mimecast

Rapport Mimecast Global Threat Intelligence

1er Semestre 2024

Introduction

Pour affronter les cybermenaces de dernière génération, les entreprises de toutes tailles doivent mettre à jour leurs processus et leur infrastructure de cybersécurité en renforçant les défenses autour des communications, des individus et des données sensibles de l'entreprise, tout en enrichissant leurs connaissances sur les menaces. Mimecast génère en permanence une mine de renseignements sur les menaces en analysant quotidiennement plus de 1,7 milliard de messages pour le compte de plus de 42 000 clients de part le monde. La messagerie d'entreprise étant le canal privilégié par lequel s'infiltrent la plupart des cybermenaces, Mimecast permet de détecter, d'analyser et de neutraliser les menaces avant qu'elles ne se propagent au reste de l'entreprise.

Dans ce rapport Global Threat Intelligence, Mimecast fait la synthèse des informations recueillies par nos analystes du renseignement durant le premier semestre 2024, en croisant ses données avec des informations provenant de l'ensemble de la communauté open source de la cybersécurité. Ce rapport fait état des résultats d'analyses approfondies de l'activité des menaces, des statistiques révélant les tendances des attaques, ainsi qu'une série de recommandations destinées aux entreprises de toutes tailles afin de mieux atténuer les risques cyber.

Dans l'attente de bientôt vous fournir d'autres informations pertinentes, nous vous invitons à prendre connaissance de ce rapport sur les menaces observées au cours du premier semestre 2024.

Résumé pour les décideurs

L'activité cyber observée au cours du premier semestre de l'année 2024 illustre parfaitement l'aphorisme d'Alfonse Karr, « Plus ça change, plus c'est la même chose ».

L'adoption croissante de l'IA par les cybercriminels et les défenseurs, laisse présager des changements fondamentaux dans la manière d'appréhender la cybersécurité. Si jusqu'à présent, l'impact avait été relativement limité dans les deux camps, la bataille pour la domination du cyberespace fait désormais rage. En effet, les services cloud et les offres de service des cybercriminels continuent à accroître la disponibilité des outils de hacking clés en mains, des kits de phishing prêts à l'emploi et des bases de données d'informations volées. Les organismes gouvernementaux en charge de faire appliquer la loi ont montré des signes encourageants d'adaptation en améliorant la collaboration intergouvernementale, portant ainsi atteinte aux principaux groupes de cybercriminels.

Les messageries d'entreprise continuent d'évoluer alors que les pirates ont moins souvent recours à des pièces jointes malveillantes, préférant opter pour des liens malveillants vers des services légitimes de partage de fichiers dans le cloud, tels que SharePoint et Google Drive.

La recrudescence des attaques contre les entreprises de taille moyenne, observée en début d'année 2024, s'est quelque peu atténuée en fin de semestre, les PME étant à nouveau les plus ciblées. Notons que le vol d'identifiants est devenu une cible prioritaire des pirates, qui revendent ensuite les identifiants volés sur le Dark Web ou bien les réutilisent pour lancer des attaques par bourrage d'identifiants (credential stuffing) afin d'accéder aux services cloud des entreprises.

L'avenir nous réserve des défis relativement prévisibles.

À mesure que les entreprises migrent vers le cloud et développent leur infrastructure, la surface d'attaque globale augmente par voie de conséquence. La dépendance croissante des entreprises vis-à-vis des données stockées dans le cloud signifie que le contrôle de la sécurité leur échappe de plus en plus, tandis que la dépendance inhérente à l'égard des applications et des infrastructures tierces fait de la sécurité de la chaîne d'approvisionnement un défi majeur. Face à la poursuite des attaques par ransomware, le maintien de la confidentialité, de l'intégrité et de la disponibilité des données est essentiel au fonctionnement de l'entreprise. En effet, les attaques sur les données peuvent entraîner des interruptions de service avec des conséquences dévastatrices sur l'activité de l'entreprise. Nous pouvons anticiper qu'à l'avenir, l'IA générative et l'apprentissage automatique amélioreront le ciblage et le contenu des campagnes de phishing, ce qui obligera les entreprises à s'adapter aux nouvelles techniques d'attaques afin de les détecter et de les contrer dans les meilleurs délais.

1 Résultats clés

1

Afin de tromper les algorithmes de détection, les techniques d'attaque par email évoluent, allant de la simple diffusion de malware en pièce jointe à l'utilisation de liens malveillants, dissimulés dans des couches de liens aux allures légitimes. Cette évolution implique également une plus grande interaction de la part des victimes devant notamment cliquer sur d'autres liens, répondre à des CAPTCHA et à d'autres fausses demandes d'authentification multifactorielle.

2

Les secteurs de la banque, de la culture, du voyage et de l'hôtellerie ont été les plus touchés par des URL malveillants au second trimestre 2024, tandis que les secteurs du conseil informatique et des services juridiques ont reçu le plus grand nombre de spams et de tentatives d'usurpation d'identité.

3

Les pirates utilisent des services de développement, tels que Replit, pour héberger et développer des campagnes. Les services de partage de fichiers, notamment SharePoint et Google Drive sont également fréquemment utilisés pour héberger des documents intermédiaires renvoyant à des pages de collecte d'informations d'identification.

4

En Europe, ce sont les attaques par usurpation d'identité qui ont le plus fréquemment ciblé les utilisateurs, tandis que le spam a été à l'origine de la plupart des attaques en Afrique. Quant à la région Asie-Pacifique, elle a connu une recrudescence spectaculaire du nombre d'attaques ciblant les PME locales.

Le paysage des menaces en 2024

Cette année montre une recrudescence des spams, du phishing et des attaques de désinformation. En effet, une convergence d'événements mondiaux importants sont autant de sources d'inspiration pour les pirates afin de produire de nombreux sujets à partir desquels ils élaborent des leurres de phishing. En 2024, un certain nombre d'élections charnières auront lieu dans le monde avec notamment des votes importants aux États-Unis en Europe et également en France. Un nombre croissant de démocraties sont impliquées dans des conflits armés.[1] La poursuite de l'invasion russe de l'Ukraine ainsi que le conflit entre Israël et le Hamas, ont entraîné une augmentation significative des tentatives de désinformation. Les grands événements sportifs, des Jeux olympiques d'été à Paris aux récents tournois de football de l'Euro 2024 et de la COPA America, ont suscité des attaques de la part de nombreux groupes de cybercriminels.

Au cours du premier semestre 2024, six événements majeurs mettent en exergue les risques centrés sur l'humain dans le paysage actuel des menaces. Les informations émanant des rapports d'incidents font état d'un grand nombre de groupes malveillants allant des pirates opportunistes qui dérobent des informations sensibles pour compromettre les systèmes de messagerie dans le cloud, jusqu'aux groupes minoritaires dont le but est d'influencer l'issue des élections.

1. « 2024 is the biggest election year in history. » The Economist. The World Ahead. 23 novembre 2023.

Evénements majeurs

Trello divulgue les données de 15 millions de d'utilisateurs[2]

Vulnérabilité: API publique non sécurisée
Conséquence: Les adresses e-mail alimentent les futures attaques

Un initié d'i-SOON divulgue des informations sensibles sur le piratage[3]

Vulnérabilité: délit d'initié
Conséquence: Informations sensibles sur les opérations de piratage chinoises rendues publiques

Le ransomware Lockbit est neutralisé au terme d'une action coordonnée au niveau mondial[4]

Vulnérabilité: Action des forces de l'ordre
Conséquence: Démantèlement d'une organisation cybercriminelle majeure

JANVIER

En janvier dernier, des analystes du cyber renseignement ont découvert que plus de 15 millions de fiches d'utilisateurs de Trello avaient été mises en vente sur le dark web. Un hacker a utilisé des appels d'API pour collecter des informations à partir d'une API trop permissive qui permettait à quiconque d'interroger des comptes utilisateurs et de trouver des forums Trello associés à ces comptes. Le pirate a récolté des noms d'utilisateur, des adresses e-mail et des noms complets, autant de données susceptibles d'alimenter diverses attaques de messagerie. Atlassian, propriétaire de Trello, a depuis modifié l'API pour rendre plus difficile la collecte de telles informations.

FÉVRIER

Plus de 570 fichiers totalisant 170 Mo de données et décrivant les activités de l'entreprise chinoise de sécurité Shanghai Anxun Information Co, connue sous le nom de « i-SOON », ont été téléchargés sur la plateforme de dépôt de code Github. La fuite, qui semble avoir été commise par un employé mécontent de son sort, a révélé que l'entreprise avait mené une opération d'espionnage pour le compte du gouvernement chinois contre plus de 20 gouvernements de pays étrangers, dont les États-Unis, la Corée du Sud et d'autres territoires tels que Taïwan.

La National Crime Agency britannique, en étroite collaboration avec les enquêteurs d'une dizaine d'autres pays, a démantelé le gang à l'origine du ransomware LockBit en prenant le contrôle de l'infrastructure et des serveurs du groupe et en confisquant environ 11 000 domaines dans le cadre d'une action d'envergure internationale baptisée « Opération Cronos ». Le groupe LockBit serait à l'origine d'un quart des attaques par ransomware au cours de l'année écoulée et aurait perçu plus de 120 millions de dollars en paiement de rançons. L'opération conjointe des forces de l'ordre a donné lieu à des arrestations en Pologne, en Ukraine et aux États-Unis.

2. Seals, Tara. « Atlassian Tightens API After Hacker Scrapes 15M Trello Profiles. » Dark Reading. 24 janvier 2024. | 3. Benincasa, Eugenio. « From Vegas to Chengdu: Hacking Contests, Bug Bounties, and China's Offensive Cyber Ecosystem. » ETH Zurich. Whitepaper. 10 juin 2024. | 4. Burgess, Matt. « A Global Police Operation Just Took Down the Notorious LockBit Ransomware Gang. » Wired. 28 février 2024.

L'agence nationale de cyber défense américaine publie les détails du piratage de la messagerie Microsoft[5]

Vulnérabilité: Clé de signature volée
Conséquence: Divulgation d'e-mails sensibles de hauts responsables américains.

AVRIL

Dans un rapport publié en avril, la CISA (Cybersecurity and Infrastructure Security Agency) a dévoilé les détails d'une intrusion dans le service de messagerie Microsoft Exchange Online par le groupe de cyber espionnage Storm-0558, lié à la République populaire de Chine. À l'aide d'une clé volée créée en 2016, les cybercriminels ont pu accéder aux e-mails de plus de 500 personnes dans 22 organisations gouvernementales, y compris des fonctionnaires du Département d'État américain, du Département du commerce américain et de la Chambre des représentants des États-Unis. Ce rapport fait suite à une analyse faite par Microsoft en janvier 2024 concernant un autre piratage attribué à un groupe de pirates lié à la Russie en novembre 2023, où des e-mails des dirigeants de Microsoft avaient été compromis.[6]

Des identifiants non sécurisés à l'origine d'une fuite massive de données de l'hébergeur Snowflake[7]

Vulnérabilité: Absence d'authentification multi-facteur
Conséquence: Données clients divulguées à partir du stockage dans le cloud

MAI

Au moins 165 clients du fournisseur de données cloud Snowflake, parmi lesquels Ticketmaster et Santander Bank cités dans la presse, ont vu leurs données divulguées après que des identifiants volés aient été utilisés pour accéder à leurs comptes Snowflake. Les identifiants des comptes ont probablement été volés à la suite d'attaques de phishing, soit parce que l'authentification à deux facteurs n'était pas activée, soit parce que l'accès par nom d'utilisateur et mot de passe était autorisé en tant que solution de secours.

Des campagnes massives de désinformation influencent les élections dans l'UE[8]

Vulnérabilité: Campagnes de désinformation généralisées par e-mail et sur les réseaux sociaux
Conséquence: Impact potentiel sur les élections

JUIN

En mai et juin derniers, la campagne de désinformation ciblant les gouvernements de l'Union européenne s'est intensifiée, selon l'Observatoire européen des médias numériques (EDMO), un groupe se consacrant à la lutte contre la désinformation. Les responsables politiques et les défenseurs de la démocratie craignent qu'une telle recrudescence de désinformation, émanant de groupes étrangers, ne soit pas efficacement contrée aux États-Unis ; les mesures visant à fermer certains centres d'échange d'informations sur la désinformation ont eu un certain impact.[9]

5. CISA. « Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023. » Department of Homeland Security Advisory. 2 avril 2024. | 6. Microsoft Security Response Center. « Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard. » Microsoft. 19 janvier 2024. | 7. « UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion. » Google Mandiant Blog. 10 juin 2024. | 8. Tsu, Tiffany. « Convergence of Anger' Drives Disinformation Around E.U. Elections. » The New York Times. 7 juin 2024 | 9. Menn, Joseph. « Stanford's top disinformation research group collapses under pressure. » The Washington Post. 14 juin 2024.

Graphiques illustrant le paysage des menaces au 1er semestre 2024

Dans l'ensemble, les PME ont connu un pic d'attaques au cours du premier trimestre, tandis que les grandes entreprises ont vu diminuer le nombre de menaces par utilisateur (TPU). Si les spams et les attaques par usurpation d'identité ont été largement utilisés, les liens malveillants demeurent le moyen privilégié des pirates pour tenter d'infecter les systèmes des utilisateurs finaux.

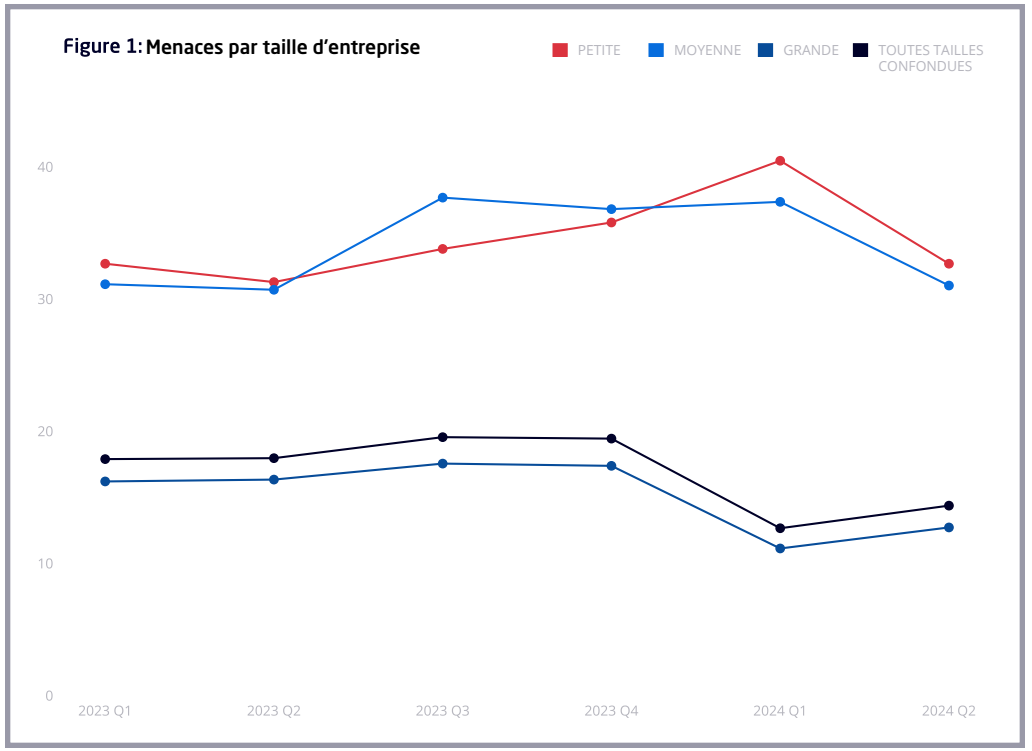
La banque, les voyages et l'hôtellerie, ainsi que la culture sont les trois secteurs les plus ciblés en ce début d'année, les pirates s'étant moins intéressés à leur cible de prédilection que sont les ressources humaines. Dans ce rapport, tous les graphiques utilisent des données mondiales. Pour visualiser les régions représentant l'Europe, le Royaume-Uni, les États-Unis, le Canada, l'Asie-Pacifique, l'Afrique subsaharienne et le Moyen-Orient, consultez le Centre de renseignements sur les menaces de Mimecast.

Graphique 1.

TPU par taille d'entreprise

Dans l'ensemble, le nombre de menaces ciblant les utilisateurs (TPU) a diminué d'environ un tiers, passant de 19 TPU en moyenne à la fin de l'année dernière (quatrième trimestre 2023) à 14 TPU au dernier trimestre (second trimestre 2024). Les menaces pesant sur les grandes entreprises ont également diminué au cours du premier trimestre, mais ont augmenté au second trimestre de cette année. En revanche, les TPU pour les moyennes entreprises sont restées stables au premier trimestre, puis ont fortement diminué au second trimestre pour atteindre 31 TPU.

Seules les PME ont observé une recrudescence significative des attaques, qui ont atteint 40 TPU au premier trimestre, en partie en raison d'un pic d'attaques au Canada, en Europe et aux États-Unis. Néanmoins, elles se sont atténuées au second trimestre. Les PME demeurent la cible favorite des pirates en raison de leurs plus faibles niveaux de sécurité.



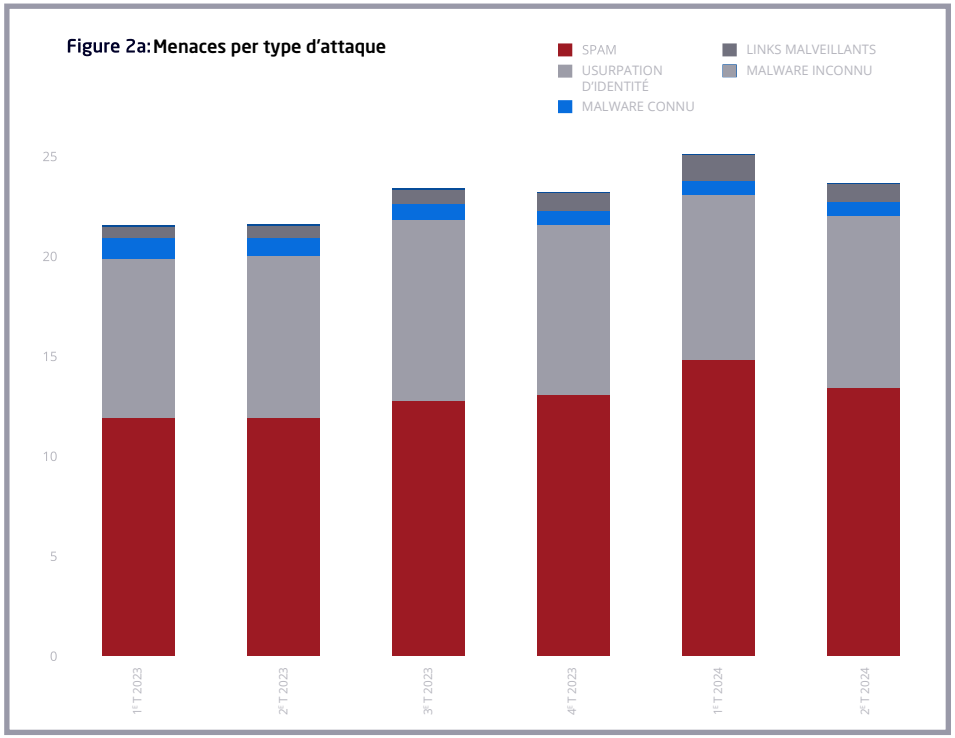
POUR AFFICHER LES MENACES PAR UTILISATEUR DANS VOTRE RÉGION, CLIQUEZ ICI

Graphique 2.

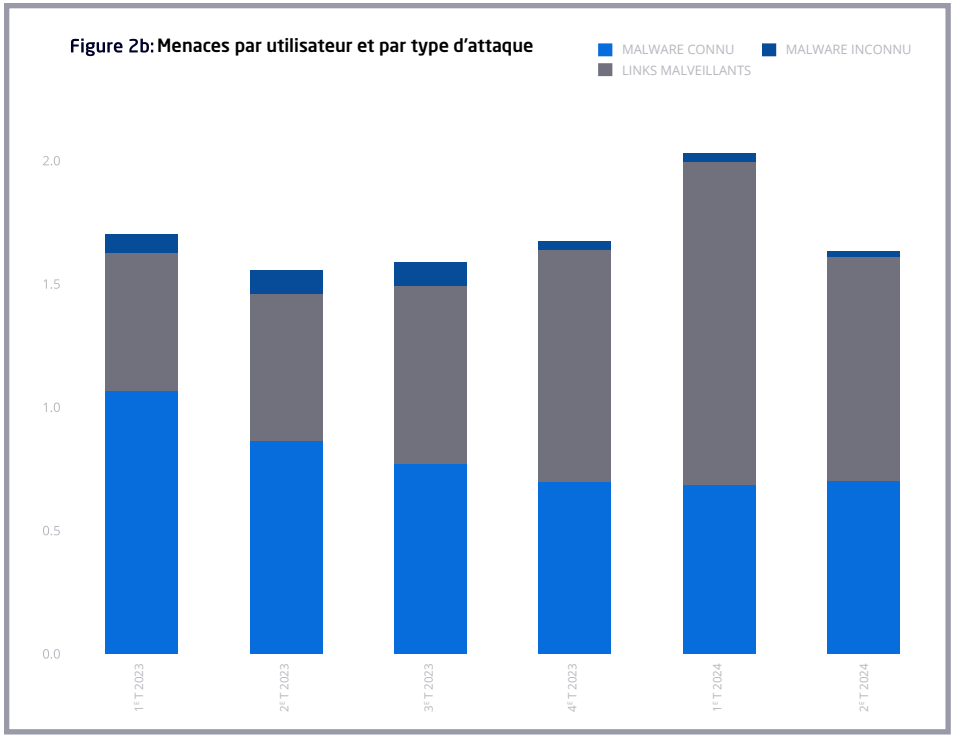
Impact du type d'attaque sur les TPU

Les attaques de spam et d'usurpation d'identité constituent l'essentiel des attaques interceptées par Mimecast, la plateforme ayant bloqué en moyenne 13 attaques de spam et 9 attaques d'usurpation d'identité par utilisateur. Le spam a connu un regain de popularité au premier trimestre 2024, bondissant de 13 % par rapport au trimestre précédent (T4 2023) et de 24 % par rapport au même trimestre en 2023. Alors que le spam a chuté au T2 2024, il reste néanmoins 12 % plus élevé que l'année précédente. Les attaques par usurpation d'identité sont restées assez stables d'un trimestre à l'autre, n'augmentant que légèrement au cours des deux premiers trimestres de 2024, 5 % et 6 %, respectivement, par rapport aux mêmes trimestres de l'année précédente.

Les attaques sans spam ni usurpation d'identité sont révélatrices de certaines tendances intéressantes (voir Figure 2b). Les pirates ont continué à peaufiner leur stratégie concernant les charges utiles des attaques de messagerie. Initialement dissimulées dans des pièces jointes aux e-mails, les charges utiles sont désormais indiquées par des liens malveillants. Ces derniers ont augmenté de 133 % au premier trimestre, soit plus du double, et de 53 % au second trimestre par rapport à l'année précédente. Le compte utilisateur Mimecast moyen a enregistré en moyenne un tiers de liens en moins au second trimestre par rapport au premier trimestre, mais cette baisse est probablement due à la forte hausse enregistrée au premier trimestre. Les malwares connus (bloqués par les défenses antivirus) et les malwares inconnus (identifiés et bloqués par les défenses liées aux pièces jointes) ont connu une baisse significative par rapport à l'année précédente, de 36 % et 54 % au premier et au second trimestre, respectivement.



POUR CONSULTER LES TYPES D'ATTAQUES DANS VOTRE RÉGION, CLIQUEZ ICI



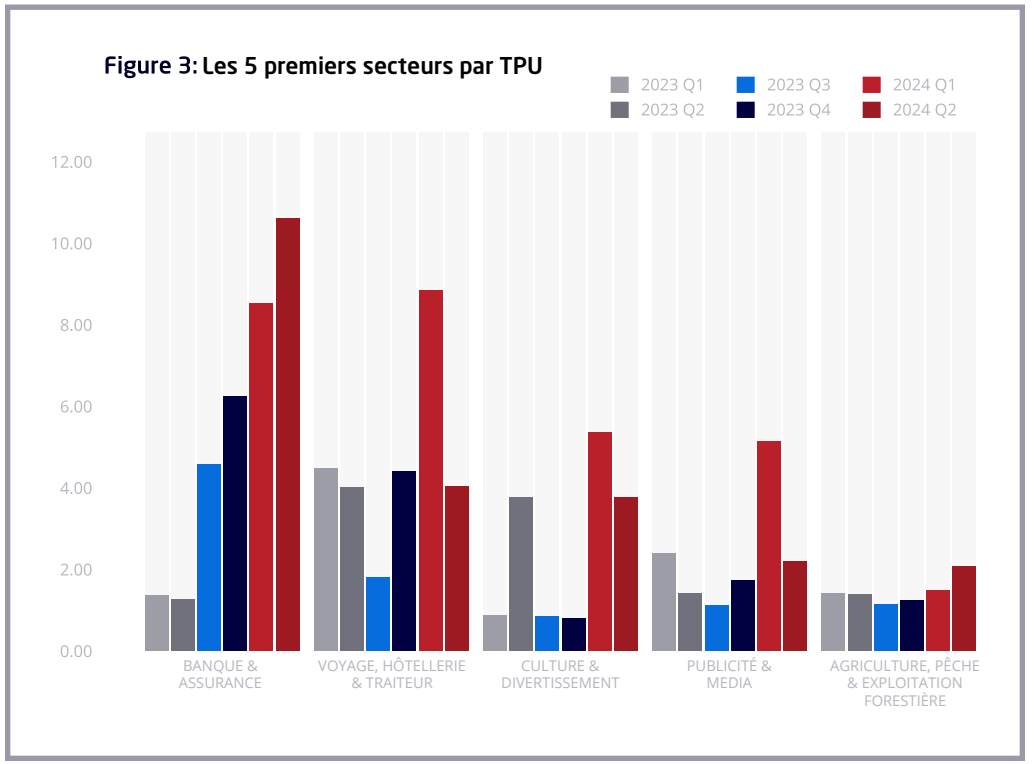
POUR CONSULTER LES TYPES D'ATTAQUES SANS SPAM NI USURPATION D'IDENTITÉ DANS VOTRE RÉGION, CLIQUEZ ICI

Graphique 3.

Principaux secteurs ciblés par TPU

Les trois secteurs les plus ciblés au cours du premier semestre 2024 sont la banque, les voyages et l'hôtellerie ainsi que les loisirs et la culture, avec respectivement 19, 13 et 9 attaques par utilisateur en moyenne, sans tenir compte des spams et des attaques par usurpation d'identité constituant l'essentiel des menaces. Dans l'ensemble, les URL malveillantes sont les plus répandues, représentant environ 10 fois plus d'attaques que les malwares connus et environ 100 fois plus d'attaques que les malwares inconnus.

Au cours du second trimestre 2024, les utilisateurs des secteurs du conseil en informatique et des services juridiques ont été la cible d'un nombre important d'e-mails d'usurpation d'identité, avec respectivement 208 et 56 messages par utilisateur bloqués par les services de Mimecast. Les utilisateurs des secteurs scientifique et technique, des services juridiques et du conseil informatique ont été les plus ciblés par les spams, les systèmes Mimecast bloquant en moyenne plus de 20 attaques par utilisateur.



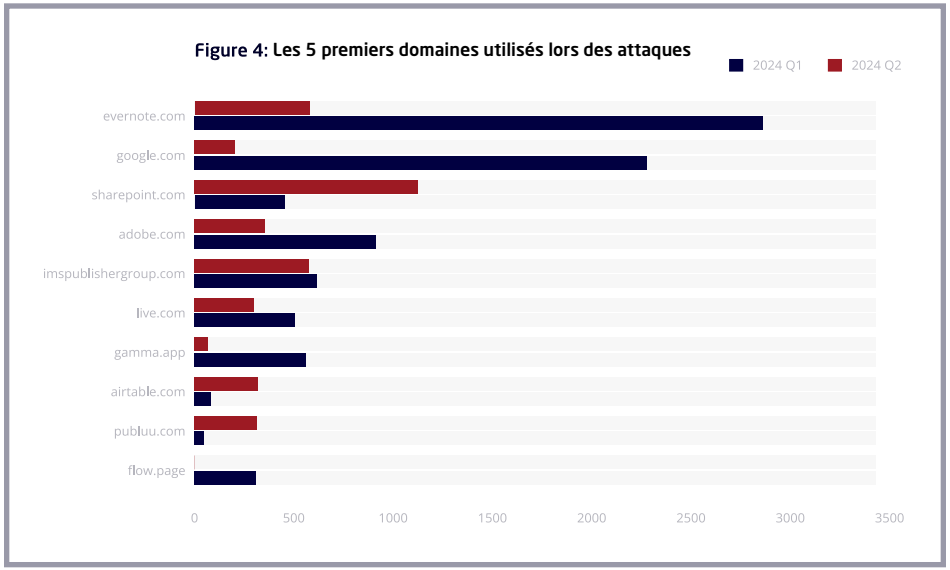
POUR VOIR LES SECTEURS CIBLÉS DANS VOTRE RÉGION, CLIQUEZ ICI

Graphique 4.

Tendances des abus liés au partage de fichiers

Les pirates ont continué à utiliser davantage de liens malveillants pour livrer des charges utiles à leurs victimes, le domaine evernote.com étant le domaine le plus utilisé au premier semestre 2024, comme au dernier trimestre 2023. L'utilisation du domaine google.com a fait un bond au premier trimestre de l'année, ce qui lui a permis de prendre la seconde place en devançant sharepoint.com.

Comme évoqué dans la section 2 (impact du type d'attaque sur les TPU), les cybercriminels privilégient davantage les liens pour diriger leurs victimes vers des pages de phishing, des sites de téléchargement furtifs et des formulaires factices de vols d'identifiants. La tendance observée est une utilisation accrue de sites de partage de données qui ne sont pas traditionnellement utilisés pour héberger des fichiers, afin de masquer leurs véritables intentions.

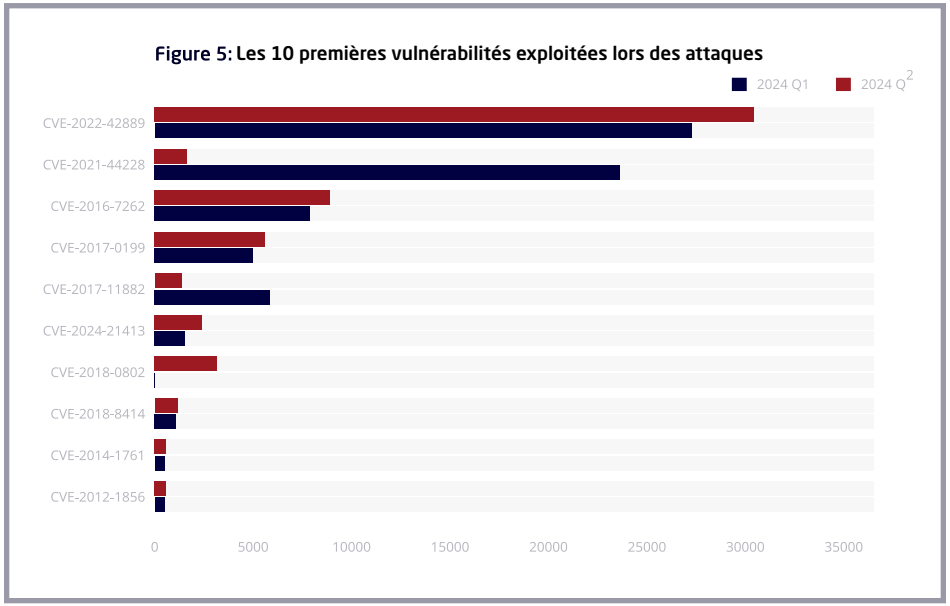


POUR CONSULTER LES TENDANCES EN MATIÈRE D'ABUS DE PARTAGE DE FICHIERS DANS VOTRE RÉGION, CLIQUEZ ICI

Graphique 5.

Les principales vulnérabilités au fil du temps

Au premier semestre 2024, la plupart des codes malveillants provenaient de cinq vulnérabilités exploitées, dont une vulnérabilité critique dans la bibliothèque Apache Commons Text (CVE-2022-42889) remportant la palme de la tentative d'exploitation la plus fréquente, avec un nombre de détections plus de deux fois supérieur à la suivante. La seconde vulnérabilité la plus populaire (CVE-2021-44228) est l'une des fameuses vulnérabilités Log4J2, utilisée par les pirates presque exclusivement au cours du premier trimestre.



POUR CONSULTER LES 10 PRINCIPALES VULNÉRABILITÉS DE VOTRE RÉGION, CLIQUEZ ICI

Principales campagnes ciblant les utilisateurs de Mimecast

3

CIBLE entreprises des secteurs chimiques et pharmaceutiques

CHARGE UTILE lien menant à un ransomware

01 montée en puissance de BlackMatter

Entre le 23 et le 25 avril 2024

Une campagne d'e-mailing visant principalement des scientifiques et des chercheurs universitaires de l'industrie chimique et pharmaceutique a ciblé près de 6 000 clients de Mimecast, alors que depuis décembre 2023, toutes les autres signatures de ransomwares détectées tournaient autour de 1 831 ou moins. Ce pic anormal de près d'un demi-million de détections est attribué au groupe de ransomware en tant que service (RaaS) BlackMatter.

Cédant à la pression judiciaire, le groupe de ransomware BlackMatter a cessé ses activités en 2021, mais son code source a ensuite été réutilisé par d'autres groupes, tels que LockBit 3.0 et Kasseika. Compte tenu des précédentes fuites de code source d'un ransomware et de sa réutilisation dans d'autres familles de ransomware10, les analystes de Mimecast estiment qu'il est fort à parier que certaines parties du code du ransomware BlackMatter soient actuellement utilisées activement par d'autres groupes cybercriminels et affiliés.

10. Lockbit 3.0 has BlackMatter ransomware code, wormable traits Tech target. Alexander Culafi. 30 Nov 2022

CIBLE Opportuniste CHARGE UTILE Un lien LinkedIn masqué menant à un contenu malveillant

02

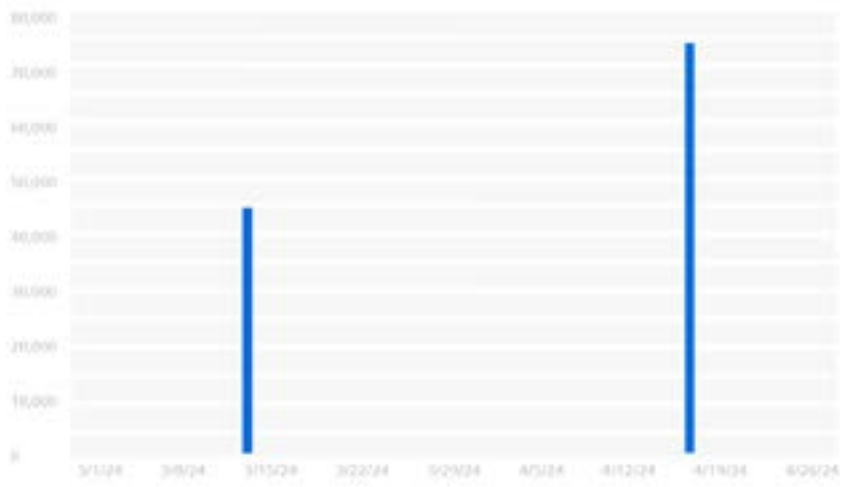
Abus de redirection sur LinkedIn

Entre mars et avril 2024

Deux grandes campagnes menées ont ciblé des destinataires avec des e-mails contenant un lien spécial vers un domaine LinkedIn qui, s'il était cliqué, redirigeait la victime vers un contenu statique, mais malveillant. Il ne s'agit pas d'une redirection ouverte traditionnelle, mais d'un lien construit par un pirate utilisant la capacité de LinkedIn à créer des liens vers du contenu statique.

Mimecast a détecté pas moins de 117 000 e-mails utilisant cette technique, les deux campagnes informant le destinataire qu'il aurait un message audio en attente. En cliquant sur le lien, une chaîne de redirections mène à une page de vérification CAPTCHA de Cloudflare et enfin, à une fausse page de connexion Microsoft Outlook. Les pirates ont également utilisé un compte Amazon Simple Email Service (SES), un service couramment utilisé de manière abusive, ce qui confère une légitimité apparente aux e-mails et augmente leurs probabilités d'outrepasser les contrôles de sécurité des courriels tels que SPF, DKIM ou DMARC.

hxxps://www.linkedin[.]com/redir/redirect?url=https%3A%2Flookerstudio%2Egoogle%2Ecom%2Fs%2FscrHqwjeA3k&urlhash=dcQj&trk=public_profile-settings_topcard-website



CLIQUEZ ICI POUR EN APPRENDRE DAVANTAGE SUR LES DÉTAILS DE LA CAMPAGNE.

CIBLE Industries alimentaire et du BTP CHARGE UTILE Lien de phishing intégré dans un e-mail menant à un site de partage de fichiers

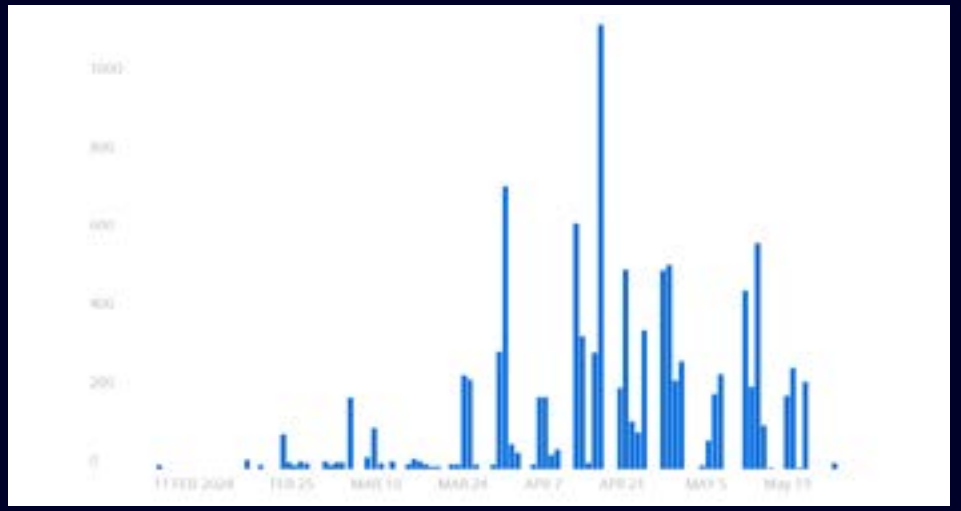
03

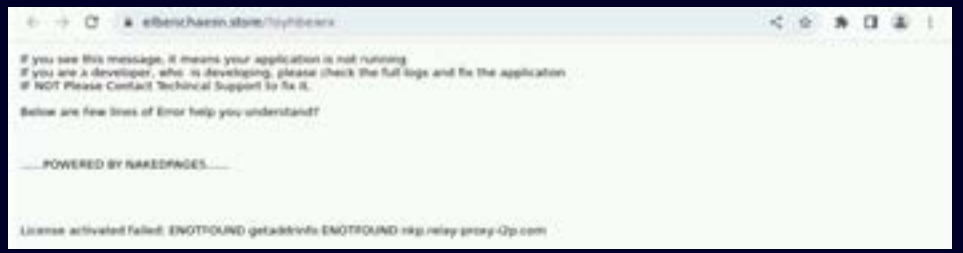
Les dossiers partagés SharePoint & Google Drive sont utilisés comme technique d'exfiltration

Entre février et mars 2024

Les pirates utilisent SharePoint et Google Drive pour héberger des documents malveillants qui semblent être des réponses à des appels d'offres pour des projets ou bien des factures pour des services. Les campagnes utilisent des comptes Office 365 piratés appartenant à des entreprises du même secteur, ce qui augmente la légitimité apparente des emails envoyés, afin de tromper leurs cibles.

En cliquant sur le document, les victimes sont redirigées vers une page de collecte d'informations d'identification Microsoft créée avec le kit de phishing Nakedpages. Les informations d'erreurs sur une page font référence à un proxy I2P, une couche réseau axée sur la confidentialité assurant des communications anonymes et pouvant indiquer que le kit est doté d'une fonction permettant d'exfiltrer des données ou de communiquer de manière anonyme.





CLIQUEZ ICI POUR EN APPRENDRE DAVANTAGE SUR LES DÉTAILS DE LA CAMPAGNE.

CIBLE Collaborateurs de l'entreprise **CHARGE UTILE** Un document PDF malveillant avec une extension de fichier HTML

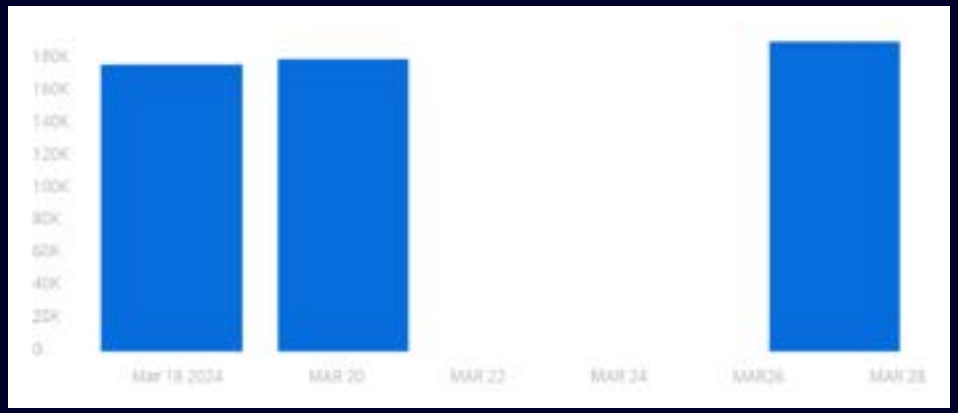
04

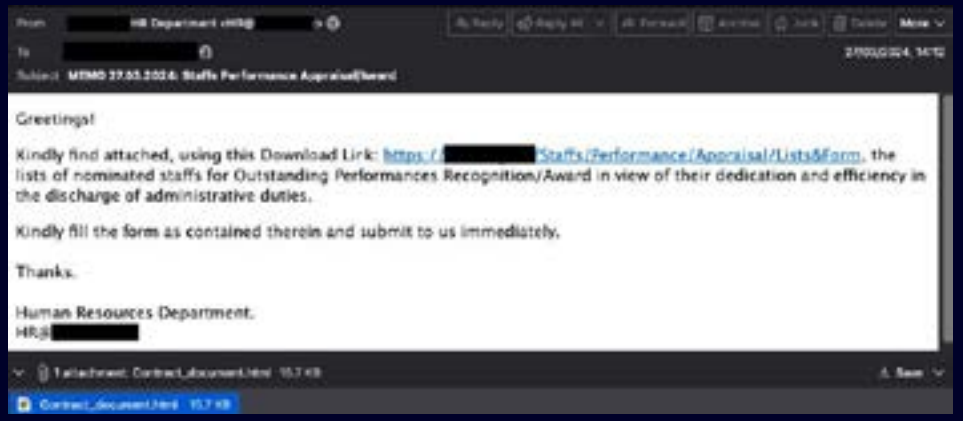
Utilisation des outils d'IA en ligne pour élaborer les campagnes d'e-mailing

Pendant trois jours de mars 2024

Les pirates ont envoyé 380 000 e-mails par le biais du service de marketing de publipostage Mailgun, avec un document PDF joint se terminant par une extension de fichier HTML. En cliquant sur le fichier, le PDF s'ouvre dans le navigateur web du destinataire et affiche deux liens vers une autre page hébergée sur Replit AI, un service d'assistance de programmation basé sur l'IA.

Se faisant passer pour le service de ressources humaines, les pirates ont alors envoyé aux collaborateurs de l'entreprise des informations pertinentes comme par exemple une mise à jour de la politique de congés annuels, la liste de formations obligatoires ou encore les évaluations des performances des employés, comme illustré ci-dessous. La dernière page de destination aux fausses allures de portail Microsoft Outlook était en fait destinée à voler les identifiants…





CLIQUEZ ICI POUR EN APPRENDRE DAVANTAGE SUR LES DÉTAILS DE LA CAMPAGNE.

CIBLE Les grands cabinets d'avocats australiens CHARGE UTILE Liens vers des étapes intermédiaires sur des plateformes, telles qu'Atlassian, Archbee et Nuclino

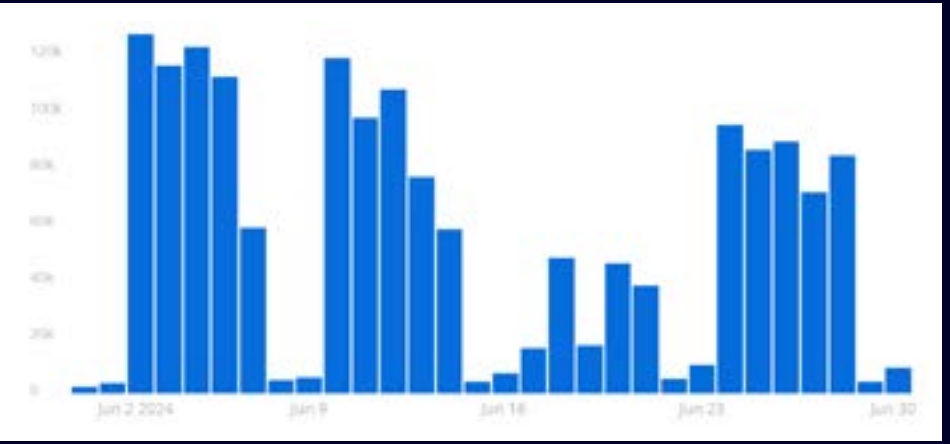
05

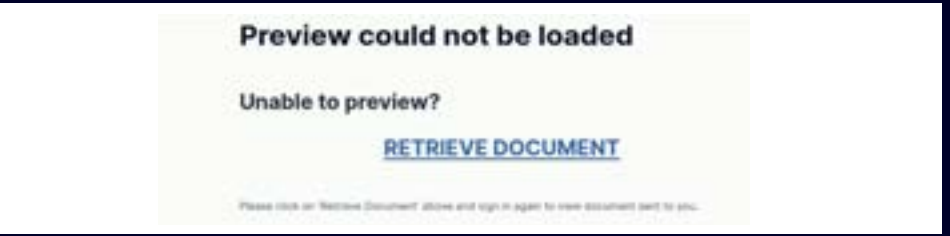
Exploitation des plateformes de création de documentation en ligne : Atlassian, Archbee et Nuclino

Entre mai et juin 2024

Une campagne prolifique a utilisé des URL masquées dans des e-mails pour rediriger les utilisateurs cliquant sur les liens vers une page intermédiaire sur l'une des nombreuses plateformes de collaboration, notamment Atlassian, Archbee et Nuclino. L'e-mail malveillant, qui semblait provenir d'une source interne, affirmait que l'appareil du destinataire n'était pas conforme et contient des informations détaillées sur son système d'exploitation.

Comme de nombreuses campagnes modernes, le fait de cliquer sur le lien dans l'e-mail, entraine une chaîne de redirection vers une page factice de connexion à Microsoft Outlook, un leurre fréquemment utilisé.





CLIQUEZ ICI POUR EN APPRENDRE DAVANTAGE SUR LES DÉTAILS DE LA CAMPAGNE.

CIBLE Consommateurs CHARGE UTILE Diverses fausses factures mentionnant un numéro de téléphone à un centre d'appels alimenté par l'IA

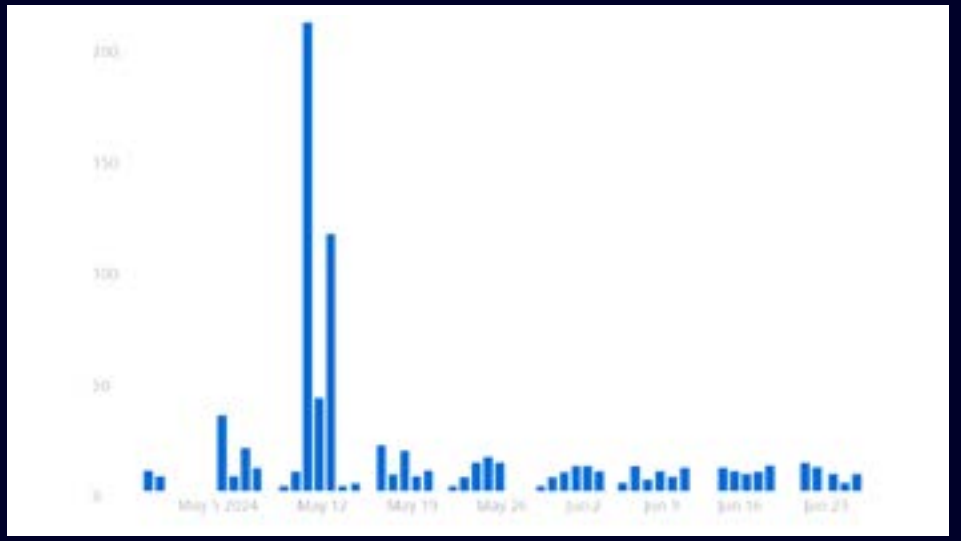
06

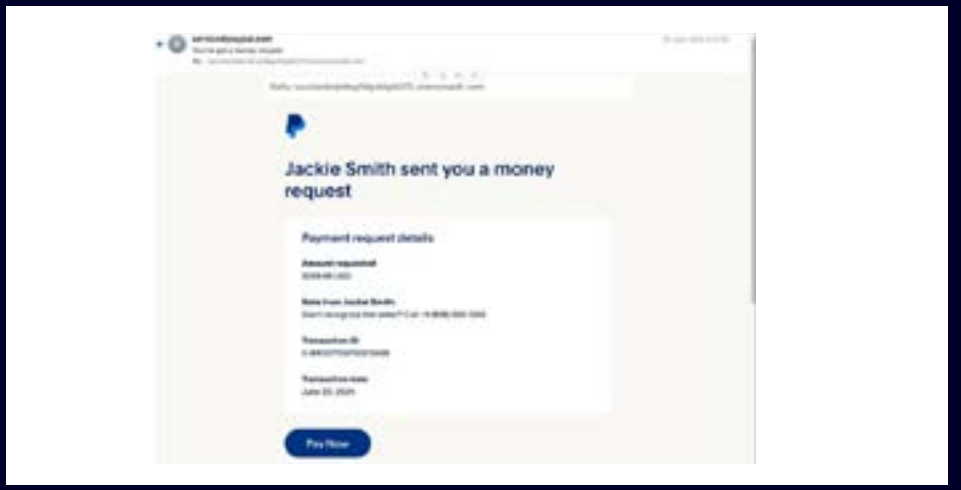
Escroqueries par e-mail soutenues par des centres d'appels automatisés par l'IA

En mai 2024

À l'aide des listes de distribution Microsoft permettant d'envoyer des e-mails en masse en passant plusieurs contrôles de sécurité, tels que SPF et DMARC, les pirates créent des messages qui semblent informer les destinataires d'un avoir ou d'une facture imminente. L'appel du numéro de téléphone connecte l'utilisateur à un centre d'appels, de plus en plus fréquemment automatisé par un grand modèle de langage (LLM) et qui recueille les informations convoitées par le fraudeur.

En mai 2024, Mimecast a détecté plus de 1,6 million d'e-mails dans ce type de campagne ciblant directement les consommateurs.





CLIQUEZ ICI POUR EN APPRENDRE DAVANTAGE SUR LES DÉTAILS DE LA CAMPAGNE.

Recommandations

Contre-mesures spécifiques

1

Bloquer les images dans les e-mails

Les pirates utilisent de plus en plus de fichiers sous forme d'images pour injecter des leurres de phishing et du code malveillant dans les emails, tout en échappant à la détection. L'analyse de Mimecast a permis d'identifier des acteurs malveillants utilisant également le chiffrement et le texte en langue étrangère dans des images afin de brouiller les pistes. Les entreprises doivent configurer les clients de messagerie pour empêcher le chargement automatique d'images dans les messages et isoler toutes les images signalées explicitement par les utilisateurs.

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

2

Segmenter le réseau et enregistrer le trafic interne

Les pirates, en particulier lors d'une attaque de ransomware, peuvent rapidement se déplacer latéralement au sein d'un réseau. La segmentation du réseau interne et l'installation d'actifs critiques dans leurs propres enclaves peuvent réduire les dommages causés par les ransomwares et autres attaques similaires. La surveillance du trafic interne, en particulier des communications vers des segments de réseaux spécifiques, peut permettre une détection plus précoce des menaces.

3

Renforcer les identifiants des utilisateurs, déployer l'authentification multi-facteur

De nombreux malwares exploitent les mots de passe courants pour s'infiltrer dans les réseaux ciblés. Les récentes attaques montrent à quel point les mots de passe faibles contribuent aux violations de données. Renforcez n'importe quel réseau en appliquant des mots de passe robustes, en particulier pour les utilisateurs disposant d'accès privilégiés. La sécurité informatique doit éliminer les mots de passe administrateur par défaut. Exiger une authentification multi-facteur peut réduire considérablement la compromission des comptes ou le vol d'identifiants.

4

Dispenser des formations de sensibilisation aux cyber-risques

L'humain se trouvant au cœur des systèmes de l'entreprise, les utilisateurs introduisent des erreurs humaines dans les opérations quotidiennes. Si le personnel est sensibilisé aux cyber-risques et à la manière de les identifier, il constitue la première ligne de défense contre de nombreuses attaques, en particulier celles qui utilisent la messagerie.

5

Renforcer la sécurité des fournisseurs et des sous-traitants.

Les attaques contre des entreprises des secteurs manufacturier, du transport, de la logistique ainsi que de la vente au détail et en gros, représentent un risque important de compromission de la chaîne d'approvisionnement pour les sous-traitants. Les entreprises doivent revoir leurs accords de niveau de service pour fixer des niveaux minimaux de sécurité des données et de cybersécurité et trouver des moyens de surveiller leurs fournisseurs de plus près, par exemple en utilisant des services de notation externes et en soumettant les acquisitions à un examen plus approfondi.

6

Analyser la périphérie du réseau d'entreprise pour détecter les failles de configuration ou les ports externes ouverts.

Les entreprises doivent scanner régulièrement leur infrastructure à la recherche d'itinéraires exploitables connus tels que des ports réseau externes ouverts non sécurisés ou des environnements de cloud public. Grâce à des outils tels que Cloud Security Posture Management, les entreprises peuvent identifier rapidement les erreurs de configuration dans leur cloud public. Cela permettra de s'assurer que tous les ports du serveur accessibles au public sont fermés ou correctement sécurisés et protégés.

Par exemple, Mimecast a constaté une augmentation constante des attaques contre les ports du protocole RDP (Remote Desktop Protocol), représentant 80 % des compromissions effectives par ransomware. Il est fort probable qu'à l'avenir, les pirates continueront à chercher et à exploiter les ports RDP ouverts pour cibler les entreprises de toutes tailles.

Bonnes pratiques et conseils

31 JANVIER 2024 **US Cyber Command, CISA, FBI, ONCD**	**« Hearing on CCP Cyber Threat »** REFERENCE	Les plus hauts responsables de la cybersécurité nationale américaine sont préoccupés par la recrudescence de l'activité des acteurs malveillants chinois dans la région Asie-Pacifique, en particulier par le pré-positionnement de compromis concernant des infrastructures critiques de la région. Volt Typhoon, un groupe malveillant lié à la Chine, a mené des attaques dans la région dès 2021.
14 FÉVRIER 2024 **Microsoft et Open AI**	**Staying Ahead of Threat Actors in the Age of AI** REFERENCE	Les groupes d'acteurs malveillants, qu'ils soient indépendants ou liés à des états, expérimentent les LLM à différentes étapes de la chaîne d'attaque, notamment la traduction de texte, l'optimisation des messages et l'automatisation de la reconnaissance. Les groupes APT connus pour avoir testé ChatGPT d'Open AI dans le cadre de ces opérations comprennent Forest Blizzard, lié à la Russie, Emerald Sleet, lié à la Corée du Nord, Crimson Sandstorm, lié à l'Iran, ainsi que Charcoal Typhoon et Salmon Typhoon, liés à la Chine.
29 MARS 2024 **Agence nationale américaine de cybersécurité (CISA)**	**Reported Supply Chain Compromise Affecting XZ Utils Data Compression Library, CVE-2024-3094** REFERENCE	Un pirate a réussi à convaincre un développeur d'accepter les mises à jour du projet open source, XZ Utils, qui était en réalité une porte dérobée vers tout système exécutant le logiciel. Après avoir passé des années à gagner la confiance du responsable du projet, la porte dérobée n'était qu'à quelques semaines de sa fusion avec une distribution Linux majeure lorsqu'un développeur de Microsoft a découvert le code et en a immédiatement informé la communauté.

2 AVRIL 2024 **Agence nationale américaine de cybersécurité (CISA)**	**Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023** REFERENCE	Troisième incident examiné par le Cyber Safety Review Board (CSRB), le rapport analyse l'intrusion de mai 2023 dans Microsoft Exchange Online par Storm-0558, un groupe de pirates informatiques lié à la République populaire de Chine et considéré comme l'auteur de l'opération Aurora en 2009 et de la compromission de RSA SecureID en 2011. L'attaque a ciblé les comptes d'e-mail du Département d'État américain, du Département du commerce américain, de la Chambre des représentants américaine et de 22 autres organisations gouvernementales américaines. Le CSRB a formulé des recommandations à l'intention de Microsoft en particulier, des fournisseurs de services cloud en général et de leurs clients.
2 MAI 2024 **FBI, State, NSA**	**North Korean Actors Exploit Weak DMARC Security Policies to Mask Spearphishing Efforts** REFERENCE	Selon une pratique courante chez les acteurs étatiques, les cyberacteurs nord-coréens mènent des campagnes de spearphishing ciblant des journalistes, des universitaires et des responsables politiques spécialisés dans les affaires de l'Asie orientale. Afin d'échapper à toute détection, les activités liées à l'acteur de Kimsuky ou d'Emerald Sleet, ciblent les organisations dont les politiques d'authentification, de reporting et de conformité des messages basées sur le domaine (DMARC) sont vulnérables.
26 JUIN 2024 **CISA, FBI, ACSC**	**Exploring Memory Safety in Critical Open Source Projects** REFERENCE	Ces groupes gouvernementaux ont exhorté les projets logiciels open-source et leurs utilisateurs à adopter des langages de programmation sans risque pour la mémoire. Plus de la moitié des lignes de code (55 %) sont écrites dans des langages qui comportent des risques pour la mémoire. Même les projets écrits dans des langages sans risque pour la mémoire reposent sur des composants à risque.

La check list de Mimecast

Cette section met en évidence des étapes spécifiques et réalisables pour les entreprises afin de protéger leurs collaborateurs contre les menaces mentionnées dans ce rapport, avec des détails techniques de niveau intermédiaire.

Single Sign-On.

Il est fortement recommandé **d'utiliser l'authentification unique** de votre fournisseur d'identité ou l'authentification multi-facteur intégrée de Mimecast pour réduire la capacité des pirates à utiliser l'e-mail comme vecteur d'attaque.

Authentification DNS.

Assurez-vous que les **politiques d'authentification DNS** respectent les enregistrements DMARC. Une seconde stratégie étendue à un groupe de stratégies avec l'action « DMARC Fail » réglée sur « Ignore/Manage » et « Permetted Senders » permet de contourner efficacement tout e-mail légitime rejeté/mis en quarantaine en raison d'échecs DMARC.

Usurpation d'identité.

Optimisez la protection contre l'usurpation d'identité conformément aux lignes directrices des meilleures pratiques, à savoir deux occurrences définies pour marquer le sujet/corps de l'email et instaurez une politique distincte pour les dirigeants basée sur la correspondance des noms, avec une mise en attente pour examen par l'administrateur. En outre, créez une autre politique pour toutes les détections de trois occurrences ou plus avec l'action de mise en attente de l'administrateur.

Réécriture des URL.

La mise en place d'une politique de **réécriture systématique 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.

Autorisations automatiques.

Envisagez de régler **les politiques d'autorisation automatique** sur « Strict » au lieu de « Allow » pour vous assurer que l'analyse des spams n'est pas contournée pour les destinataires d'e-mails externes. Ceci doit être défini conjointement avec la fonction « **Auto Allow Spam Detection** » pour être conservé pour examen ultérieur afin de garantir qu'aucun message potentiellement malveillant ne contourne l'analyse.

Fournisseurs de solutions SIEM et XDR.

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 de conformité à la politique de sécurité de l'entreprise.

Flux de menaces de solutions tierces.

Exploitez vos propres renseignements sur les menaces pour tirer parti de tout flux de menaces de tiers et rejeter automatiquement les indicateurs concordants.

Remontée d'informations des utilisateurs.

Il est recommandé aux utilisateurs finaux de signaler les messages potentiellement malveillants reçus **par le biais des outils utilisateur de Mimecast** au SOC de Mimecast en vue d'une analyse approfondie.

Si vous avez des interrogations sur l'une de ces recommandations, veuillez contacter votre partenaire Mimecast ou le service d'assistance de Mimecast

5

Conclusion

L'évolution du paysage des menaces continue de poser un défi de taille aux équipes de cybersécurité, alors que la numérisation des activités commerciales basée dans le cloud s'est largement intensifiée. Cette situation entraine une recrudescence des attaques par ransomware, des compromissions complexes de la chaîne d'approvisionnement numérique, des vulnérabilités intégrées ainsi qu'une augmentation des attaques contre les systèmes d'identification.

Dans l'ensemble, la plupart des tendances évoquées l'année dernière se sont vérifiées au premier semestre 2024. Les liens malveillants continuent d'être le moyen privilégié par les cybercriminels pour acheminer des charges utiles vers les systèmes de leurs victimes. Les utilisateurs des PME continuent d'être confrontés à deux fois plus de menaces que ceux des grandes entreprises et les services légitimes de partage de fichiers continuent d'être utilisés de manière abusive par les acteurs malveillants.

Dans le même temps, les groupes de cybercriminels continuent d'intensifier leurs activités. L'impact du durcissement de la loi contre des groupes de premier plan tels que LockBit a probablement entraîné une baisse à court terme des activités malveillantes, qui devraient revenir à des niveaux normaux en fin d'année.

À court terme, l'avenir nous réserve des défis assez prévisibles. Au fur et à mesure que les entreprises migrent vers le cloud et développent leur infrastructure, la surface d'attaque globale ne peut qu'augmenter. Afin de relever ce défi, les entreprises devront veiller à ce que leurs infrastructures soient configurées de manière sécurisée et qu'une politique de surveillance étroite et systématique des flux réseaux soit mise en place.

Une dépendance croissante à l'égard des ensembles de données, stockés dans le cloud, signifie que la sécurité échappe souvent au contrôle de l'entreprise, tandis que la dépendance inhérente à des logiciels et à des infrastructures tierces fait de la sécurité de la chaîne d'approvisionnement un défi majeur.

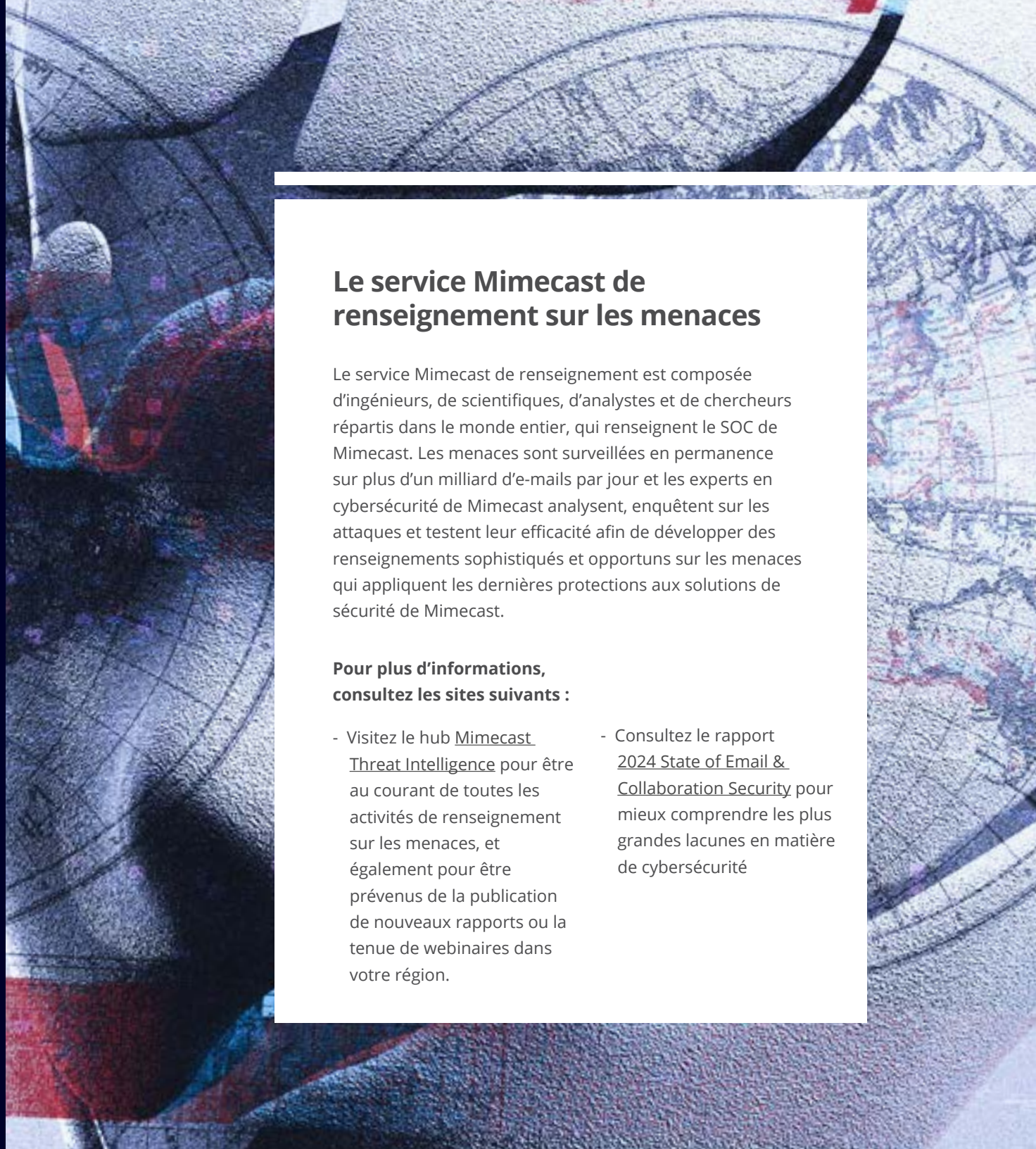
Face aux attaques incessantes de ransomware, la disponibilité des données est un élément crucial car l'interruption de l'activité ou le déni de service sont extrêmement coûteux tant pour la réputation de l'entreprise que pour la prestation de services. Les sauvegardes sont de plus en plus fréquemment ciblées et nécessitent une attention particulière pour garantir la protection des données sensibles de l'entreprise dans un environnement sécurisé.

Le facteur humain a toujours joué un rôle critique dans l'identification des risques auxquels est confrontée une entreprise alors que celle-ci fournit des accès plus directs à des informations pertinentes ou à un réseau. Le ciblage des employés reste un vecteur d'attaque très efficace et il est peu probable que cela change à court terme car cette tactique s'adapte facilement aux changements organisationnels de l'entreprise.

A l'avenir, l'utilisation abusive de l'IA générative et de l'apprentissage automatique améliorera le ciblage et le contenu des campagnes de phishing, ce qui obligera les entreprises à disposer d'indicateurs techniques pour être en mesure de détecter et de répondre à des attaques innovantes et inédites.

mimecast

Conçue pour protéger les entreprises contre l'ensemble des cybermenaces actuelles, Mimecast est une plateforme connectée de gestion des risques humains, alimentée par l'IA et dotée d'API. Intégrant une technologie de pointe à des parcours centrés sur l'humain, notre plateforme améliore la visibilité et fournit des informations stratégiques permettant de prendre des mesures décisives et de donner aux entreprises les moyens de protéger leurs environnements collaboratifs, de sauvegarder leurs données sensibles et d'impliquer activement leurs collaborateurs dans la réduction des risques cyber et l'amélioration de la productivité. Plus de 42 000 entreprises dans le monde font confiance à Mimecast pour les aider à garder une longueur d'avance sur le paysage des cybermenaces en constante évolution. En matière de prévention des risques internes ou de menaces externes, nos clients obtiennent toujours davantage : davantage de visibilité, davantage d'informations, davantage de souplesse, davantage de sécurité.



Le service Mimecast de renseignement sur les menaces

Le service Mimecast de renseignement est composée d'ingénieurs, de scientifiques, d'analystes et de chercheurs répartis dans le monde entier, qui renseignent le SOC de Mimecast. Les menaces sont surveillées en permanence sur plus d'un milliard d'e-mails par jour et les experts en cybersécurité de Mimecast analysent, enquêtent sur les attaques et testent leur efficacité afin de développer des renseignements sophistiqués et opportuns sur les menaces qui appliquent les dernières protections aux solutions de sécurité de Mimecast.

Pour plus d'informations, consultez les sites suivants :

- Visitez le hub Mimecast Threat Intelligence pour être au courant de toutes les activités de renseignement sur les menaces, et également pour être prévenus de la publication de nouveaux rapports ou la tenue de webinaires dans votre région.
- Consultez le rapport 2024 State of Email & Collaboration Security pour mieux comprendre les plus grandes lacunes en matière de cybersécurité