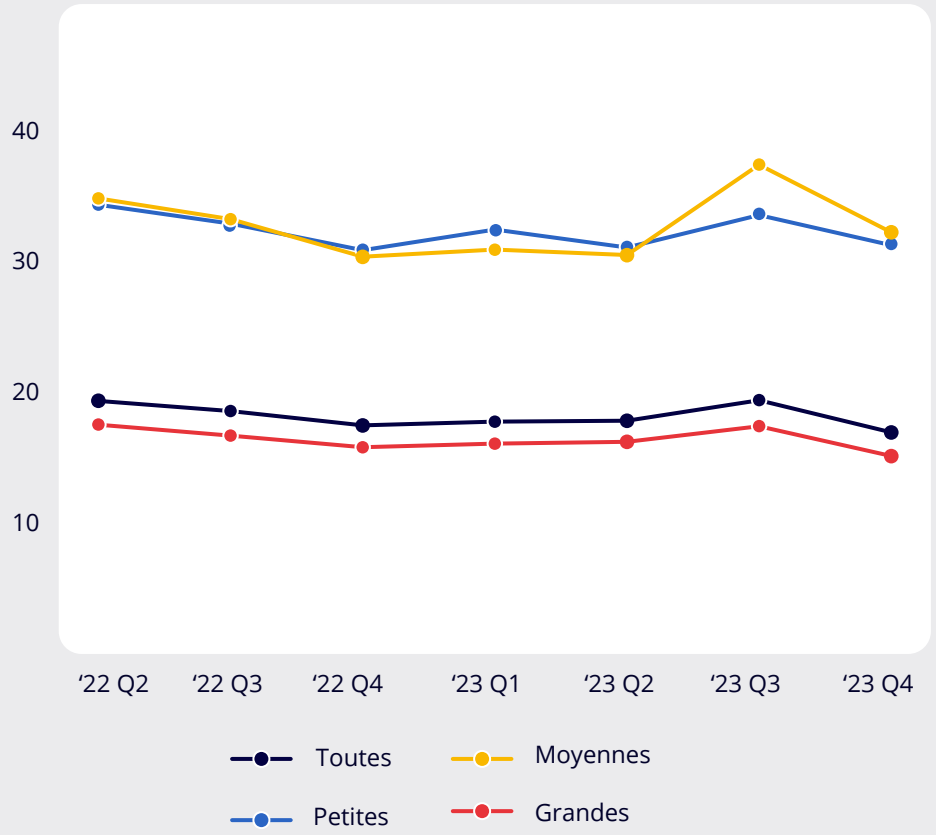
Taux d'occurrence : les PME sont confrontées à deux fois plus de menaces

La hausse significative des menaces observée au troisième trimestre semble s'être atténuée, mais les moyennes entreprises ont tout de même enregistré un peu plus de menaces par utilisateur que les petites entreprises au quatrième trimestre. Les utilisateurs moyens des petites et moyennes entreprises (PME) ont été confrontés à plus de deux fois plus de menaces (31 et 32 menaces par utilisateur, respectivement) que les utilisateurs des grandes entreprises, qui en ont enregistré environ 15 au quatrième trimestre.

Le risque plus important pour les PME est dû à une plus grande proportion d'employés occupant des postes critiques ; cibler ces utilisateurs entraîne un niveau plus élevé de menaces par utilisateur. De plus, comme les PME s'appuient sur des services cloud basés sur des identifiants pour une grande partie de leurs opérations, les attaquants se concentrent davantage sur le vol d'identifiants, un objectif courant de phishing.

Le quatrième trimestre de chaque année a tendance à être marqué par une baisse du volume de menaces par rapport au trimestre précédent. La baisse du nombre de menaces par utilisateur est donc courante dans toutes les organisations.

Graphique 1. Menaces par utilisateur et par taille de l'entreprise

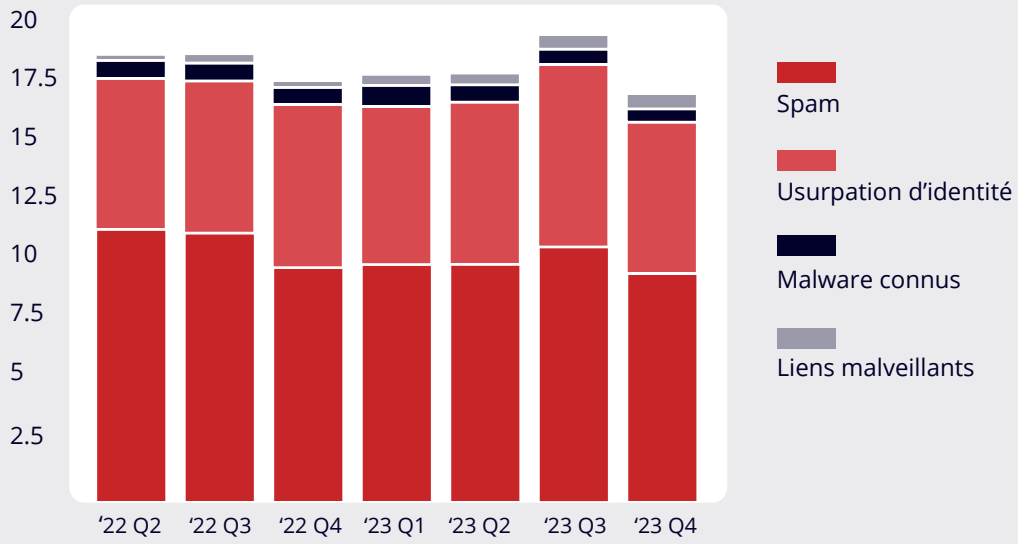


2. Taux d'occurrence : les liens malveillants se multiplient

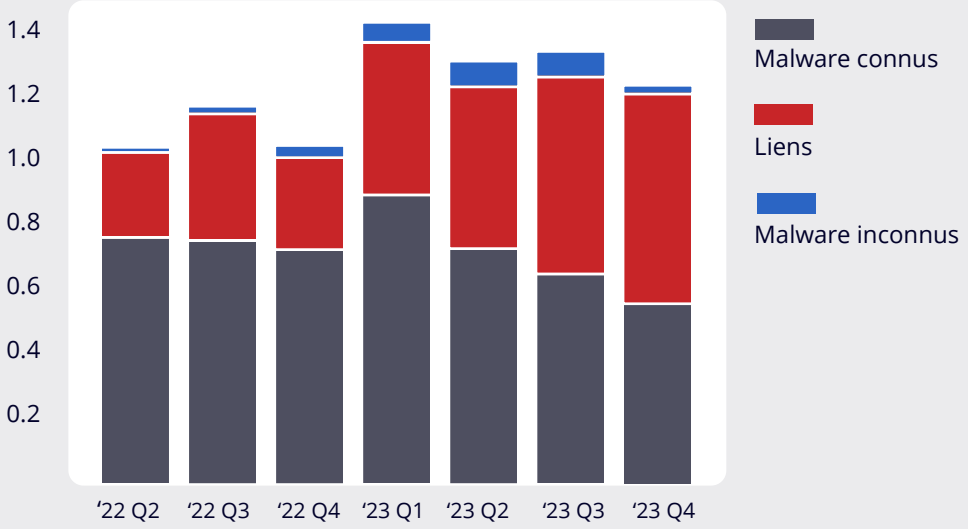
Le spam et l'usurpation d'identité ont tous deux diminué au quatrième trimestre 2023, mais sont restés les principales menaces visant les boîtes de réception des utilisateurs. Les défenses Mimecast ont en effet bloqué respectivement 9,5 et 6,3 e-mails classés comme spam ou usurpation d'identité par utilisateur moyen. La catégorie des malware inconnus, que Mimecast bloque grâce à la détection de codes d'exploitation dans les pièces jointes, est trop petite pour être visible sur le premier graphique.

En supprimant les deux plus grandes catégories de menaces (le spam et l'usurpation d'identité) une autre tendance devient évidente. Pour la première fois, l'utilisateur moyen était plus susceptible de rencontrer un lien malveillant qu'une pièce jointe malveillante au quatrième trimestre 2023. Les utilisateurs ignorant le volume écrasant d'e-mails bloqués pour cause de spam ou d'usurpation d'identité (phishing), les attaquants passent clairement de la livraison de charges utiles sous forme de logiciels malveillants à l'envoi de liens vers des sites malveillants, qui livrent ensuite la charge utile.

Graphique 2a. Menaces par utilisateur et par type de menace



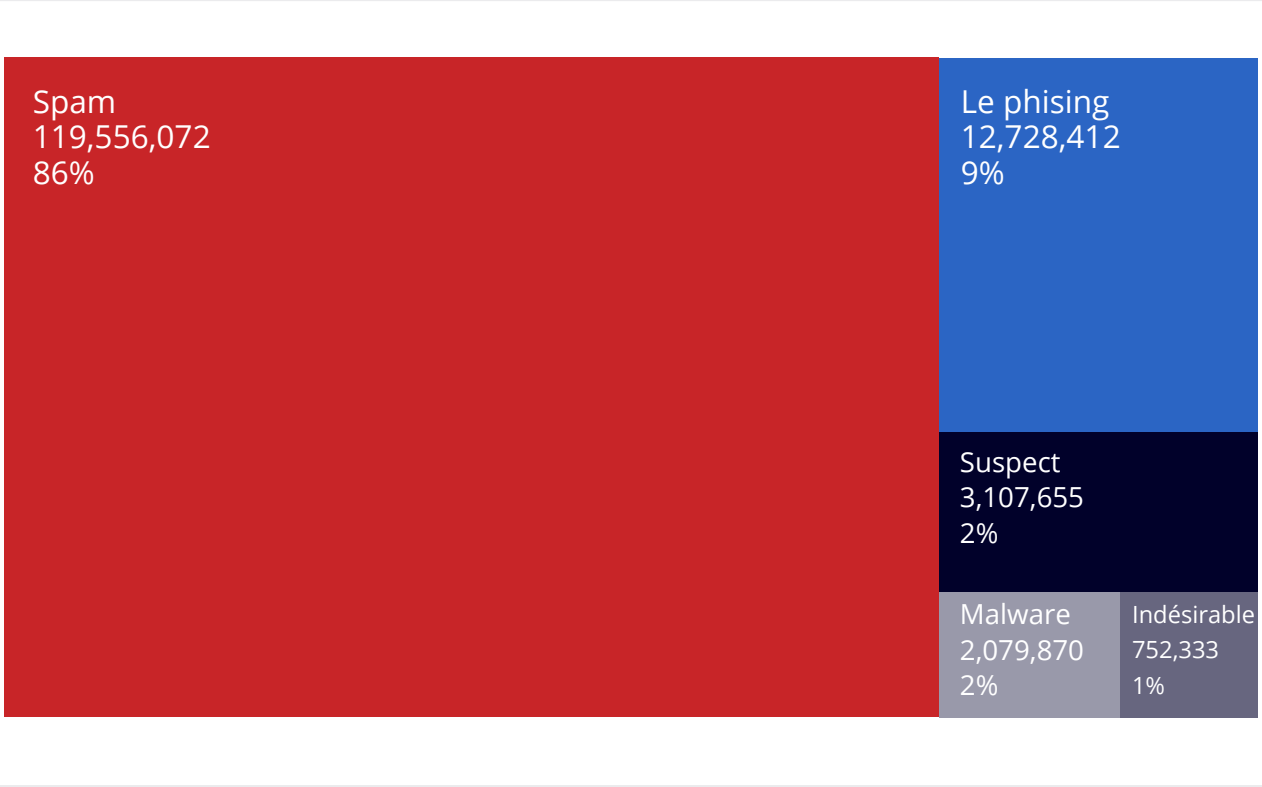
Graphique 2b. Menaces par utilisateur pour les malware et liens malveillants



Types de menaces : le phising domine les menaces actives, les liens étant le vecteur le plus courant

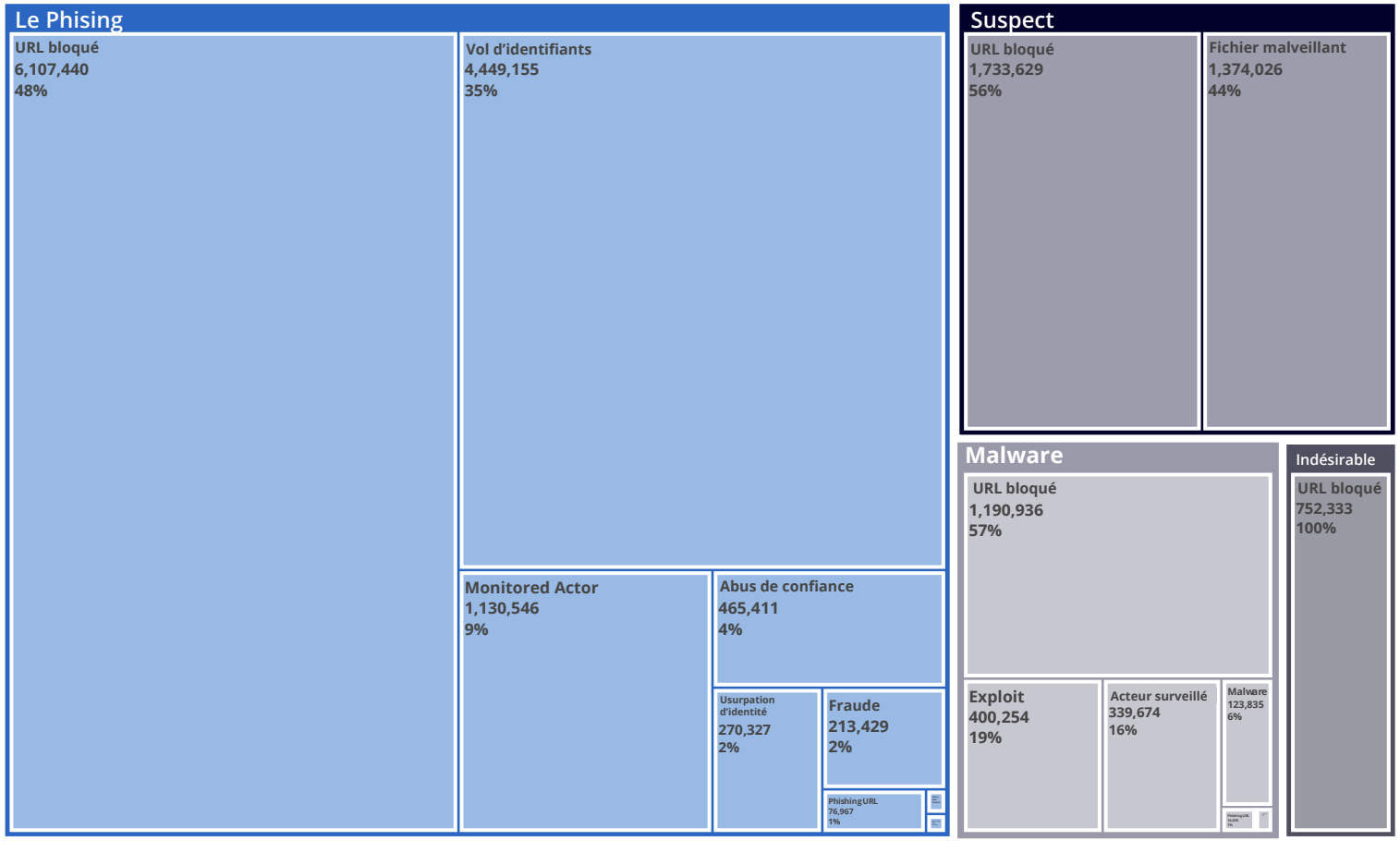
Alors que les spams représentent toujours la majorité des messages malveillants et suspects rejetés, avec 86% de l'ensemble des messages bloqués (voir le graphique 3(a)), l'analyse des principales menaces en dehors du spam met en évidence des tendances intéressantes (voir le graphique 3(b)).

Graphique 3a. Volume relatif de l'ensemble des menaces



Les URL malveillantes représentent toujours la plus grande part des principaux types de détection, y compris le phishing, les malware et les e-mails suspects et indésirables. La collecte d'identifiants est le deuxième attribut le plus détecté dans les attaques de phishing. Cela souligne l'importance d'avoir des identifiants solides et de les renforcer grâce à l'authentification multifacteur pour protéger les entreprises qui adoptent de plus en plus de services et d'infrastructures basés sur le cloud.

Graphique 3b. Logiciels malveillants et liens malveillants

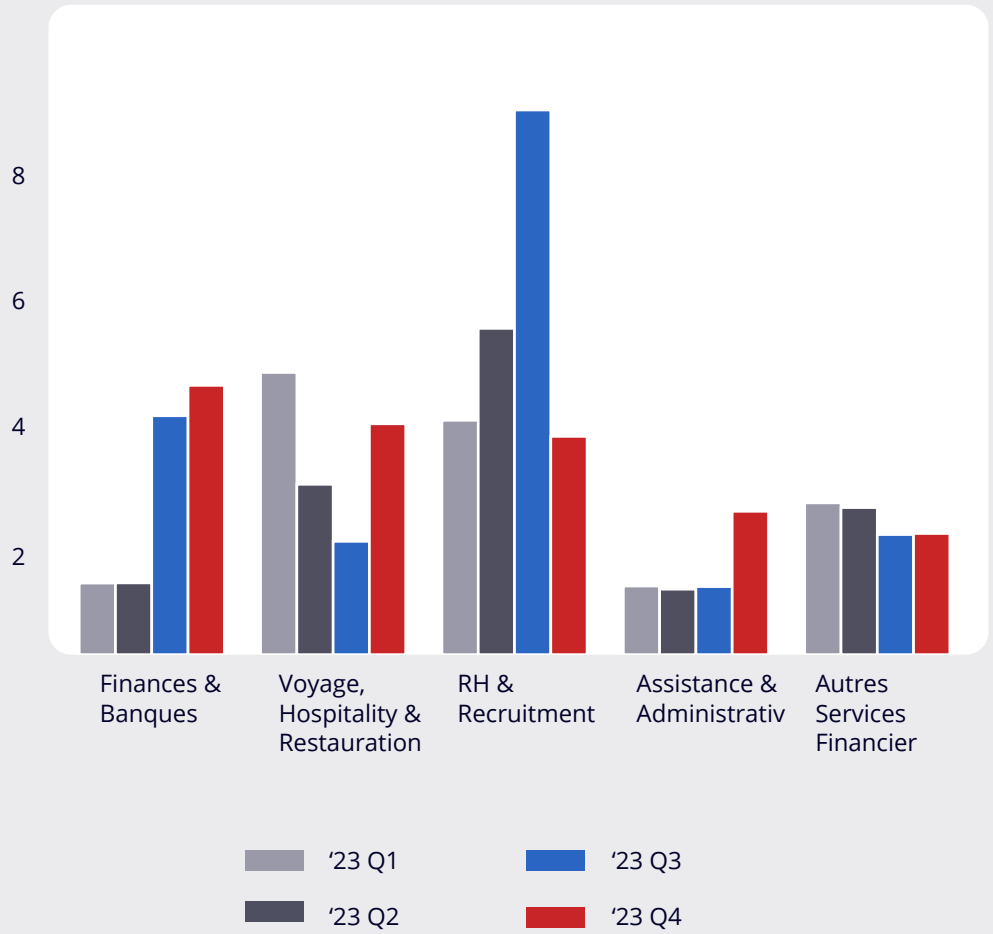


Aperçu du secteur : les attaques augmentent dans tous les secteurs, tandis que les attaques ciblant les RH diminuent

Le nombre moyen d'attaques, hors spam et usurpation d'identité, a baissé au quatrième trimestre 2023. Les utilisateurs du secteur anciennement le plus attaqué (les ressources humaines et les services de recrutement) ont rencontré 60% de menaces en moins qu'au trimestre précédent, ce qui a fait chuter ce secteur à la troisième place au quatrième trimestre 2023. Par ailleurs, le secteur des logiciels informatiques et des logiciels en tant que service est sorti du top 5 des secteurs les plus ciblés, tombant à la 20e place au quatrième trimestre 2023.

Cependant, les autres secteurs ont tous connu une augmentation des menaces les plus importantes, notamment les malware connus, les liens malveillants et les malware inconnus, par rapport au trimestre précédent. Les utilisateurs du secteur bancaire ont continué de faire face à un nombre important d'attaques, tout comme les utilisateurs du secteur des voyages, de l'hôtellerie et de la restauration, y compris les casinos. L'utilisateur moyen, tous secteurs confondus, a été confronté à 1,2 menace au cours du trimestre, soit un peu moins que la moyenne de 1,3 menace par utilisateur au troisième trimestre 2023.

Graphique 4. Top 5 des menaces par utilisateur et par secteur pour les malware et liens malveillants



5

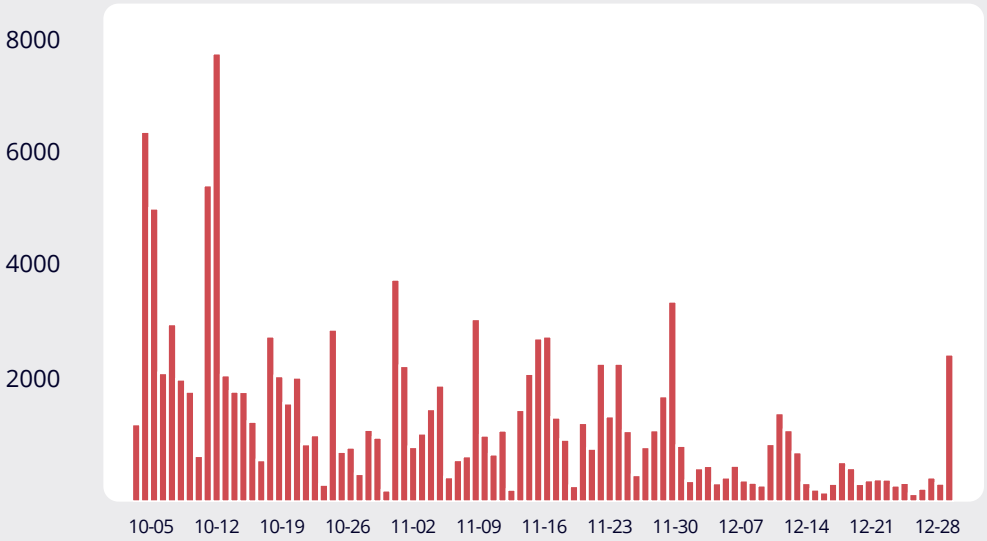
Aperçu des vulnérabilités : les principales vulnérabilités au fil du temps

Le nombre total de vulnérabilités a diminué, ce qui est une tendance typique au cours du quatrième trimestre. En effet, l'activité cesse et les attaquants, tout comme les victimes, font une pause à la fin de l'année.

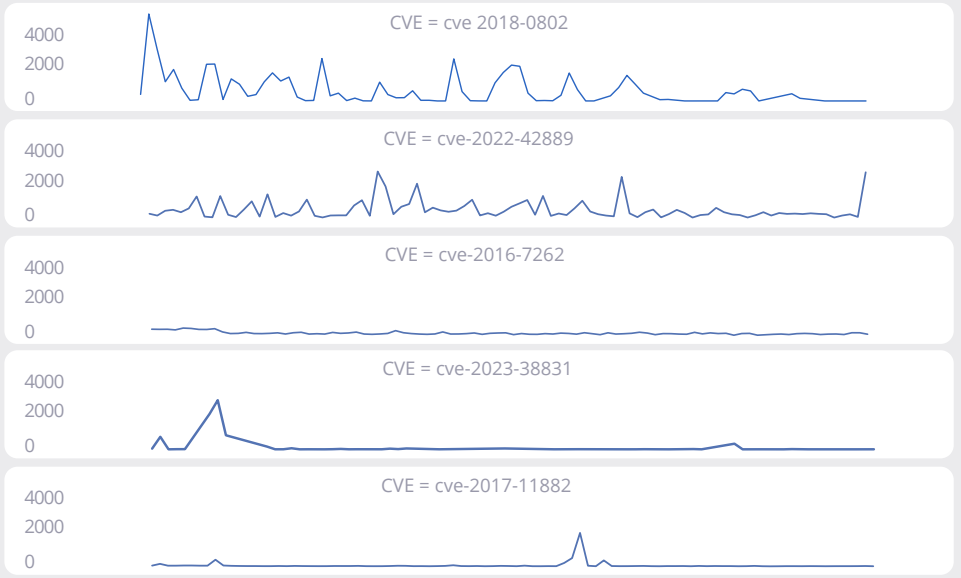
Les cinq principales vulnérabilités ont présenté des modèles d'utilisation distincts. La vulnérabilité la plus courante dans les malwares, à savoir une faille d'exécution de code à distance dans l'éditeur d'équations de Microsoft Office 2007 à 2016 (CVE-2018-0802), a été le principal outil des attaquants au quatrième trimestre 2023. Une autre attaque exploitant une vulnérabilité de corruption de mémoire dans Microsoft Office (CVE-2017-11882) a été peu utilisée jusqu'à un pic au cours de la troisième semaine de novembre, correspondant aux journées d'achat les plus populaires de l'année.

Une seule vulnérabilité du top 5 et seulement deux du top 10 datent de 2023. Cela indique que les attaquants préfèrent exploiter les logiciels qu'ils considèrent comme les plus vulnérables, même si la faille exploitée est généralement ancienne.

Graphique 5a. Nombre total de vulnérabilités bloquées au Q4 2023



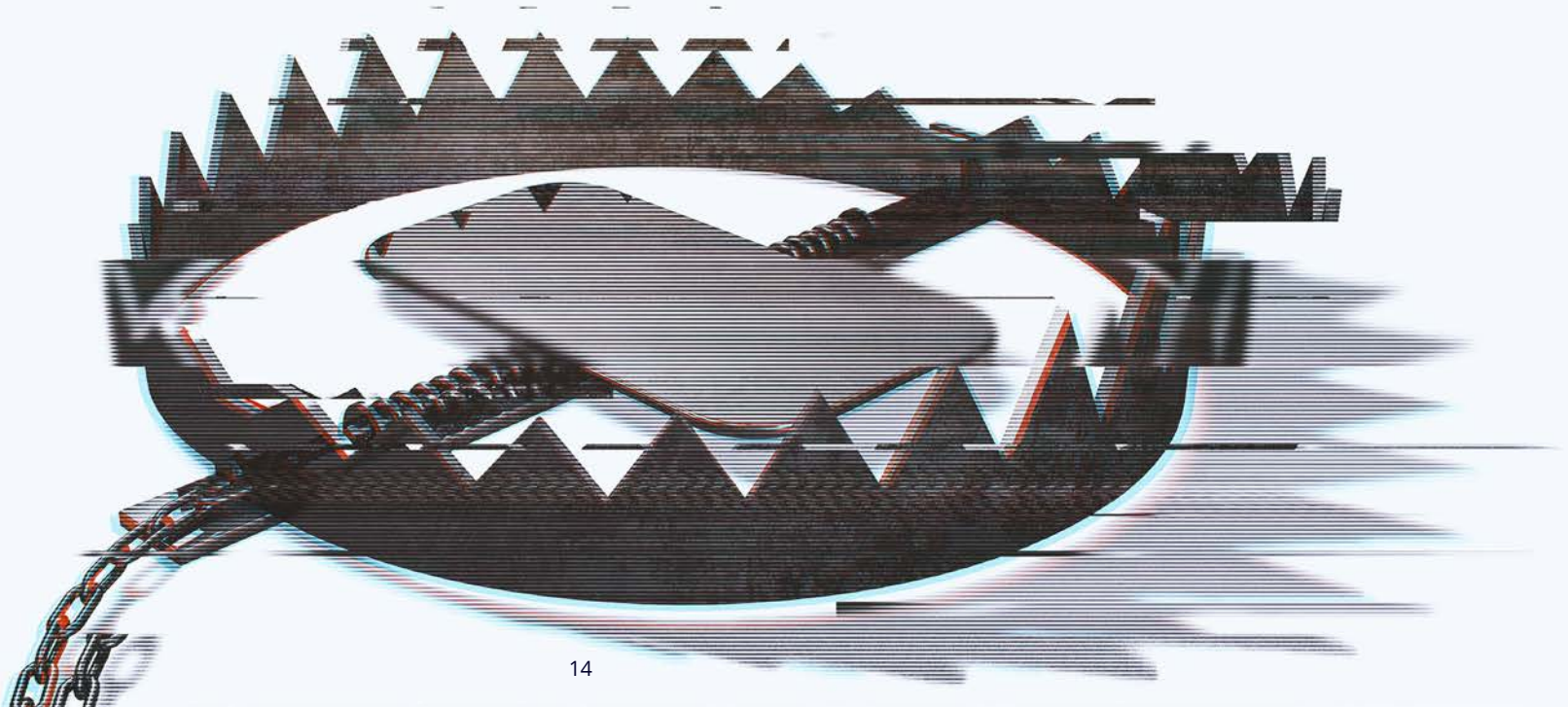
Graphique 5b. Top 5 des détections de vulnérabilités au Q4 2023



L'ABUS DE MARQUE DEVIENT PLUS CONVAINCANT

Presque tous les types d'attaques par e-mail utilisent des marques légitimes pour gagner la confiance des utilisateurs et les convaincre d'effectuer des actions qui compromettent leur sécurité, comme divulguer des informations sensibles ou cliquer sur des liens. Au cours du quatrième trimestre 2023, par exemple, un acteur malveillant a utilisé le service de marketing par e-mail de SendGrid pour envoyer des campagnes par e-mail usurpant l'identité des services des ressources humaines et demandant aux utilisateurs ciblés de cliquer sur un lien semblant provenir d'un serveur Microsoft SharePoint Online.

Alors que les attaquants utilisent de plus en plus l'IA générative pour créer des notifications à l'aspect officiel et abusent de services légitimes pour contourner les défenses axées sur la réputation, les abus de marque vont devenir de plus en plus problématiques.

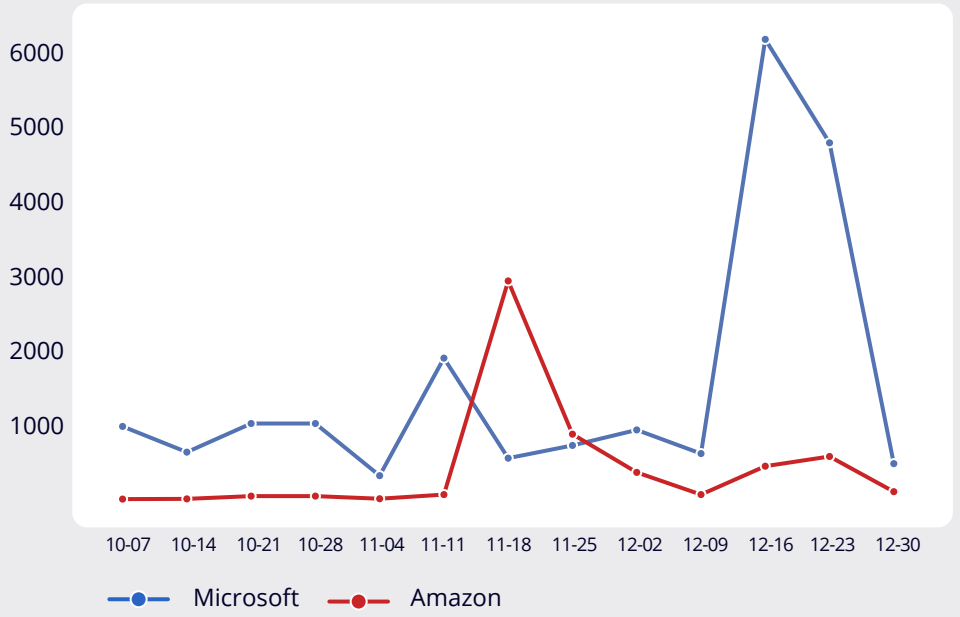


Les attaquants utilisent différentes marques en fonction du contexte

La marque la plus usurpée reste Microsoft, comme l'ont démontré les données de notre rapport du troisième trimestre 2023. Cependant, des événements spécifiques peuvent amener les attaquants à utiliser d'autres marques pour tenter de gagner la confiance des utilisateurs.
En 2020 par exemple, pendant la pandémie de coronavirus, Amazon, Apple et la Social Security Administration ont été les trois marques les plus usurpées.

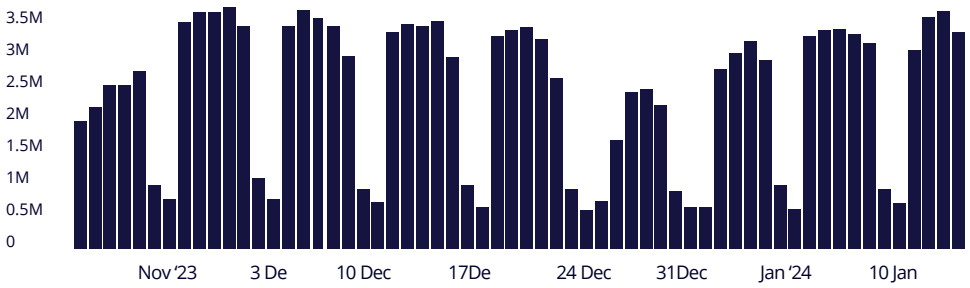
Au quatrième trimestre, les attaquants ont de nouveau modifié leurs tactiques d'usurpation d'identité de marque. Cherchant à tirer parti de la saison des achats de Noël, les fraudeurs ont intensifié leur usurpation de l'identité d'Amazon, entraînant un pic des détections de spam et de phishing pour la marque. Au cours des deux semaines précédant le Black Friday, considéré comme le début de la saison des achats de Noël aux États-Unis, Mimecast a détecté davantage de menaces.

Grahique 6. Les attaquants se concentrent sur Amazon avant les



Dans le même temps, les attaquants utilisent des codes QR pour masquer la destination d'un lien, tout en s'appuyant sur l'image de marque pour convaincre les utilisateurs que les codes QR proviennent de sources officielles. Cette méthode spécifique est devenue courante, comme le montre le nombre d'e-mails contenant des codes QR, qui dépasse régulièrement les 3,5 millions par jour (voir graphique 7). Mimecast a documenté deux campagnes majeures utilisant des codes QR : l'une portant le nom de Microsoft Password Reset et l'autre de DocuSign.

Graphique 7. Détection de codes QR sur 60 jours

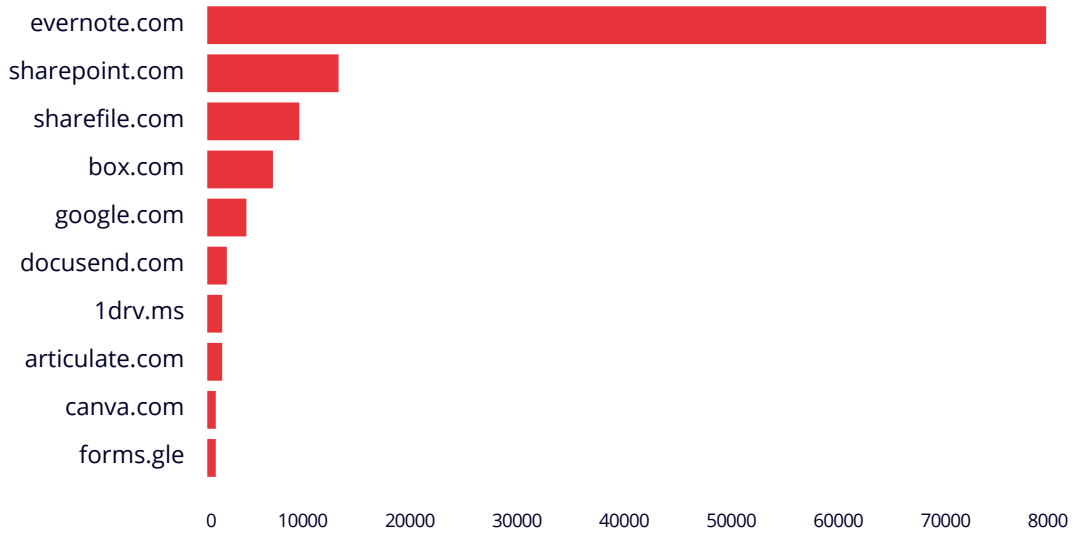


Les abus liés au partage de fichiers concernent les marques

Les attaquants utilisent de plus en plus des liens plutôt que des pièces jointes pour les charges utiles, qu'il s'agisse d'un site de phishing destiné à voler des informations d'identification ou d'un malware à télécharger par la victime. Pour ne pas être détectés par les solutions de sécurité et gagner la confiance des utilisateurs, les attaquants ont largement recours à des sites de partage de fichiers appartenant à des marques de confiance pour diffuser du contenu malveillant (voir graphique 8).

La marque la plus utilisée comme site de partage de fichiers au cours des trois derniers trimestres est le service de prise de notes et de partage Evernote. Microsoft SharePoint arrive loin derrière en deuxième position, suivi du service de stockage géré ShareFile en troisième position.

Graphique 8. Evernote en tête des domaines les plus populaires pour les attaques de phishing

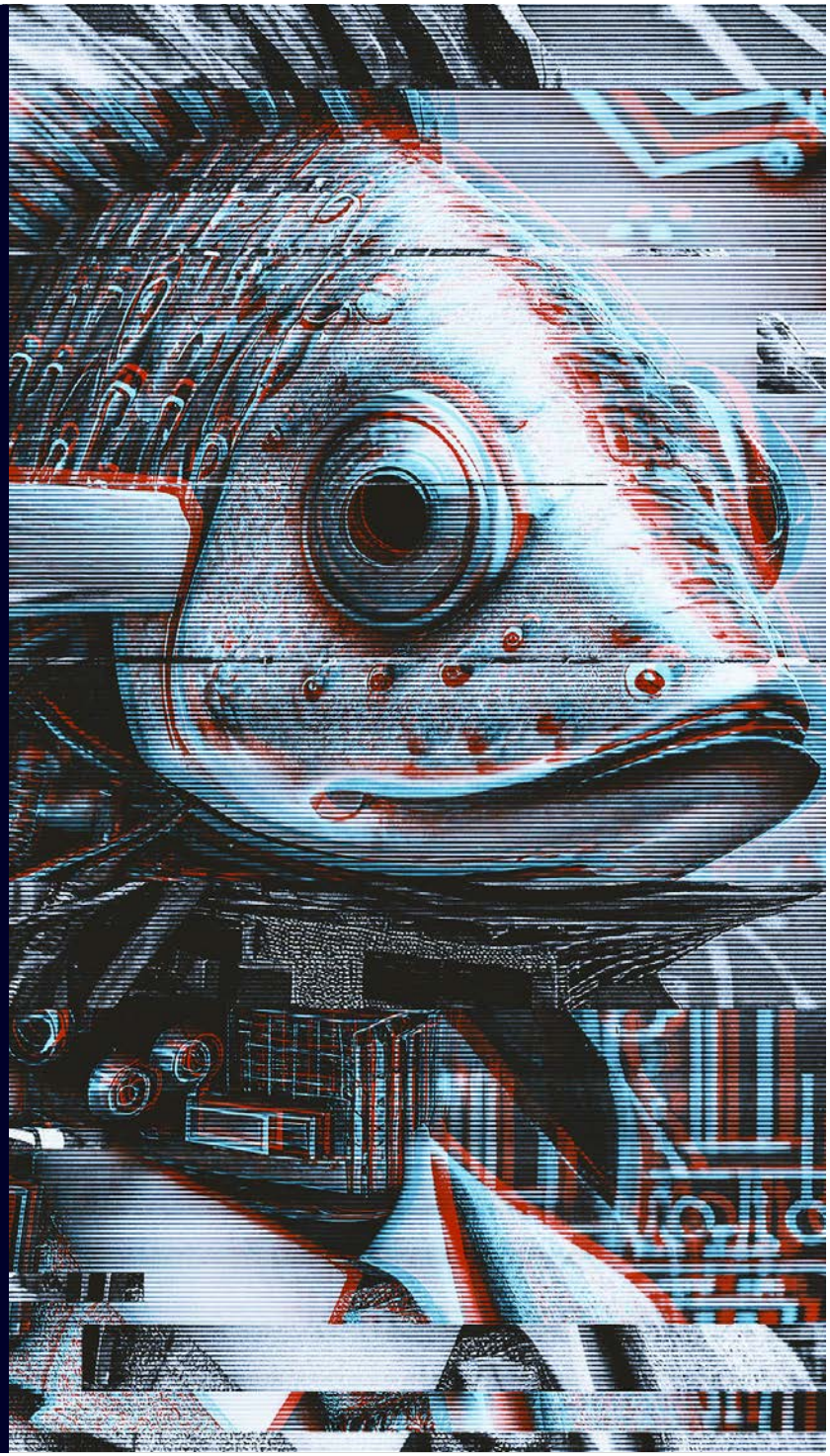


ÉVALUATION DES MENACES

Les attaquants ont redoublé d'efforts pour contourner les mécanismes d'authentification multifacteur (MFA). EvilProxy, une plateforme de phishing en tant que service (PHaaS), a ciblé les secteurs de la finance et de l'assurance en utilisant un proxy pour contourner l'authentification multifacteur, tandis qu'un autre groupe a utilisé la plateforme DadSec PHaaS pour renvoyer les victimes vers un proxy qui fait office d'adversaire intermédiaire (AITM) afin de recueillir les demandes d'authentification multifacteur et compromettre les comptes Microsoft 365 des victimes.

Les opérateurs de ransomware ont continué à cibler davantage les entreprises du secteur de l'énergie au quatrième trimestre. Les courtiers d'accès initiaux (IAB) ont activement recherché des informations d'identification et compromis des systèmes au sein des réseaux des fournisseurs d'énergie.

Les cyberconflits entre États-nations se sont intensifiés à la suite de l'attaque terroriste du Hamas contre des civils israéliens et de la réponse militaire israélienne avec l'invasion de Gaza. En plus des opérations en ligne qui se poursuivent dans le cadre du conflit entre la Russie et l'Ukraine, les cyberattaques parrainées par des États sont devenues plus fréquentes.



ÉVÉNEMENTS MAJEURS AU QUATRIÈME TRIMESTRE

1 Oct

Les attaques de phishing se poursuivent contre le secteur de l'hôtellerie et de la restauration

Les cybercriminels ont ciblé le secteur hôtelier avec des attaques de phishing sophistiquées conduisant à des violations, comme celles qui ont visé MGM et Caesars. Les données de Mimecast montrent que le secteur de l'hôtellerie a été la cible n° 2 au quatrième trimestre.

LIRE L'ARTICLE

3 Oct

Une attaque de phishing d'EvilProxy cible des entreprises américaines

Les chercheurs décrivent une attaque utilisant des e-mails déguisés en notifications du site d'emploi Indeed.com présentant une vulnérabilité de redirection.
L'attaque a été lancée via la plateforme PHaaS EvilProxy et visait des dirigeants des secteurs de la banque et de l'assurance.

LIRE L'ARTICLE

9 Oct

Les hacktivistes se lancent dans le conflit entre Israël et le Hamas des deux côtés

Des dizaines, voire des centaines, de sites et de réseaux ont été attaqués alors que les cyberopérations s'intensifiaient à la suite de l'attaque terroriste du Hamas contre Israël et de la réponse militaire israélienne qui a suivi. Le Comité international de la Croix-Rouge a publié des règles d'engagement pour les pirates informatiques civils afin de minimiser les dommages causés aux civils pendant la guerre.

LIRE L'ARTICLE

17 Oct

Les attaquants combinent DadSec Phishing et Cloudflare

Utilisant une combinaison désormais classique pour contourner l'authentification à deux facteurs, une attaque de phishing AitM a envoyé de faux e-mails contenant un lien, l'outil Turnstile de Cloudflare pour la vérification humaine et un faux site Microsoft 365 pour convaincre les utilisateurs de dévoiler leurs identifiants de connexion et leurs codes à deux facteurs.

LIRE L'ARTICLE

18 Oct

Des acteurs parrainés par l'État s'en prennent à WinRAR Flw

L'acteur malveillant Sandworm, lié à la Russie, également connu sous les noms de FrozenBarents et Black Energy, s'est fait passer pour une école de formation ukrainienne à la guerre par drones et a envoyé un fichier ZIP malveillant exploitant une vulnérabilité de l'utilitaire d'archivage WinRAR.

LIRE L'ARTICLE

6 Nov

Un groupe iranien cible des secteurs israéliens

Le groupe Agonizing Serpens, lié à l'Iran, a poursuivi sa campagne de vol et d'effacement de données visant les secteurs de l'enseignement supérieur et de la technologie en Israël. Ces attaques ne sont pas liées à une demande de rançon, mais visent à provoquer une perte massive de données.

LIRE L'ARTICLE

12 Nov

Le secteur de l'énergie fait face à un nombre d'attaques croissant

Pendant l'hiver, les courtiers d'accès initiaux (IAB) ont activement recherché des informations d'identification volées et d'autres méthodes visant à compromettre les réseaux d'énergie. Les attaques de ransomware signalées contre le secteur de l'énergie ont augmenté jusqu'à la fin de 2023, en particulier en Amérique du Nord, en Asie et dans l'Union européenne (UE).

LIRE L'ARTICLE

29 Nov

Des attaques de phishing visant les services financiers diffusent le malware LUMMA

Des e-mails de phishing utilisant de fausses factures ont redirigé les utilisateurs vers un site malveillant, les renvoyant ensuite vers un fichier JavaScript qui installe le malware LUMMA occasionnant le vol des informations.

LIRE L'ARTICLE

6 Dec

Les protections de ChatGPT peuvent être contournées pour créer des e-mails de phishing

La BBC a utilisé la version payante de ChatGPT et l'ingénierie d'invite pour créer un bot privé appelé Crafty Emails qui a exécuté presque toutes les tâches de phishing malveillantes demandées par le service de presse. Le service a créé des variantes d'escroqueries populaires, telles que « Hi Mum » qui consiste à demander de l'argent à un parent, et des e-mails de spear-phishing. Le bot a également facilité la création de versions culturellement distinctes.

LIRE L'ARTICLE

19 Dec

Les forces de l'ordre ferment le site ALPHV

Les sites de fuite de données et de négociation du gang de ransomware ALPHV/ BlackCat ont disparu d'Internet, suite à une intervention signalée des forces de l'ordre.Le ministère américain de la Justice a affirmé avoir fermé les sites et offert à 500 victimes un outil de décryptage, mais le groupe aurait ensuite récupéré l'accès aux sites.

LIRE L'ARTICLE

PRINCIPALES CAMPAGNES DE MENACES AU QUATRIÈME TRIMESTRE

Chaque trimestre, nous sélectionnons un sous-ensemble de menaces à analyser dans ce rapport. Certaines campagnes ont un volume important, comme en témoignent les graphiques (voir ci-dessous) montrant le nombre de menaces détectées au cours du trimestre, tandis que d'autres présentent des techniques d'attaque ou de ciblage intéressantes.

Codes QR Microsoft

Depuis la pandémie, les codes QR sont devenus extrêmement populaires et Mimecast bloque régulièrement des campagnes utilisant ce code-barres de nouvelle génération pour masquer les liens. Les consommateurs et les employés utilisent de plus en plus les codes QR, que ce soit pour accéder à un menu numérique dans un restaurant, recueillir des informations sur un événement ou installer un nouveau logiciel en cliquant sur un lien. Par conséquent, les internautes sont moins méfiants à l'égard des liens masqués, ce qui les rend plus enclins à scanner les codes en contournant la sécurité de l'entreprise.

Au cours du quatrième trimestre, Mimecast a identifié une tentative de phishing qui usurpe l'identité d'une entreprise et demande à la victime ciblée de configurer l'authentification Microsoft. Comme le contenu de l'e-mail est une image et que l'utilisateur n'a pas à cliquer dessus, de nombreuses solutions de sécurité ne détectent pas l'attaque. Une fois scanné, le lien derrière le code QR renvoie l'utilisateur vers une page qui tente de récupérer ses informations d'identification Microsoft Office 365.

Codes QR Docusign

Les attaquants ne privilégient pas seulement les codes QR pour du phishing usurpant la marque Microsoft ; ils abusent également d'autres infrastructures. Au quatrième trimestre, Mimecast a identifié une campagne visant le service de partage de documents sécurisé DocuSign. La campagne dissimule un lien malveillant sous la forme d'un code QR censé mener à un document partagé par un service de paie.

Attaques par Google app script

Les attaquants ont mené plusieurs campagnes en utilisant Google App Script, une plateforme de développement rapide d'applications conçue pour créer des applications professionnelles à intégrer dans Google Workspace. Basé sur JavaScript, Google App Script peut accéder aux données de Gmail, du calendrier et des espaces de stockage personnels de Google. Les acteurs malveillants ont détourné cette technologie en utilisant des vulnérabilités logicielles afin de créer des pages de phishing et utiliser les applications liées pour diffuser des malware.

Campagne de spam fauduleuse ciblant la Banque du Mexique

Un groupe de fraude bancaire a lancé en décembre une importante campagne basée sur des URL, visant principalement les pays d'Amérique latine, en particulier le Mexique. Le groupe utilise des campagnes de spam modestes, composées de 1 000 à 6 000 e-mails envoyés à partir de domaines enregistrés par l'acteur malveillant. Les victimes qui cliquent sur les liens contenus dans les e-mails téléchargent des malware sur leurs systèmes. Mimecast a identifié deux formats d'URL utilisés par le groupe dans ses campagnes, qui remontent à avril 2023.

Usurpation d'identité sur Instagram

Une autre campagne importante se fait passer pour Meta Instagram avec une notification qui semble indiquer une violation du droit d'auteur. Les versions initiales de l'alerte ne sont pas convaincantes, car elles contiennent des fautes de grammaire et emploient un ton très informel. Les attaquants utilisent toutefois des services d'infrastructure cloud légitimes, tels que Salesforce, pour envoyer les notifications, ce qui permet aux messages de contourner les filtres initiaux.
L'objectif du groupe à l'origine de ces attaques est de permettre aux attaquants de contourner l'authentification à deux facteurs et d'accéder aux comptes.

PRINCIPAUX AVERTISSEMENTS

Des sources gouvernementales ont publié de nombreux avis axés sur la sécurité des entreprises au cours du trimestre, notamment des avertissements sur l'utilisation continue du spear phishing par le groupe russe Star Blizzard et le recours accru à des tiers non sécurisés pour compromettre des cibles. En outre, la NSA et la CISA ont dressé une liste de dix erreurs de configuration courantes en matière de cybersécurité qui pourraient conduire à une violation.

5 Oct [NSA/CISA] Les équipes rouge et bleue de la NSA et de la CISA partagent les dix principales erreurs de configuration en matière de cybersécurité

La National Security Agency (NSA) et la Cybersecurity and Infrastructure Security Agency (CISA) ont publié une liste des 10 erreurs de configuration les plus courantes en matière de cybersécurité dans les grandes organisations, telles que le fait de laisser les applications dans leur configuration par défaut et le manque de segmentation du réseau. Pour chaque mauvaise configuration, les agences ont également répertorié les tactiques, techniques et procédures les plus utilisées par les attaquants. **RÉFÉRENCE**

7 Nov [FBI] Les acteurs du ransomware continuent d'utiliser des tiers et des outils système légitimes

Les attaques ont ciblé des fournisseurs de services tiers et des outils de gestion pour compromettre des entreprises ciblées, souvent dans les secteurs du jeu et de l'hôtellerie. Les attaques contre les fournisseurs de jeux tiers ont ciblé les petits casinos et les casinos tribaux, tandis que les attaques par callback-phishing ont conduit à des vols de données et à l'installation de ransomware sur les systèmes des entreprises. **RÉFÉRENCE**

16 Nov [FBI/CISA] Le vol et l'extorsion de données ciblent les entreprises par l'intermédiaire de fournisseurs informatiques tiers

Le Federal Bureau of Investigation (FBI) et la CISA ont publié une analyse du groupe Scattered Spider, qui se fait passer pour du personnel du service d'assistance informatique et demande aux employés d'utiliser des outils d'accès à distance commerciaux, en contournant l'authentification multifactorielle. **RÉFÉRENCE**

7 Dec [NCSC/NSA/FBI/CISA/ACSC/CCCS] L'acteur malveillant russe du FSB Star Blizzard poursuit ses campagnes de spear phishing dans le monde entier

Le groupe Star Blizzard, lié à la Russie, a ciblé une grande variété d'organisations avec des attaques de spear phishing basées sur des leurres bien documentés et des contacts sociaux et professionnels, avec pour résultat final la transmission d'un lien malveillant. Le groupe semble cibler principalement des entreprises aux États-Unis et au Royaume-Uni, mais des campagnes ont également visé des organisations dans les pays de l'OTAN et les pays voisins de la Russie. **RÉFÉRENCE**

19 Dec [CISA/FBI] #StopRansomware : ALPHV Blackcat

Le FBI et la CISA ont publié un avis conjoint décrivant les indicateurs de compromission (IoC) du dernier ransomware diffusé par le groupe ALPHV/BlackCat, ALPHV Blackcat Ransomware 2.0 Sphynx. En septembre 2023, le groupe avait compromis plus de 1 000 entités, dont les trois quarts aux États-Unis, et collecté près de 300 millions de dollars de paiements de rançon. **RÉFÉRENCE**

COMMENT AGIR

Les cybercriminels et les acteurs malveillants ciblent généralement des postes privilégiés, des vulnérabilités non corrigées, des chaînes d'approvisionnement précaires et des tiers. Les organisations doivent prendre des mesures pour protéger les utilisateurs les plus privilégiés et trouver des moyens de ralentir les attaquants.

- Contre-mesures spécifiques à la menace
- Recommandations générales pour lutter contre les menaces
- Étapes spécifiques aux clients de Mimecast

Contre-mesures spécifiques à la menace

Contre-mesures spécifiques à la menace Protéger les postes sensibles

Les attaquants s'attaquent généralement à des postes commerciaux spécifiques. Les organisations doivent donc isoler certains membres de leur personnel des contenus potentiellement malveillants, tels que les exécutables et les scripts contenus dans les documents. Par exemple, les commerciaux et les cadres ne devraient pas recevoir ou exécuter de code, tandis que les administrateurs informatiques devraient être surveillés à l'aide de la détection des comportements anormaux.

Ralentir les attaquants en utilisant la segmentation et la tromperie

Certains attaquants, en particulier les groupes de ransomware tels que Cl0p, développent leurs propres exploits de type zero-day pour cibler des vulnérabilités jusque-là inconnues. La segmentation du réseau permet d'isoler les parties sensibles du réseau des acteurs malveillants, tandis que les techniques trompeuses, telles que les honeytokens, peuvent à la fois ralentir les attaquants et alerter les défenseurs.

Développer une stratégie de chaîne d'approvisionnement sécurisée

Les attaquants ciblent de plus en plus les tiers et les services professionnels comme voies alternatives d'accès aux réseaux ciblés. Les entreprises doivent définir des exigences minimales en matière de sécurité pour leurs partenaires et fournisseurs de services et trouver des moyens de mesurer la conformité à ces exigences. Il est également recommandé d'effectuer les transactions par le biais de systèmes dédiés ou authentifiés, ce qui renforce la méfiance des utilisateurs lorsqu'ils reçoivent des demandes de paiement par e-mail.

Sensibiliser les utilisateurs et bloquer les codes QR malveillants

Les codes QR ont pris leur essor et les attaquants cherchent à masquer l'utilisation d'images pour insérer des liens vers du spam, du phishing et d'autres attaques par e-mail. En plus d'empêcher le chargement d'images par défaut*, les organisations doivent sensibiliser leurs employés aux dangers que représentent les codes QR. Mimecast permet de déterminer si un code QR conduit à une charge utile malveillante et, si c'est le cas, de le bloquer.

Remarque : les utilisateurs de CyberGraph doivent utiliser des sites de confiance pour s'assurer que les bannières se chargent correctement.

Recommandations générales pour lutter contre la menace

Évaluer vos surfaces d'attaque

Avec la migration de nombreuses organisations vers les services cloud, la surface d'attaque globale s'est accrue. Les entreprises doivent adopter une approche de type zero-trust pour l'accès des employés aux ressources de l'entreprise, en exigeant une nouvelle authentification si nécessaire et une visibilité stricte sur tous les actifs.

Réduire la surface d'attaque en bloquant les services non utilisés

Si une entreprise n'utilise pas ou ne prévoit pas d'utiliser certains hébergeurs de contenu et certains sites Web, ceux-ci doivent être bloqués. Par exemple, si Dropbox n'est pas une norme de l'entreprise, il ne devrait pas être autorisé. De même, si les documents Excel ne doivent pas être envoyés par e-mail, des contrôles doivent être mis en place pour empêcher de telles actions.

Hiérarchiser les vulnérabilités à corriger

Les attaquants continuent de réduire le délai entre la divulgation d'une vulnérabilité et la diffusion d'exploits et d'attaques ciblant les problèmes de sécurité identifiés. La liste des vulnérabilités exploitées connues (KEV) gérée par la Cybersecurity and Infrastructure Security Agency (CISA) américaine est passée à 1 053 failles logicielles à la fin du quatrième trimestre 2023. Cependant, corriger toutes les failles de la liste KEV n'est pas suffisant. Les entreprises doivent utiliser différents indicateurs de vulnérabilité et leur connaissance des systèmes critiques pour hiérarchiser les correctifs.

Rendre les identifiants résistants au phishing

Nos données (voir graphique 3) montrent que le phishing est le deuxième type d'attaque le plus courant après le spam, les attaquants utilisant généralement les e-mails pour voler les informations d'identification des utilisateurs. Voilà pourquoi les organisations doivent essayer de minimiser l'impact d'une attaque de phishing réussie. L'adoption d'un facteur d'authentification supplémentaire, en particulier d'une technologie résistante au phishing, peut permettre de réduire significativement les attaques basées sur des identifiants dans le cadre d'une approche zero-trust en matière de sécurité. Les entreprises qui ajoutent une authentification multifacteur omniprésente à leur infrastructure cloud et interne réduisent leur risque d'un ordre de grandeur.

Étapes spécifiques aux clients de Mimecast

- Il est recommandé d'utiliser l'authentification unique de votre fournisseur d'identité ou l'authentification multifacteur intégrée de Mimecast pour réduire la capacité des attaquants à utiliser l'e-mail comme vecteur d'attaque. **EN SAVOIR PLUS**

- Assurez-vous que les politiques d'authentification DNS respectent les enregistrements DMARC. Une deuxième stratégie étendue à un groupe de stratégies avec l'action Échec DMARC définie sur Ignorer/Gérer et Expéditeurs autorisés permet de contourner efficacement tout e-mail légitime rejeté/mis en quarantaine en raison d'échecs DMARC. **EN SAVOIR PLUS**

- Optimisez la protection contre l'usurpation d'identité conformément aux meilleures pratiques, à savoir 2 occurrences définies comme sujet/corps, et ajoutez une politique distincte pour les cadres/postes importants sur la base de la correspondance des noms avec une mise en attente pour examen par l'administrateur. Par ailleurs, créez une autre politique pour toutes les détections de 3 occurrences ou plus avec l'action de mise en attente par l'administrateur.
  EN SAVOIR PLUS

- La mise en place d'une réécriture agressive des URL garantira que toutes les URL sont analysées au clic, mais gardez à l'esprit que tout ce qui ressemble à une URL sera réécrit, par exemple les adresses IP et les liens internes. **EN SAVOIR PLUS**

- Envisagez de définir les politiques d'autorisation automatique sur « strict » au lieu de « autoriser » pour vous assurer que l'analyse des spams n'est pas contournée au niveau de l'organisation pour les destinataires d'e-mails externes.
  Ce paramètre doit être associé à l'option « Autorisation automatique de détection du spam », afin de s'assurer qu'aucun message potentiellement malveillant n'échappe à l'analyse.
  EN SAVOIR PLUS

- Utilisez les intégrations prédéfinies avec la majorité des fournisseurs de solutions SIEM et XDR pour assurer l'enregistrement et l'analyse des journaux à des fins d'application de la politique de sécurité. **EN SAVOIR PLUS**

- Exploitez vos propres renseignements sur les menaces pour tirer parti de tout flux de menaces de tiers et rejeter automatiquement les indicateurs correspondants.
  EN SAVOIR PLUS

- Il est recommandé de déployer des outils destinés aux utilisateurs finaux afin de signaler les messages potentiellement malveillants au SOC de Mimecast pour une analyse plus approfondie. **EN SAVOIR PLUS**

Si vous avez des doutes concernant l'un des paramètres proposés, veuillez contacter votre partenaire Mimecast ou directement le service d'assistance de Mimecast.

RESSOURCES

Voici une liste de ressources du gouvernement américain (webinaires, documents, avis) que les équipes de sécurité peuvent consulter pour mieux comprendre les menaces et les modes de défense

- **CISA/NSA** Les équipes rouge et bleue de la NSA et de la CISA partagent les dix principales erreurs de configuration en matière de cybersécurité
  5 October 2023
- **CISA** La CISA publie de nouvelles ressources identifiant les vulnérabilités exploitées connues et les mauvaises configurations liées aux ransomware
  12 October 2023
- **CISA** Directives en matière de phishing : arrêter le cycle d'attaque dès la première phase
  18 October 2023
- **CISA/NSA** La CISA, la NSA et leurs partenaires publient de nouvelles directives sur la sécurisation de la chaîne d'approvisionnement logicielle
  9 November 2023
- **CISA/NCSC** La CISA et le NCSC du Royaume-Uni dévoilent des directives conjointes pour le développement de systèmes d'IA sécurisés
  26 November 2023
- **CISA/NCSC /ACSC/FBI** L'acteur malveillant russe du FSB Star Blizzard poursuit ses campagnes de spear phishing dans le monde entier
  7 December 2023

CONCLUSION

Le quatrième trimestre 2023 a confirmé de nombreuses tendances des trimestres précédents. Les attaquants utilisent de plus en plus les marques pour tromper les utilisateurs et les amener à faire confiance aux spams et aux attaques de phishing. Pour cela, ils associent souvent la marque à un code QR ou à un lien vers un service de fichiers légitime. Les tensions géopolitiques se sont intensifiées à la suite de l'attaque du Hamas contre des civils israéliens et des représailles israéliennes qui ont suivi, entraînant une augmentation des attaques liées au conflit et une nouvelle série de sujets pour les leurres de phishing.

Les attaquants ont ciblé des secteurs légèrement différents au quatrième trimestre 2023, en se concentrant sur le secteur financier, comme les banques et d'autres services, les services professionnels, tels que les RH et la comptabilité, et le secteur des voyages, de l'hôtellerie et de la restauration. Bien que les campagnes visant les ressources humaines et les services de recrutement aient quelque peu diminué, ce secteur reste le troisième le plus ciblé.

WORK PROTECTED.™

Advanced Email & Collaboration Security

mimecast®