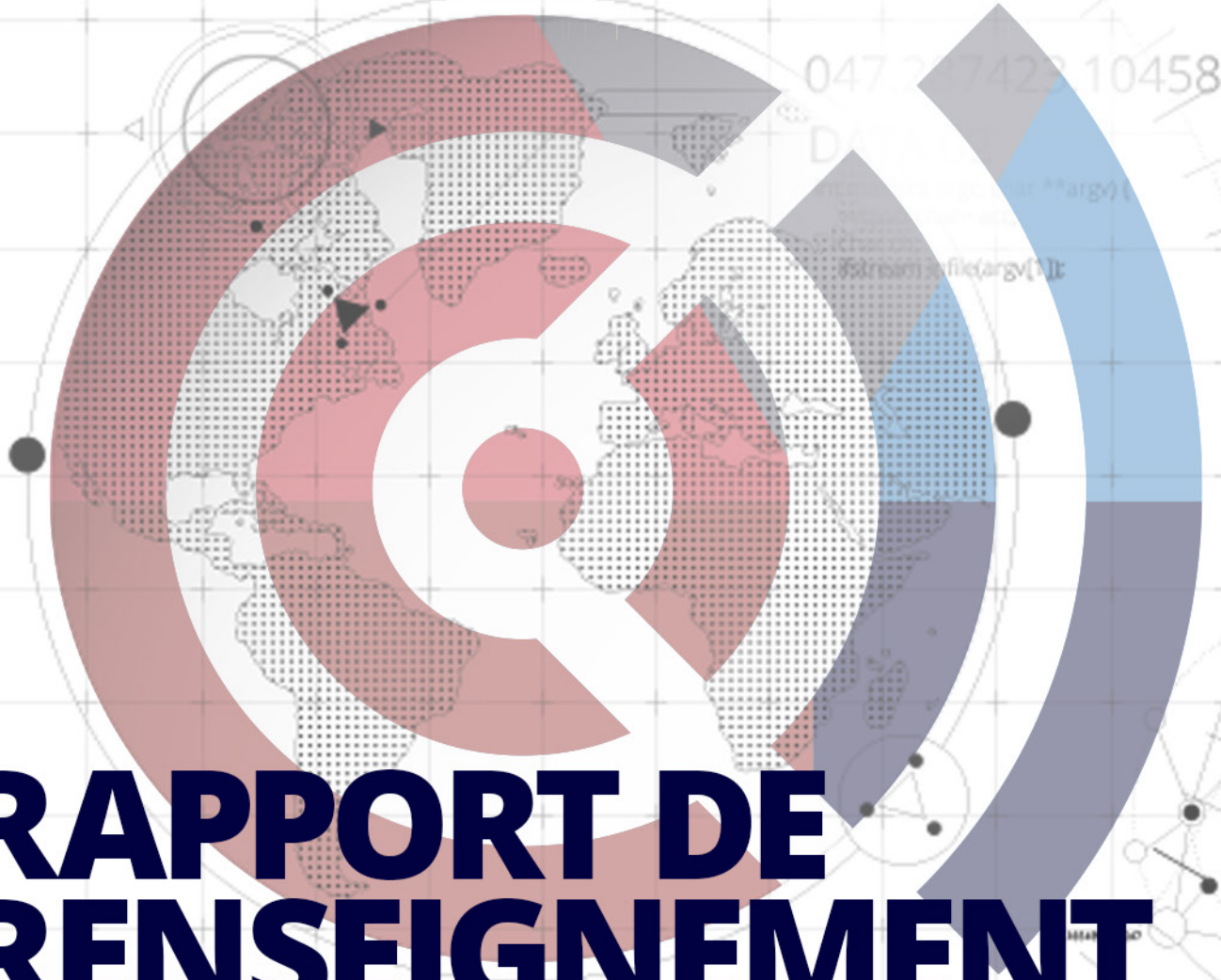
mimecast

RISK RADAR

DETECTION | ANALYSIS | ACTION



RAPPORT DE RENSEIGNEMENT SUR LES CYBERMENACES MONDIALES

JUILLET À DÉCEMBRE 2024

SOMMAIRE :

INTRODUCTION

Afin faire face à l'ingéniosité grandissante des cybercriminels, il est indispensable que les entreprises et les organisations disposent de renseignements de qualité sur les cybermenaces actuelles. Les entreprises de toutes tailles doivent rester au fait des dernières tendances, suivre l'évolution des menaces ciblant leur secteur d'activité et leurs fournisseurs, renforcer leurs défenses et adapter leurs processus pour éviter que leurs communications et leurs collaborateurs ne soient utilisés à mauvais escient.

Au cours du second semestre 2024, Mimecast a traité plus de 90 milliards de données pour une grande partie de ses 43 000 clients et a intercepté plus de 5 milliards de menaces, le nombre total d'interactions protégées étant largement supérieur à ce chiffre. Les messageries et les outils de collaboration continuent d'être les canaux privilégiés des pirates informatiques pour tenter de compromettre les entreprises ciblées, permettant ainsi à Mimecast de détecter et d'analyser bon nombre de ces menaces avant qu'elles ne soient largement diffusées.

Au cours du second semestre 2024, Mimecast a traité plus de 90 milliards de données pour une grande partie de ses 43 000 clients et a intercepté plus de 5 milliards de menaces

Pour préparer le rapport Global Threat Intelligence du second semestre 2024, Mimecast a recueilli les données en provenance de ses systèmes protégeant des dizaines de millions d'utilisateurs parmi ses clients. Elle a également mis en avant les conclusions de ses analystes et a pris en compte des informations open source sur les dernières menaces. Le rapport associe l'analyse de l'activité cybercriminelle, les statistiques des dernières tendances en matière de cyberattaque et les recommandations permettant aux entreprises de protéger leurs salariés et d'atténuer l'impact des utilisateurs à risque.

Nous vous invitons à découvrir notre rapport de renseignements sur les menaces du second semestre 2024, dans l'attente de partager d'autres informations.

SYNTHÈSE POUR LES DIRIGEANTS

02

AU COURS DU SECOND SEMESTRE 2024, LES CYBERCRIMINELS ONT EU DAVANTAGE RECOURS AUX SERVICES LÉGITIMES POUR DISSIMULER LEURS ATTAQUES ET TENTER DE CONTOURNER LES DÉFENSES.

Au vu de cette tendance à exploiter les services de confiance, les systèmes de réputation et d'authentification ne suffisent plus aux entreprises pour se protéger des attaques par messagerie et plus généralement centrées sur le risque humain. En outre, les pirates exploitent volontiers les accès attribués aux prestataires externes (logiciels ou services) pour s'infiltrer plus facilement dans les réseaux ciblés.

LE CONTEXTE GÉOPOLITIQUE FOURNIT AUX CYBERCRIMINELS UNE OPPORTUNITÉ DE LANCER PLUS FRÉQUEMMENT DES TENTATIVES DE COMPROMISSION AINSI QU'UNE SOURCE D'INSPIRATION POUR ÉLABORER DE NOUVELLES ATTAQUES.

De leur côté, les Etats-nations ont continué à recourir aux cyberattaques et au cyber espionnage pour mener des actions inavouables à l'encontre de leurs rivaux. Ainsi, la Chine a compromis les infrastructures américaines et canadiennes,[1] l'Iran et Israël ont chacun ciblé leurs infrastructures réciproques[2] et la Russie a continué à cibler les organisations gouvernementales européennes et américaines[3] une fois l'invasion de l'Ukraine freinée.

1. Catharine Tunney, « China "compromised" Canadian government networks and stole valuable info : spy agency », CBC, 30 octobre 2024. https://www.cbc.ca/news/politics/cse-cyber-threats-china-1.7367719
2. Robert Lemos, « As Geopolitical Tensions Mount, Iran's Cyber Operations Grow », Dark Reading. Article de presse, 18 septembre 2024. https://www.darkreading.com/cyberattacks-data-breaches/geopolitical-tensions-mount-iran-cyber-operations-grow
3. Nathan Eddy, « Ukraine-Russia Cyber Battles Tip Over Into the Real World », Dark Reading, article de presse, 3 octobre 2024. https://www.darkreading.com/cyberattacks-data-breaches/ukraine-russia-cyber-battles-tip-over-into-real-world

LES TECHNOLOGIES DE L'IA CONTINUENT D'OFFRIR DES AVANTAGES INDÉNIABLES AUX DÉFENSEURS ET AUX ATTAQUANTS.

L'IA permet aux spécialistes en cybersécurité d'analyser plus rapidement les événements de sécurité, tandis que les équipes de réponse aux incidents l'utilisent pour neutraliser les attaques et réduire leur impact plus vite et de manière plus efficace. Mais, les cyberattaquants bénéficient également de l'IA : selon une étude menée par Mimecast[4] en s'appuyant sur l'analyse linguistique, environ 12 % des e-mails, y compris dans le cadre des attaques de phishing, semblent avoir été rédigés par de grands modèles linguistiques (LLM). Des deepfakes audios et vidéos ont permis de se faire passer pour des PDG amenant leurs salariés à effectuer des virements sur des comptes bancaires reliés aux cybercriminels.

TOUTES CES TENDANCES ONT VOCATION À SE POURSUIVRE EN 2025.

Le nombre d'attaques s'appuyant sur le cloud a plus que doublé en 2024 et ce, dans un contexte géopolitique toujours plus chaotique : en Europe, les citoyens français et allemands ont été appelés aux urnes, tandis que le président américain Donald Trump vient d'entamer son deuxième mandat non consécutif et que la Russie et la Chine continuent d'affirmer leur puissance militaire sur la scène internationale. Les chercheurs en sécurité et les pirates mettent au point de nouvelles méthodes pour exploiter les systèmes de l'IA, soit en exploitant les failles de sécurité, soit en améliorant leur stratégie d'attaque.

4. Evonne Lee, « New Mimecast Threat Intelligence: How ChatGPT Upended Email », Blog Mimecast - Renseignement des menaces, 30 septembre 2024, https://www.mimecast.com/blog/how-chatgpt-upended-email/.

RÉSULTATS CLÉS

Si l'activité malveillante est globalement en hausse, certaines tendances se dégagent :

K-1 ONE

LES CYBERCRIMINELS UTILISENT DE PLUS EN PLUS DE SERVICES LÉGITIMES.

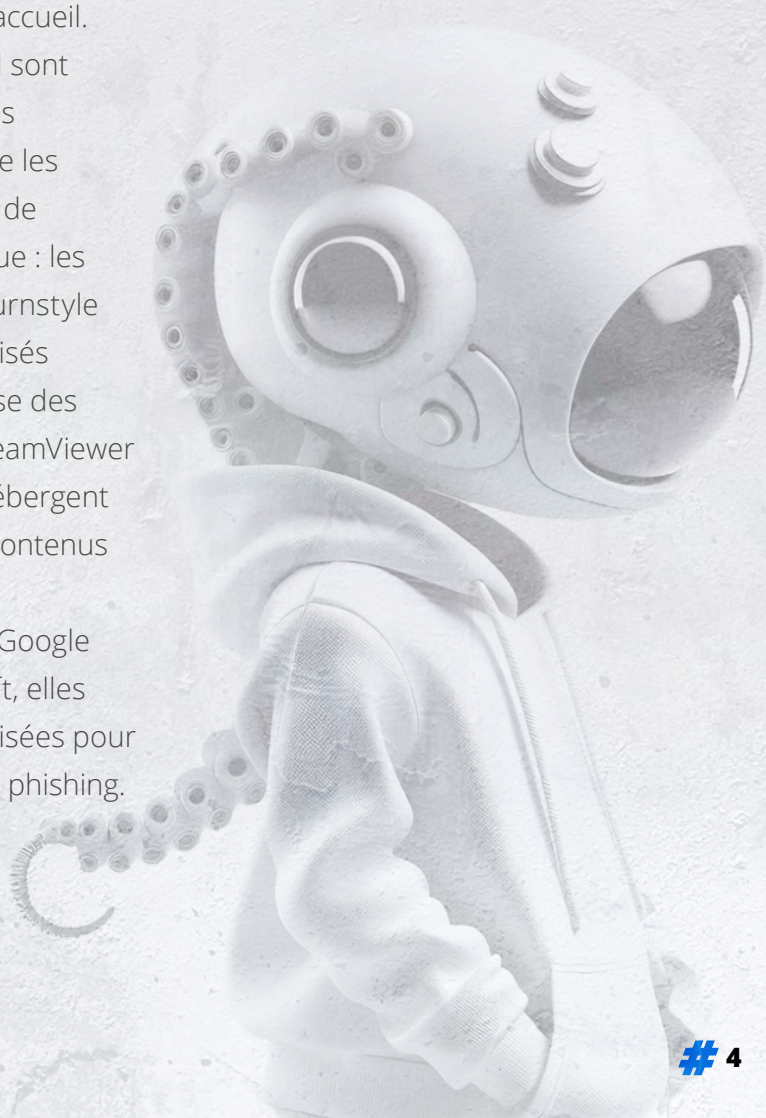
Les services cloud de Microsoft, Google et Evernote sont souvent utilisés par les pirates pour héberger leurs charges utiles et leurs pages d'accueil. D'autres services cloud sont fréquemment employés pour prendre en charge les différents composants de l'infrastructure d'attaque : les CAPTCHA Cloudflare Turnstyle sont régulièrement utilisés pour empêcher l'analyse des menaces ; Docusign, TeamViewer et Wave Compliance hébergent par inadvertance des contenus malveillants, quant aux messageries Gmail de Google et Outlook de Microsoft, elles sont régulièrement utilisées pour lancer des attaques de phishing.

03

PIEUVRES

ESPÈCE :

Expertes en **analyse**, elles sont dotées d'un système nerveux, d'un cerveau très développé et d'une grande capacité d'adaptation. Elles s'adaptent parfaitement à leur environnement et surmontent les défis, ce qui les distingue dans le renseignement sur les menaces.



K-2 TWO

LE CONTEXTE GÉOPOLITIQUE AUGMENTE LES RISQUES DE CYBERATTAQUE.

Les élections françaises et allemandes, ainsi que l'incertitude persistante concernant l'issue de la guerre entre la Russie et l'Ukraine, accroissent les tensions politiques au sein de l'Union européenne. L'abandon par le gouvernement américain des normes prévisibles pourrait également entraîner une hausse de l'activité cyber. Les experts en économie, en politique et en cybersécurité n'ont cessé d'alerter sur le fait que les tensions géopolitiques et le risque cyber sont étroitement liés. En 2025, les deux principaux risques identifiés lors de l'évaluation annuelle Systemic Risk Barometer menée par la société américaine de services financiers Depository Trust & Clearing Corporation (DTCC) étaient les risques cyber et géopolitiques.[5]

K-3 TWO

ALORS QUE LES PRINCIPALES TECHNOLOGIES D'AUTHENTIFICATION DES E-MAILS RENDENT LA TÂCHE PLUS DIFFICILE AUX CYBERCRIMINELS, L'IA AU CONTRAIRE LEUR OUVRE DE NOUVEAUX CHAMPS DE POSSIBILITÉS.

En exploitant des services légitimes, les pirates peuvent satisfaire aux exigences croissantes d'authentification des technologies de messagerie (SPF, DKIM et DMARC) et réussir ainsi, à apparaître comme une source fiable. Bien que ces technologies compliquent leurs attaques, les pirates continuent de trouver des services pour passer les contrôles d'authentification et d'alignement. De plus, la prolifération des chatbots d'IA permet aux apprentis hackers d'acquérir rapidement les compétences nécessaires.

5. « Geopolitical and Cyber Risks Remain Top Threats to the Financial Services Sector in 2025 », DTCC, 4 décembre 2024. https://www.dtcc.com/news/2024/december/04/geopolitical-and-cyber-risks-remain-top-threats-to-the-financial-services-sector-in-2025

K-4 FOUR

LES SECTEURS DES ACTIVITÉS JURIDIQUES, DES MÉDIAS, DE L'ÉDITION ET DE LA CULTURE ONT ENREGISTRÉ LE PLUS DE MENACES PAR UTILISATEUR AU SECOND SEMESTRE 2024.

La plupart des secteurs d'activité ont présenté un profil de menace bien spécifique : une proportion plus élevée de fichiers malveillants a ciblé le secteur de la culture, alors que les salariés du secteur des médias et de l'édition ont reçu le plus grand nombre de liens malveillants. Quant au secteur des logiciels et du SaaS, ce sont des attaques par usurpation d'identité qui ont été observées le plus fréquemment.

K-5 FIVE

LES HUMAINS DEMEURENT LE TALON D'ACHILLE DE LA CYBERSÉCURITÉ.

En règle générale, les violations de sécurité sont souvent rendues possibles par une intervention humaine permettant aux pirates d'accéder à des ressources sensibles ou protégées. La version 2024 du rapport annuel Data Breach Investigations Report (DBIR) révèle que plus des deux tiers (68 %) des violations survenues en 2023[6] comportaient « un élément humain non malveillant ». Une enquête menée en 2024 auprès de 1 000 salariés a révélé qu'un tiers (34 %) craignait de devenir eux-mêmes la vulnérabilité exploitée par des pirates, même si la grande majorité (86 %) considérait disposer de connaissances suffisantes en matière de cybersécurité[7]. Plus de la moitié des personnes interrogées craignaient de perdre leur emploi si elles se rendaient involontairement complices d'une cyberattaque portée à l'encontre de leur entreprise.

6. Rapport Verizon Data Breach Investigations Report, 2024
https://www.verizon.com/business/resources/reports/dbir/#takeaways
7. Why AI fuels cybersecurity anxiety, particularly for younger employees
https://www.ey.com/en_us/consulting/human-risk-in-cybersecurity

04

L'ENVI-RONNEMENT DES CYBER-MENACES

- DANS LES GRAPHIQUES
- PRINCIPALES MENACES ET CAMPAGNES
- MIMECAST RISK RADAR
- CHRONOLOGIE DES ÉVÉNEMENTS MAJEURS

CHAUVE-SOURIS

ESPÈCE :

Détecter les menaces est leur spécialité. Grâce à l'écholocalisation, elles émettent des ultrasons qui rebondissent sur les objets et leur fournissent une cartographie détaillée de leur environnement. Cela leur permet d'éviter les obstacles, même dans l'obscurité la plus totale.

04
.1

PANORAMA DES CYBERMENACES : GRAPHIQUES

Le panorama des menaces au second semestre 2024 a révélé une utilisation accrue des services cloud à la fois grand public et professionnels, permettant aux pirates d'échapper à toute détection. En effet, plusieurs services cloud majeurs sont exploités pour héberger du contenu malveillant, et nous observons une utilisation accrue de liens cloud en tant que mécanisme de distribution de charges utiles malveillantes.

Au cours du second semestre 2024, les cybercriminels se sont concentrés sur les secteurs de la culture, des services juridiques et des logiciels & services SaaS : un changement par rapport au premier semestre 2024 où les secteurs des banques, des voyages et de l'hôtellerie, ainsi que de la culture, constituaient les cibles privilégiées. Alors que chaque secteur d'activité a été confronté à un nombre significatif d'attaques par e-mail en masse provenant de sources de faible réputation, les pirates ont ciblé le secteur de la culture avec davantage d'attaques utilisant des fichiers malveillants. De leur côté, les services juridiques ont essuyé plus d'attaques par usurpation d'identité.

Voici ce à quoi ressemble le panorama des menaces, d'après les données recueillies :

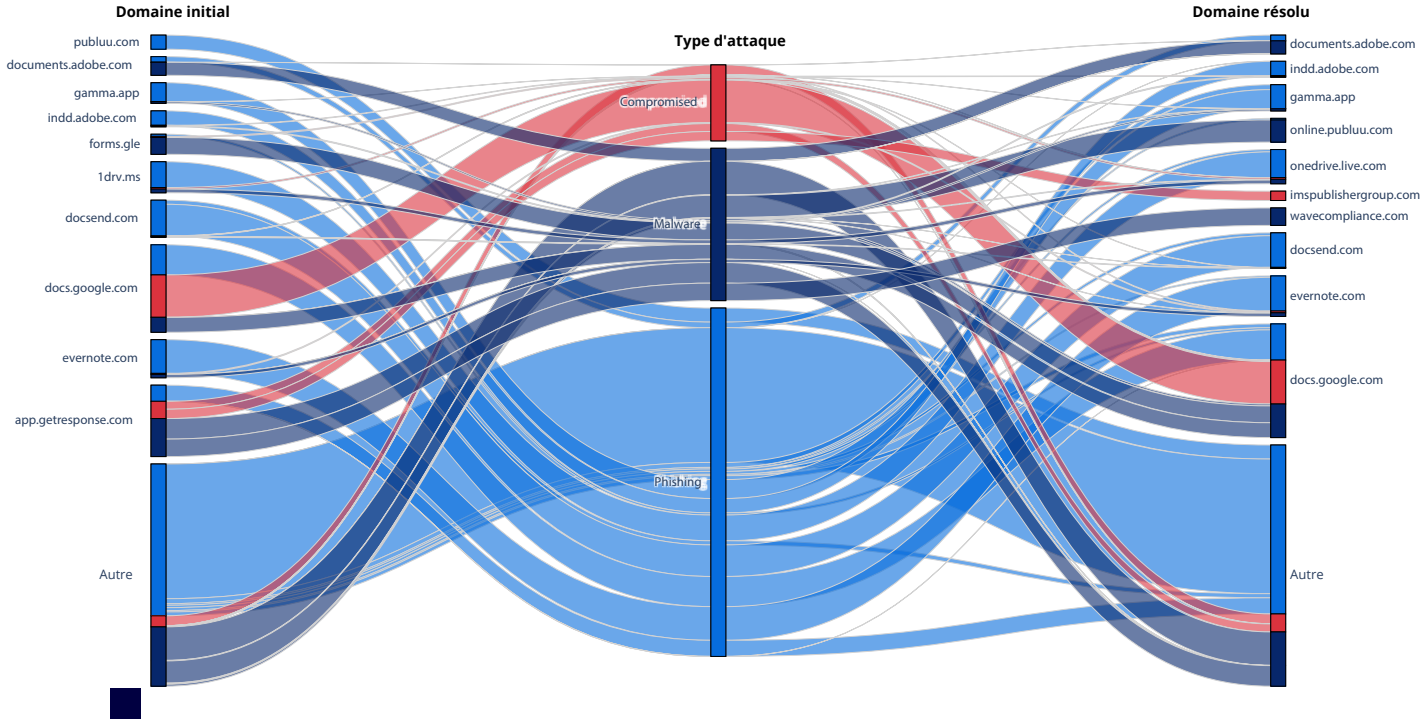
W 41°24'12.2 "
E 23°44'54.4"
PE-3 Nvgt B

UTILISATION ABUSIVE DES SERVICES CLOUD

#01

Les cybercriminels exploitent de plus en plus souvent des services cloud légitimes pour contourner les mécanismes de défense qui identifient principalement les attaques en détectant du code, des ressources et des services en ligne non fiables. Bien que certains choix pour héberger les infrastructures malveillantes apparaissent évidents, comme les plateformes Google Docs, Evernote.com et Dropbox DocSend, les pirates font également appel à d'autres services en ligne moins connus, comme le site de publication interactif Publuu, l'hôte de webinaires en ligne Wave Compliance et le site de présentations de diaporamas Gamma.

Les groupes malveillants ont également recours à des plateformes spécifiques pour envoyer des e-mails de phishing et différents sites pour héberger les charges utiles qui, souvent, sont de simples formulaires web ou fichiers comportant un lien. Le site de marketing GetResponse par exemple, reste une source importante d'e-mails de phishing, bien que beaucoup d'entre eux ne sont sans doute pas considérés comme malveillants, mais simplement comme indésirables. Bien que les sites Adobe ne soient pas les principaux hôtes de charges utiles, au moins deux d'entre eux ont été utilisés par les pirates pour héberger leurs pages d'accueil.



Graphique 1 : La plupart des domaines initiaux sont mis en relation avec des domaines finaux similaires, comme la plupart des attaques utilisant initialement Evernote et hébergeant également une charge utile. Toutefois, plusieurs cas se distinguent : une première plateforme qui héberge la page de redirection initiale, un grand volume de spams provenant du service de marketing GetResponse.com, puis une deuxième plateforme qui héberge la page de destination, comme le service de formation et de webinaire WaveCompliance.Compliance.

TPU PAR TYPE D'ATTAQUE

02

Alors qu'au second semestre 2024, les spams représentent toujours la grande majorité des messages bloqués par Mimecast, une augmentation des messages indésirables a pu être observée au cours de l'été. Bien que cette hausse se soit atténuée en fin d'année, les attaques de phishing, consistant à intégrer une URL renvoyant vers un site ou un service contrôlé par un hacker, ont connu une croissance modérée.

Mimecast classe les activités malveillantes et indésirables en fonction du moment où elles sont détectées :

LE SPAM interceptant les e-mails en masse et provenant de domaines non fiables et ceux dont le contenu est largement répandu.

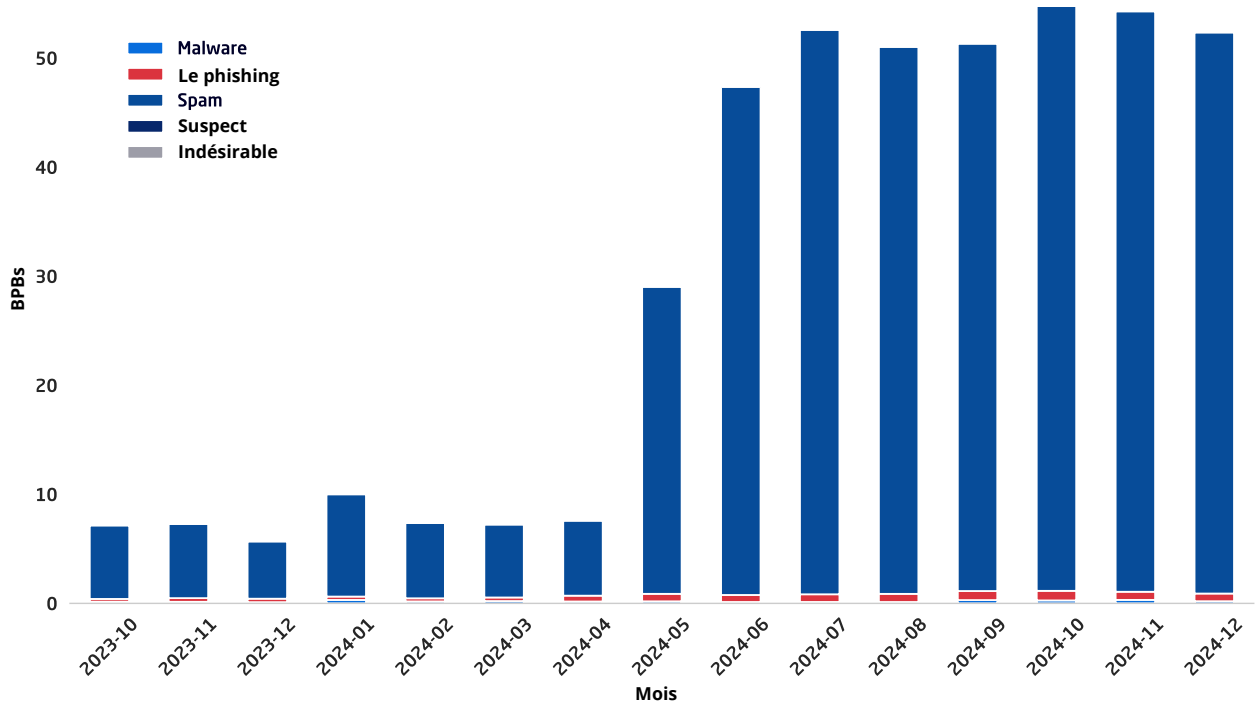
LES MESSAGES SUSPECTS messages, fichiers ou URL potentiellement malveillants - c'est-à-dire qu'aucun contenu nuisible n'a encore été détecté. Toutefois, certains indicateurs montrent que le message doit être traité avec prudence, notamment s'il provient d'un service qui subit actuellement un compromis ou d'une source réputée peu fiable.

LES INDÉSIRABLES comprenant les messages bloqués par l'utilisateur.

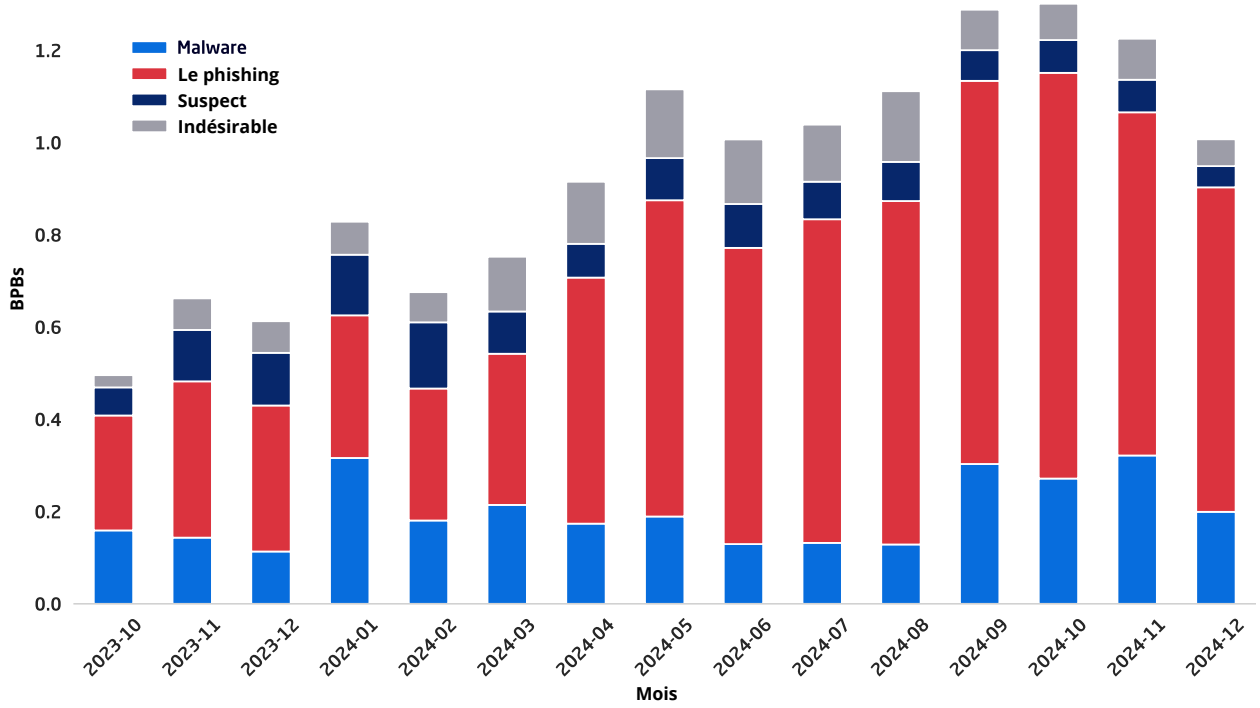
LES MENACES DE PHISHING conçues pour inciter leurs victimes à révéler des informations sensibles, telles que des identifiants ou des informations de paiement. Cela englobe les liens de phishing, les BEC, l'usurpation d'identité ou les pièces jointes HTML conçues pour imiter les pages de connexion.

LES MESSAGES DE MALWARE contenant des pièces jointes identifiées comme malveillantes ou des liens pointant vers des malwares.

L'augmentation significative du nombre de spams détectés entre le premier et le second semestre 2024 est davantage due à l'évolution du système de détection et de collecte des données de Mimecast, plutôt qu'à une réelle augmentation du volume de spams. L'augmentation des détections de spams survient car Mimecast a intégré les spams retenus au niveau de la passerelle aux données de détection, une option configurable par l'administrateur, plutôt que de se fier uniquement aux rejets de spams.



Graphique 2a : L'augmentation significative du nombre de spams détectés résulte de l'intégration des spams retenus au niveau de la passerelle, plutôt que de se fier uniquement aux rejets de spam. Ce changement introduit également un élément configurable au niveau de l'administration pour gérer la rétention des spams.



Graphique 2b : Eliminer l'influence écrasante de l'ensemble de données sur les spams montre que le phishing est en hausse et qu'une recrudescence des attaques de malware a eu lieu à la fin du second semestre 2024. En décembre 2024, la détection de malware en Afrique subsaharienne a bondi de 42,14 %, soit une augmentation significative par rapport à l'année précédente, en raison de l'instabilité politique et de l'augmentation de l'activité cyber. En outre, cette région observe une nette augmentation des attaques par ransomware, qui deviennent plus opportunistes, exploitant souvent des vulnérabilités et se manifestant sous forme d'infections secondaires. Ceci témoigne d'une tendance préoccupante dans le contexte des menaces.

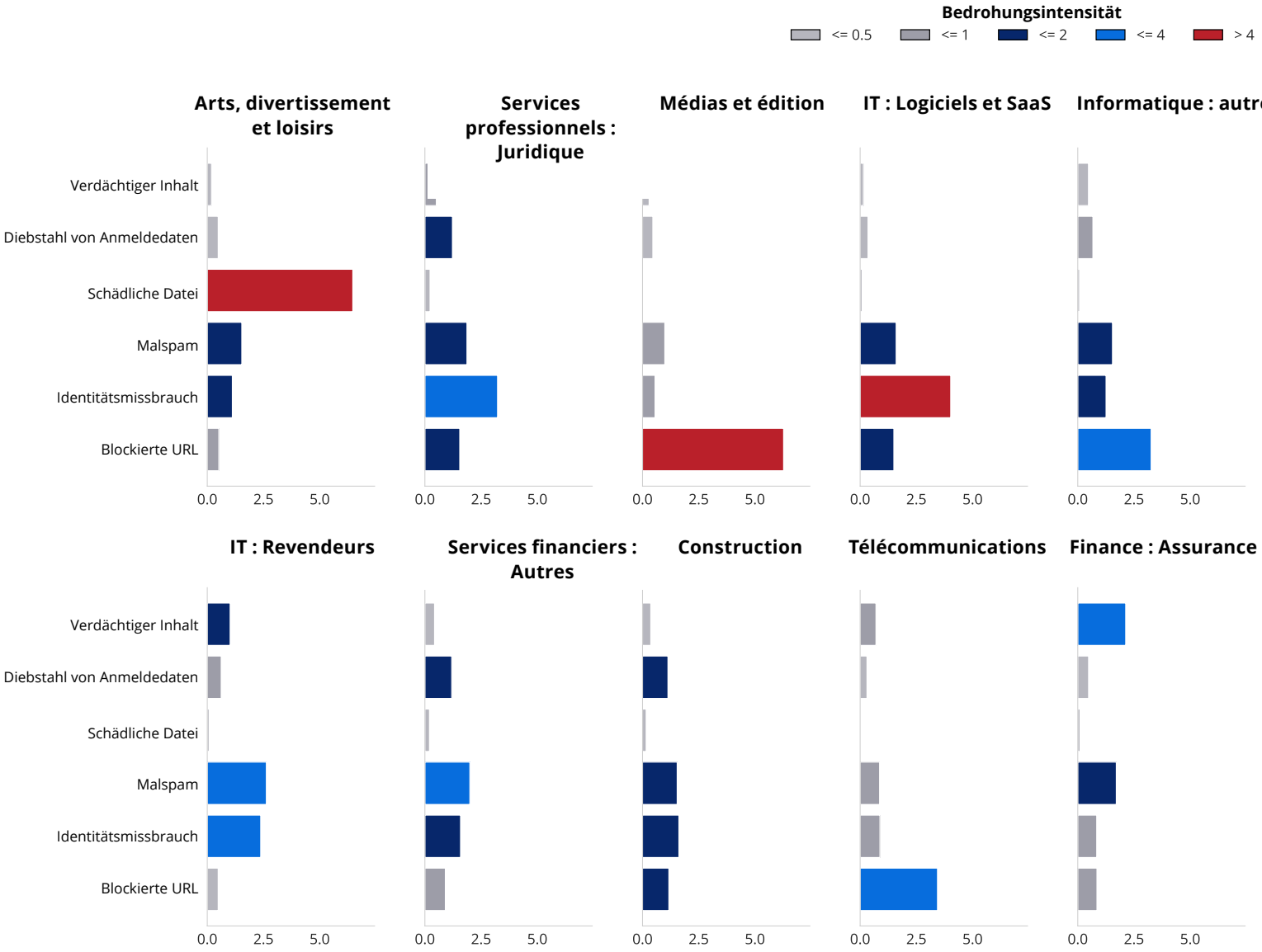
PRINCIPAUX SECTEURS D'ACTIVITÉ CIBLÉS, CLASSÉS PAR TPU

03

Les cybercriminels ont tendance à recourir à divers types d'attaques pour cibler différents secteurs, conférant à chacun un profil de menace distinctif. Le secteur de la culture, le plus ciblé après la suppression d'un grand volume de spams, a fait face au plus grand nombre de menaces par utilisateur (TPU), la plupart des attaques prenant la forme d'e-mails et de messages contenant des charges utiles malveillantes.

Services professionnels : les secteurs des activités juridiques, des médias et de l'édition ont enregistré le deuxième plus fort niveau de menace, chacun ayant été confronté à près de 9 menaces par utilisateur. Le secteur du juridique a subi un plus grand nombre d'attaques par usurpation d'identité, tandis que le secteur des médias et de l'édition a été confronté à un grand nombre d'URL malveillantes.

Chaque secteur note un volume significatif de spams et de menaces détectées en raison de l'utilisation par les attaquants d'une infrastructure à faible réputation. Dans le cadre de cette analyse, Mimecast a supprimé les e-mails groupés, détectés comme spams ou ayant une faible réputation. Ces derniers représentaient respectivement 17 TPU et 5 TPU.



Graphique 3 : Le profil de menace pour les 10 principaux secteurs, sans les catégories Spam et Faible réputation qui ont tendance à surcharger les données. Le nombre de menaces par utilisateur (axe des x) est gradué selon une échelle logarithmique.

GROUPES DE MENACE
#04

Remonter à la source des cybermenaces est intrinsèquement complexe. Cette tâche est encore plus ardue avec les tactiques mixtes que de nombreux cybercriminels utilisent et l'essor des modèles de cybercriminalité en tant que service, tels que le Ransomware-as-a-Service (RaaS), le Phishing-as-a-Service (PhaaS) et les courtiers d'accès initiaux (IAB). Ces services permettent aux pirates de réutiliser les mêmes outils et les mêmes infrastructures, conduisant au lancement d'attaques similaires par des groupes cybercriminels différents. Les pirates appliquent souvent une combinaison de techniques issues de divers vecteurs d'attaque et modifient fréquemment leurs méthodes, ce qui rend particulièrement difficile l'identification d'un hacker ou d'un motif en particulier.

Les méthodes traditionnelles d'attribution des cybermenaces reposant sur l'infrastructure ou les signatures de malwares, deviennent ainsi de moins en moins fiables. Mimecast se concentre sur l'analyse des tactiques, techniques et procédures (TTP) pour classer et référencer systématiquement les opérations liées aux menaces. En suivant le mode de fonctionnement des hackers, nous regroupons les menaces et identifions des schémas à travers les campagnes, même lorsque les méthodes d'attribution traditionnelles échouent. Cette approche permet d'obtenir une compréhension plus claire et plus fiable de l'évolution de leurs capacités. Les opérations malveillantes les plus prolifiques, référencées en interne par Mimecast, sont mises en évidence ci-dessous, accompagnées des campagnes associées pour décrire leurs comportements et leur impact potentiel.

Nom de la menace

TO1014

Première observation : 2020

OBJECTIF

VOL D'INFORMATIONS ET ESPIONNAGE

CIBLE

AMÉRIQUE DU NORD
EUROPE
MOYEN-ORIENT

Secteur

AÉRONAUTIQUE
AÉROSPATIALE
TRANSPORT

OCT. 2021

Dernières campagnes

Nom de la menace

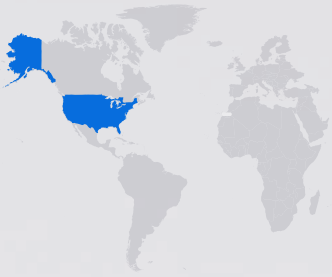
TO1003

Première observation : 2018

OBJECTIF

VOL DE DONNÉES

CIBLE



PRINCIPALEMENT AMÉRICAIN

SECTEUR

INFORMATIQUE
ÉDUCATION

OCT. 2021

Dernières campagnes

Nom de la menace

TO3010

Première observation : 2018

OBJECTIF

RASSEMBLER LES IDENTIFIANTS POUR LA DISTRIBUTION

CIBLE

AFRIQUE DU SUD

Secteur

TOUTES

NOV. 2021

Dernières campagnes

Nom de la menace

TO5004

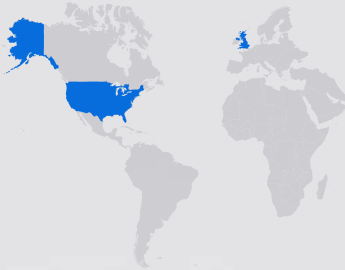
Première observation : 2024

OBJECTIF

FINANCIER

INFORMATIONS SUR LA CAMPAGNE

CIBLE



PRINCIPALEMENT
ROYAUME-UNI
ÉTATS-UNIS

Secteur

FABRICATION
IMMOBILIER
VENTE AU DÉTAIL

DÉC. 2021

Dernières campagnes

Nom de la menace

TO3028

Première observation : 2018

OBJECTIF

COLLECTE D'IDENTIFIANTS

INFORMATIONS SUR LA CAMPAGNE

CIBLE

MONDE ENTIER

Secteur

TOUTES

DEC 2021

Dernières campagnes

Nom de la menace

TO3001

Première observation : 2023

OBJECTIF

VOL D'IDENTIFIANTS ET DE DONNÉES

CIBLE

AUSTRALIE

SECTEUR

PRINCIPALEMENT ÉDUCATION

DEC 2021

Dernières campagnes

Nom de la menace

TO5005

Première observation : 2020

OBJECTIF

FINANCIER

CIBLE

MONDE ENTIER

Secteur

TOUTES

DEC 2021

Dernières campagnes

Nom de la menace

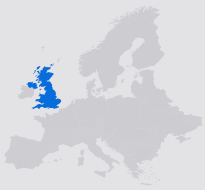
TO3022

Première observation : 2021

OBJECTIF

COLLECTE D'IDENTIFIANTS

CIBLE



PRINCIPALEMENT ROYAUME-UNI

Secteur

TOUTES

DEC 2021

Dernières campagnes

EVOLUTION DES PRINCIPALES VULNÉRABILITÉS AU FIL DU TEMPS

#05

Alors que la grande majorité des attaques visant à exploiter des problèmes logiciels se sont concentrées sur deux vulnérabilités bien connues (CVE-2017-0199 et CVE-2022-42889), les cybercriminels ont tenté d'exploiter 89 problèmes différents lors du second semestre 2024. En comparant les 10 principales vulnérabilités détectées par Mimecast au sein d'un e-mail ou distribuées sous forme de lien, 7 problèmes ont atteint un score EPSS (Exploitability Prediction Scoring System) d'au moins 0,88, ce qui équivaut à une probabilité d'exploitation de 88 % sous 30 jours. De même, 2 vulnérabilités, toutes deux découvertes en 2024, n'ont pas encore été enregistrées comme étant exploitées.

La cartographie ci-dessous illustre également la divergence entre le score EPSS et le score CVSS (Système d'Evaluation de la Criticité des Vulnérabilités), qui semble être corrélé avec la gravité potentielle de l'exploitation.

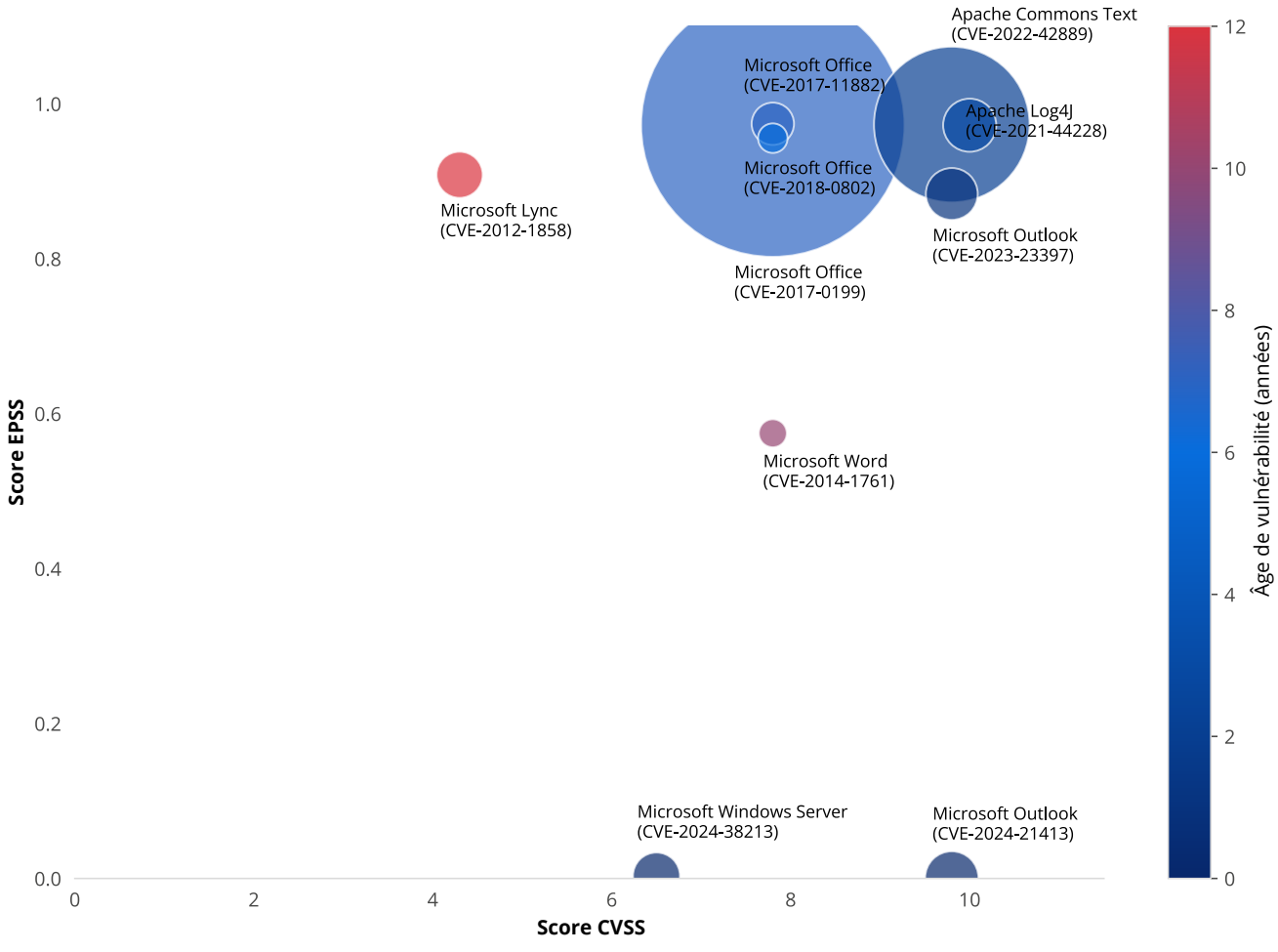


Chart 5: The Top 10 vulnerabilities detected in messages, compared by EPSS and CVSS scores. Two popular vulnerabilities are at least 10 years old. EPSS data collected as of 15 January 2025.

PRINCIPALES MENACES ET CAMPAGNES

04.2

01
SPOOFING OUVERT

02
VIOLATION DES DROITS D'AUTEUR / CONFIRMATION D'ABONNEMENT

03
INCITER LES VICTIMES À COPIER/COLLER DES LIENS - FRAUDE AU FAUX FOURNISSEUR

04
ESCROQUERIE BEC CIBLÉE AVEC DEEPFAKE AUDIO

05
LIVRAISON MANQUÉE

06
PIRATAGE D'UN COMPTE FACEBOOK - USURPATION D'IDENTITÉ DE MARQUE

#01 SPOOFING OUVERT

TECHNIQUE : Routeurs de particuliers compromis utilisés comme relais pour des e-mails de phishing usurpés via les services de messagerie des FAI

SERVICES UTILISÉS : Zimbra, MagicMail

CIBLES : International, tous secteurs d'activité

LIRE L'ARTICLE

Cybercriminel

↓

Exploitation des routeurs FAI de particuliers en raison de vulnérabilités connues ou de mots de passe faibles

↓

Routeur configuré pour servir de proxy

↓

E-mails de phishing relayés par les serveurs de messagerie des FAI

↓

Liens malveillants hébergés sur divers services cloud

↓

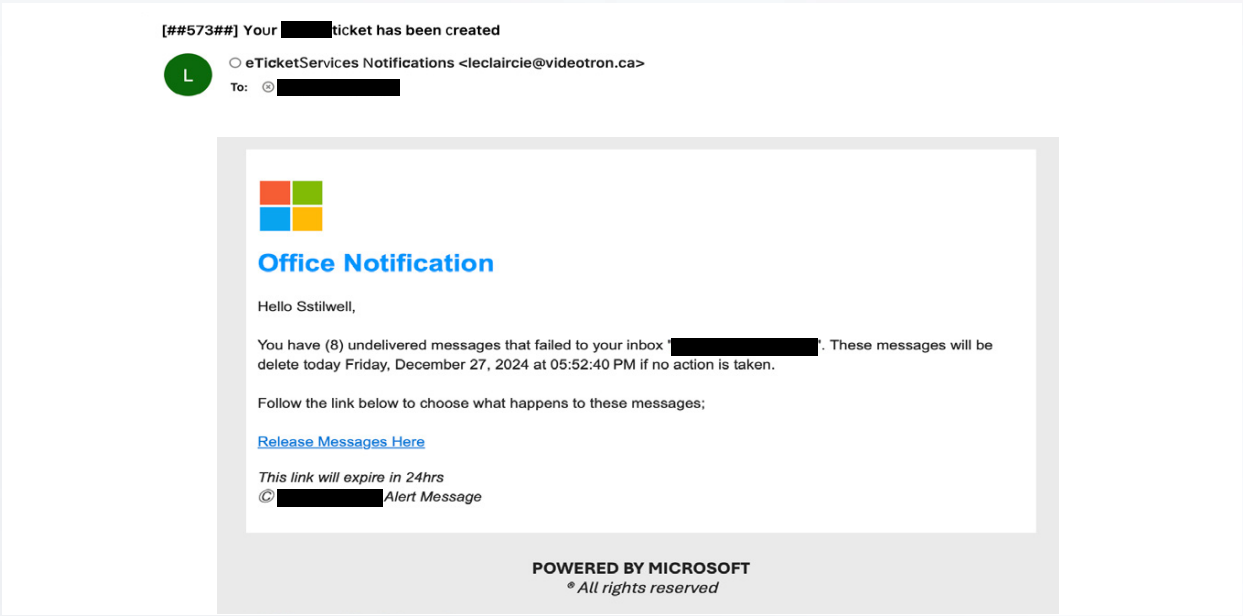
Demande de saisie du nom d'utilisateur et du mot de passe Microsoft 365

↓

Identifiants collectés et utilisateur redirigé vers la vraie page de connexion de Microsoft 365

Les cybercriminels exploitent des routeurs de particuliers compromis comme des proxys pour envoyer des campagnes de phishing d'identifiants à grande échelle via les services de messagerie des FAI, masquant ainsi leur propre infrastructure et contournant les mécanismes d'authentification des e-mails. En exploitant les FAI dont l'authentification des e-mails sortants est faible ou inexistante, les cybercriminels parviennent à distribuer des volumes élevés et à utiliser des capacités d'usurpation d'identité de l'expéditeur sans restriction.

Les fournisseurs d'accès à Internet concernés et identifiés lors de notre enquête utilisent des solutions de messagerie électronique telles que Zimbra et MagicMail, et ne semblent pas disposer de mesures anti-spam sortantes particulièrement efficaces. La combinaison d'une authentification insuffisante et de contrôles de sécurité plus faibles permet aux pirates d'atteindre des taux d'envoi élevés et de mener facilement des campagnes de spams à grande échelle sans être inquiétés.



#02 VIOLATION DES DROITS D'AUTEUR / CONFIRMATION D'ABONNEMENT

TECHNIQUE : usurpation d'identités de cabinets d'avocats utilisant de prétendues violations de droits d'auteur comme prétexte pour dérober des informations

SERVICES UTILISÉS : Gmail, publipostage

CIBLES : l'international, mais principalement le Royaume-Uni, le commerce de détail, le commerce de gros, les secteurs du tourisme et de l'hôtellerie

LIRE L'ARTICLE

Cybercriminel

↓

E-mail de phishing par le biais du service de publipostage

↓

Liens vers du contenu hébergé sur Dropbox

↓

Téléchargement d'un fichier zip contenant le code exécutable

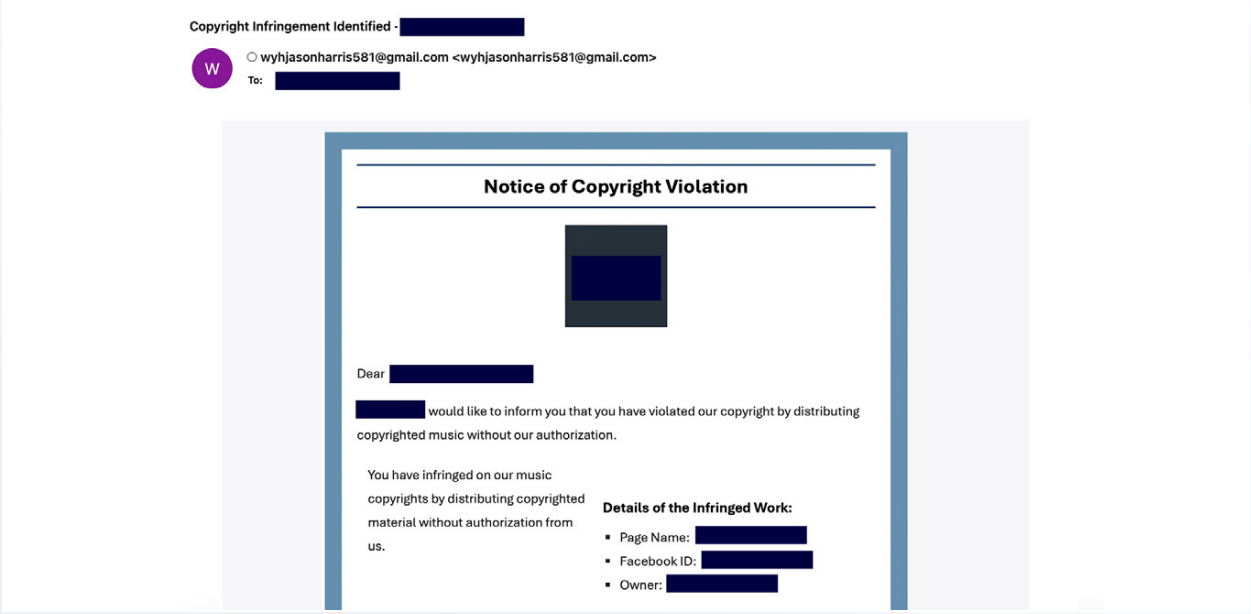
↓

Téléchargement d'un infostealer depuis Github via le fichier exécutable

↓

Exfiltre les données sensibles

Au moyen d'e-mails malveillants envoyés via Gmail par un service de publipostage, des pirates se font passer pour des cabinets d'avocats réputés et prétendent que les entreprises ciblées violent des droits d'auteur. L'e-mail ainsi envoyé contient un lien direct ou une redirection vers Dropbox entraînant le téléchargement d'un fichier zip contenant un code exécutable. L'objectif de ces campagnes est d'utiliser divers logiciels malveillants pour voler des informations sensibles sur les machines infectées, telles que des identifiants et des données financières confidentielles.



#03 INCITER LES VICTIMES À COPIER/COLLER DES LIENS - FRAUDE AU FAUX FOURNISSEUR

TECHNIQUE : Amener les utilisateurs à copier et à coller un lien pour contourner les défenses

SERVICES UTILISÉS : Amazon Simple Email Service, mailers Python

CIBLES : Les États-Unis principalement : l'industrie manufacturière, le commerce de détail et le secteur juridique

LIRE L'ARTICLE

Cybercriminel

↓

E-mail de phishing via AWS en utilisant le mailer Python

↓

L'utilisateur est invité à coller une URL malformée dans son navigateur

↓

Redirection vers un fichier partagé hébergé sur un faux SharePoint

↓

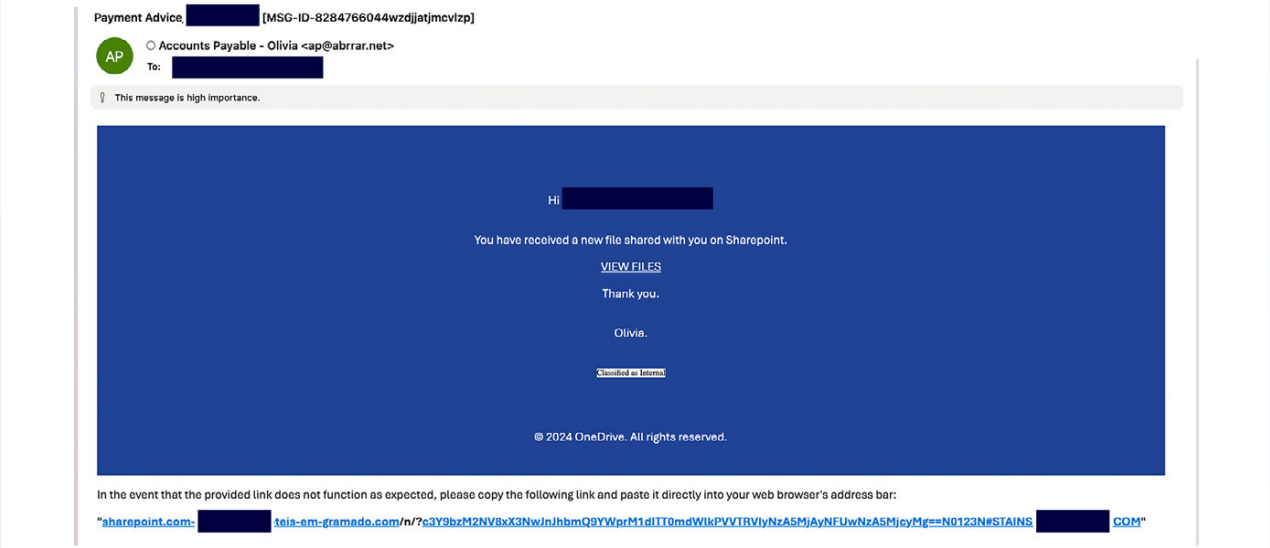
Demande de saisie du nom d'utilisateur et du mot de passe Microsoft 365

↓

Identifiants collectés et utilisateur redirigé vers la vraie page de connexion de Microsoft 365

En s'efforçant d'échapper aux logiciels et aux services de détection des menaces, les cybercriminels tâchent de convaincre les utilisateurs de copier des liens mal formés depuis un e-mail, d'où le préfixe « http:// » est souvent absent, et de les coller dans leur navigateur. Les leurres analysés par Mimecast comprenaient généralement un bouton avec un lien inactif et un message du genre « Si ce lien ne fonctionne pas, veuillez copier et coller le lien ci-dessous dans votre navigateur ».

Cette technique s'ajoute à d'autres méthodes visant à tromper les victimes, telles que l'utilisation de codes QR pour rendre les liens illisibles par les humains et le recours au stress comme moyen de pression pour inciter les victimes à appeler un centre d'appel contrôlé par des pirates. L'objectif des campagnes reposant sur ce type d'attaque est généralement de dérober les identifiants des victimes.



#04 ESCROQUERIE BEC CIBLÉE AVEC DEEPFAKE AUDIO

TECHNIQUE : Deepfake audio, compromission de messagerie d'entreprise (BEC)
SERVICES UTILISÉS : Adobe Sign, DocuSign
CIBLES : International, principalement les secteurs financiers

LIRE L'ARTICLE

Cybercriminel

Envoi d'un e-mail BEC via Docusign ou Adobe Sign

L'utilisateur signe un accord de confidentialité numérique

L'utilisateur appelle un faux numéro pour vérifier l'accord de non-divulgation

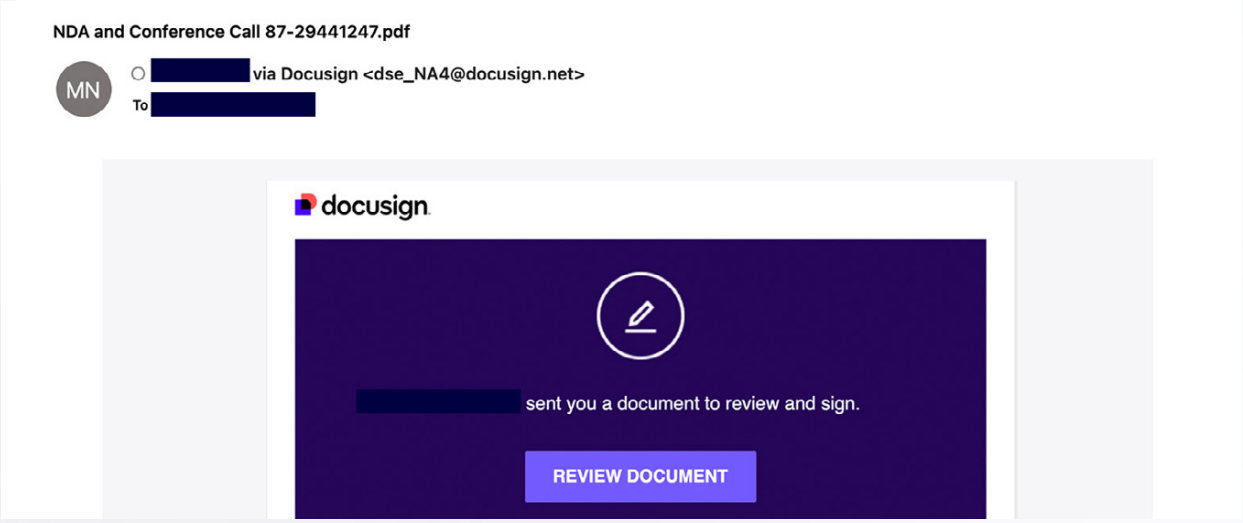
L'interaction par e-mail donne lieu à une facture pour un paiement

Audio deepfake d'un dirigeant validant le paiement

Virement effectué sur le compte bancaire du pirate

Les employés des secteurs de la banque, de l'assurance et d'autres secteurs financiers sont la cible d'e-mails de spear phishing semblant provenir d'un cabinet d'avocats réputé. Pour parfaire l'illusion, les documents font appel à un service de signature qualifiée comme Docusign ou Adobe Sign.

Les messages ciblés demandent à l'employé de signer l'accord de non-divulgation, puis d'appeler un numéro censé provenir d'un cabinet d'avocats, en réalité contrôlé par l'attaquant. Le cybercriminel se fait passer pour un expert juridique en utilisant des techniques de deepfake audio pour déguiser sa voix. Il envoie un e-mail depuis un domaine qu'il contrôle, semblable à celui du cabinet d'avocats usurpé. Enfin, le pirate envoie une facture prétendument émise par le cabinet d'avocats et enchaine avec un appel (deepfake audio) en se faisant passer pour le PDG de l'entreprise ou un autre dirigeant.



#05 LIVRAISON MANQUÉE

TECHNIQUE : Exploitation des services de confiance
SERVICES UTILISÉS : Compartiments Amazon S3 pour héberger des fichiers HTML
CIBLES : Royaume-Uni, organisations à but non lucratif et secteur de l'immobilier

LIRE L'ARTICLE

Cybercriminel

↓

E-mail de phishing via le FAI japonais Biglobe

↓

Redirigé vers un fichier HTML hébergé sur AWS

↓

Fichier HTML usurpe l'identité de la page de livraison manquée EVRI

↓

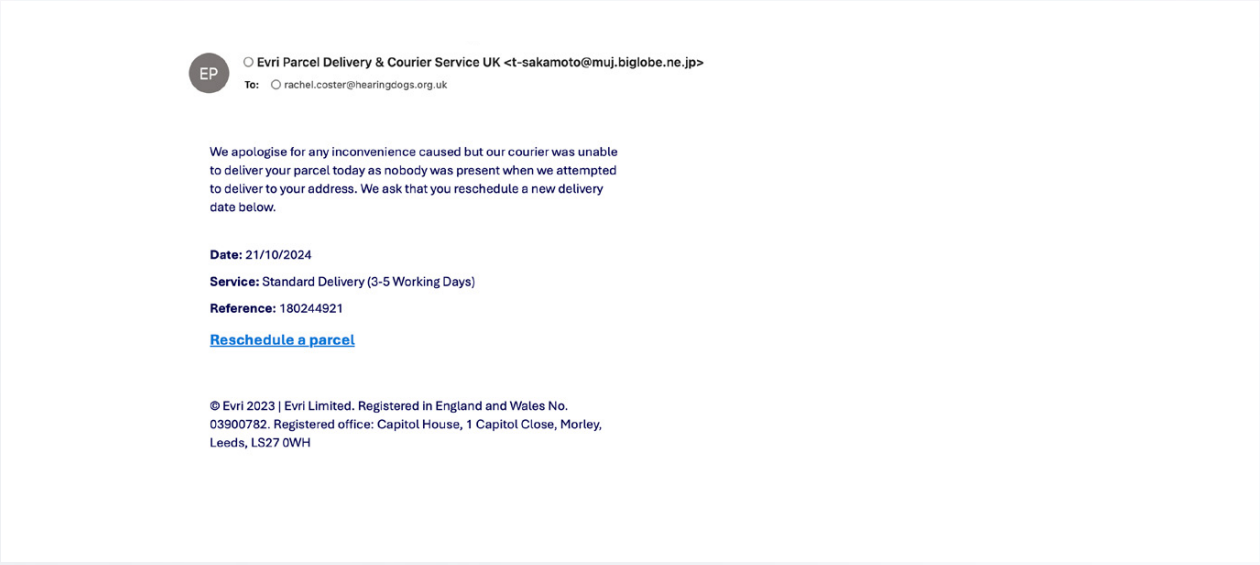
Informations personnelles identifiables (PII) et coordonnées bancaires fournies pour effectuer la nouvelle livraison

↓

Carte de crédit utilisée ou vendue sur un marché clandestin

Les messages envoyés via BIGLOBE, fournisseur d'accès Internet japonais souvent exploité par des cybercriminels, ciblent les associations à but non lucratif et les organismes du logement au Royaume-Uni avec des messages indiquant qu'une livraison n'a pas pu être effectuée.

De nombreux fournisseurs d'accès à Internet en Asie ont permis, ou ne sont pas conscients, des abus significatifs de leurs réseaux. Les cybercriminels profitent de ces fournisseurs d'accès en achetant des comptes authentifiés sur des marchés clandestins. Cela leur donne ainsi un accès légitime à leur infrastructure et leur permet d'envoyer des e-mails malveillants qui contournent la plupart des protocoles d'authentification des e-mails.



EP ○ Evri Parcel Delivery & Courier Service UK <t-sakamoto@muj.biglobe.ne.jp>
To: ○ rachel.coster@hearingdogs.org.uk

We apologise for any inconvenience caused but our courier was unable to deliver your parcel today as nobody was present when we attempted to deliver to your address. We ask that you reschedule a new delivery date below.

Date: 21/10/2024
Service: Standard Delivery (3-5 Working Days)
Reference: 180244921

Reschedule a parcel

© Evri 2023 | Evri Limited. Registered in England and Wales No. 03900782. Registered office: Capitol House, 1 Capitol Close, Morley, Leeds, LS27 0WH

#06 PIRATAGE D'UN COMPTE FACEBOOK - USURPATION D'IDENTITÉ DE MARQUE

TECHNIQUE : Fausse proposition d'emploi sur les réseaux sociaux en se faisant passer pour des marques réputées telles que Victoria's Secret, Red Bull ou Coca-Cola

SERVICE UTILISÉ : Recruitee

CIBLES : Le Royaume-Uni et les États-Unis principalement, et notamment les secteurs des médias, de l'édition et du commerce de détail

Cybercriminel

↓

E-mail de phishing envoyé par le logiciel de recrutement Recruitee

↓

Page d'inscription possédant le même domaine que la marque usurpée

↓

Connexion via une fausse page Facebook pour soumettre sa candidature

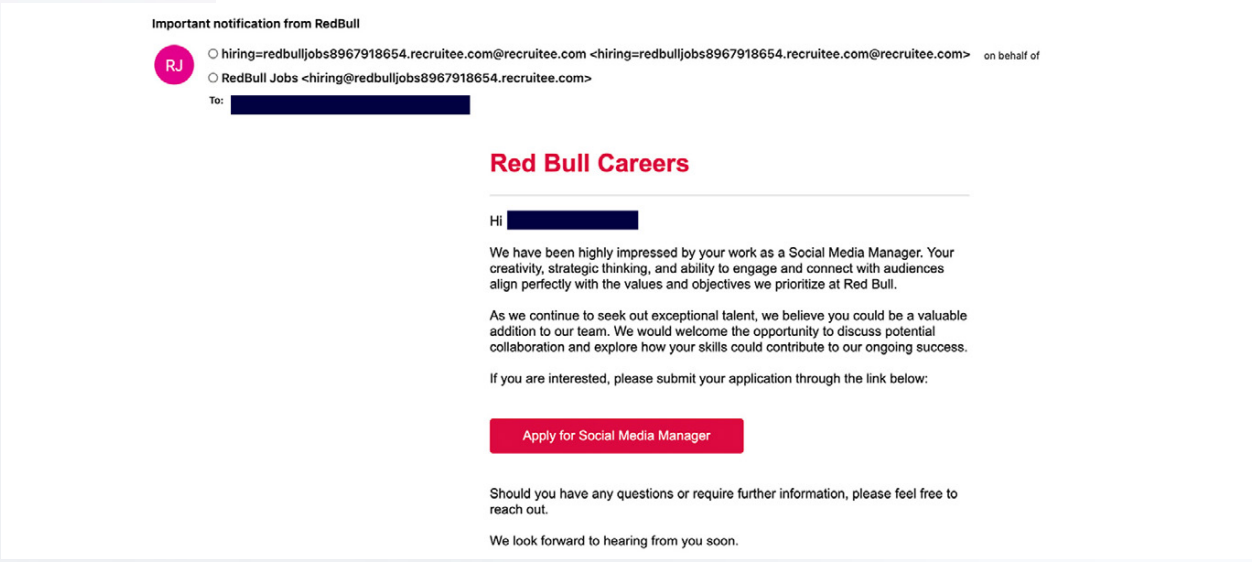
↓

Codes MFA requis pour postuler

↓

Identifiants Facebook obtenus et partagés via un logger Telegram

Une récente campagne de phishing a exploité Recruitee, un logiciel légitime de recrutement collaboratif, pour envoyer des e-mails frauduleux portant sur des offres d'emploi factices. Les cybercriminels enregistrent des domaines similaires et se font passer pour des marques réputées pour ajouter plus de crédibilité à la fraude. Les pages de phishing utilisent des CAPTCHA et un filtrage de l'adresse IP pour empêcher la détection automatique et visent à collecter les identifiants Facebook.



Important notification from RedBull

RJ

hiring=redbulljobs8967918654.recruitee.com@recruitee.com <hiring=redbulljobs8967918654.recruitee.com@recruitee.com> on behalf of

RedBull Jobs <hiring@redbulljobs8967918654.recruitee.com>

To: [redacted]

Red Bull Careers

Hi [redacted]

We have been highly impressed by your work as a Social Media Manager. Your creativity, strategic thinking, and ability to engage and connect with audiences align perfectly with the values and objectives we prioritize at Red Bull.

As we continue to seek out exceptional talent, we believe you could be a valuable addition to our team. We would welcome the opportunity to discuss potential collaboration and explore how your skills could contribute to our ongoing success.

If you are interested, please submit your application through the link below:

Apply for Social Media Manager

Should you have any questions or require further information, please feel free to reach out.

We look forward to hearing from you soon.

04
.3

MIMECAST RISKRADAR

LES CYBERCRIMINELS UTILISENT DE PLUS EN PLUS DES SERVICES LÉGITIMES

Les cybercriminels ont aujourd'hui davantage recours à des services légitimes pour contourner les défenses basées sur la réputation et la confiance. Cela va des fournisseurs de messagerie de confiance aux sites de partage de fichiers, sans oublier les services d'hébergement de webinaires. Les attaques sont couramment lancées sur les principales plateformes de messagerie, tels que Gmail de Google et Outlook de Microsoft (anciennement Hotmail), tandis que les liens malveillants insérés dans les e-mails se retrouvent souvent sur un service d'hébergement légitime comme Google Docs, Evernote ou encore les services OneDrive et SharePoint de Microsoft.

Alors que les plus grands fournisseurs de services légitimes trouvent régulièrement de nouveaux moyens de dissuader les abus, les attaquants se tournent également vers de plus petits fournisseurs. Les principales campagnes suivies par Mimecast par exemple, ont eu recours à des fournisseurs tels que Airtable, Publuu et WaveCompliance.

LES RISQUES GÉOPOLITIQUES AUGMENTENT

Alors que les tensions géopolitiques augmentent aux quatre coins du monde, l'environnement des menaces continue d'évoluer. Les cybercriminels sont plus actifs que jamais et utilisent le domaine cyber pour recueillir des renseignements, compromettre les infrastructures critiques de nations rivales et accroître leurs revenus. La perception d'une certaine forme d'immunité et d'absence de conséquences concrètes pour les opérations cyber incite les nations à étendre la portée de leurs opérations et encourage les groupes cybercriminels à mener des attaques toujours plus audacieuses.

Cependant, les forces de l'ordre sont de plus en plus en mesure de mettre à mal les infrastructures des cybercriminels. En parallèle, les systèmes de défense déployés par les entreprises les rendent de moins en moins faciles à pirater. Suite de l'invasion de l'Ukraine par la Russie, les deux pays ont épuisé leur stock d'exploits zero-day et n-day, provoquant un pic (voir Figure 1) qui s'est atténué depuis. En 2024, le nombre total de vulnérabilités signalées dans le catalogue des vulnérabilités exploitées connues (KEV) a conservé un rythme stable, mais somme toute relativement faible.

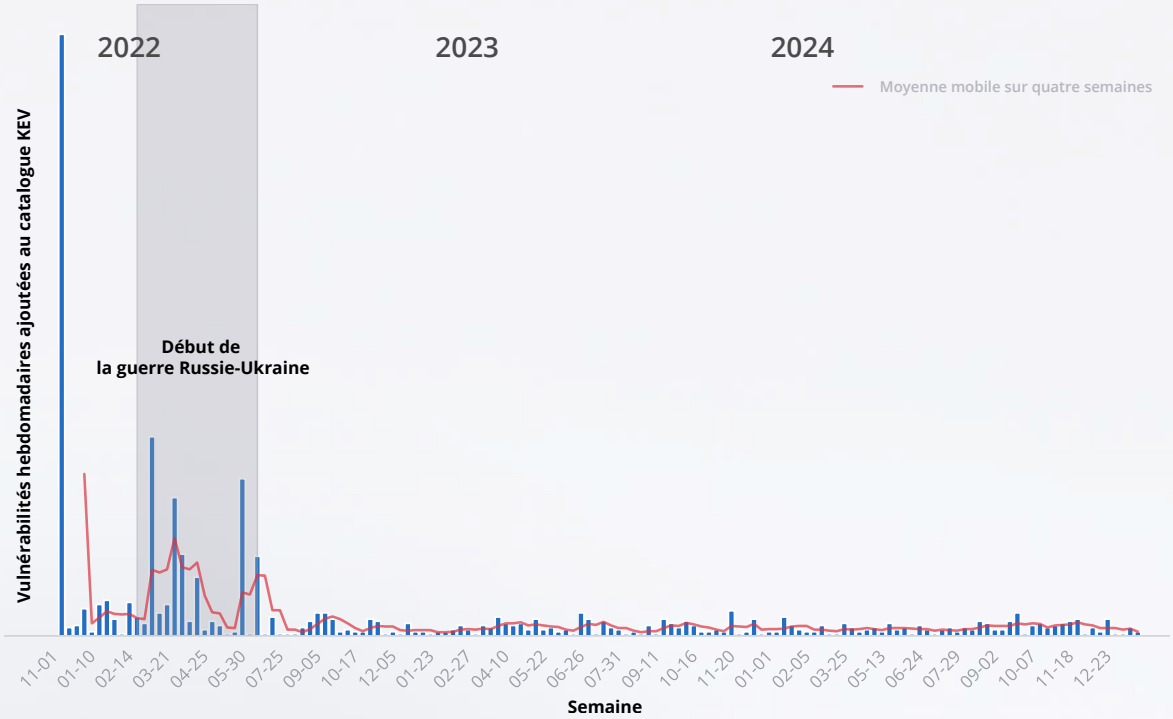


Figure 1 : Du milieu de l'année 2022 jusqu'à la fin 2024, l'agence fédérale américaine de cybersécurité et de sécurité des infrastructures (CISA) a ajouté environ 4 vulnérabilités par semaine au catalogue KEV, selon les données recueillies pendant cette période. Ces données révèlent un pic important lors de la première publication de la liste, suivi d'une activité soutenue pendant les premiers mois de l'invasion de l'Ukraine par la Russie.

Si la géopolitique est à l'origine de l'augmentation du niveau de la cybermenace, les événements mondiaux offrent également aux groupes de cybercriminels une plus grande variété de leurres.

Voici les principaux leurres géopolitiques identifiés par Mimecast :

01
CHINE-TAÏWAN

02
CHINE-MER DE CHINE MÉRIDIONALE

03
CÂBLE SECTIONNÉ EN CHINE

04
GUERRE ENTRE LA RUSSIE ET L'UKRAINE

05
CONFLIT ISRAËL-GAZA

06
LÉGISLATION DE L'UNION EUROPÉENNE

07
ÉLECTIONS EN RUSSIE ET AUX ÉTATS-UNIS

08
ÉLECTIONS EN IRAN ET AUX ÉTATS-UNIS

09
ÉVÉNEMENTS MÉTÉOROLOGIQUES AUX ÉTATS-UNIS

SECTEURS D'ACTIVITÉS LES PLUS CIBLÉS :

Parmi les secteurs confrontés aux plus importants niveaux de menace, on retrouve le secteur de la culture (arts, divertissements, loisirs), avec plus de 10 menaces par utilisateur (TPU) enregistrées, suivi des services professionnels « juridique » et enfin, le secteur des médias et de l'édition, confrontés à près de 9 TPU.

La plupart des secteurs d'activité ont été confrontés à un profil de menace distinct. Le secteur de la culture a observé une proportion bien plus élevée d'attaques utilisant des fichiers malveillants, tandis que les salariés des cabinets d'avocats ont constaté un nombre significatif d'attaques par usurpation d'identité. Les pirates ont ciblé les employés du secteur des médias et de l'édition principalement avec des liens malveillants, tandis que le secteur des logiciels et du SaaS a été la cible de nombreuses attaques par usurpation d'identité.

Dans le cadre de cette analyse, Mimecast a supprimé les e-mails groupés, détectés comme étant du spam ou ayant une faible réputation. Ces derniers représentaient respectivement 17 TPU et 5 TPU.

01	CULTURE	10.322010 TPU
02	CABINETS D'AVOCATS	8.613564 TPU
03	MÉDIAS ET ÉDITION	8.622578 TPU

CHRONOLOGIE DES ÉVÉNEMENTS MAJEURS

04.2

JUIL.
10 MILLIARDS DE MOTS DE PASSE DIVULGUÉS

SEPT.
LES PLATEFORMES D'ÉCHANGE DE CRYPTOMONNAIES ASIATIQUES VICTIMES DE VOLS

OCT.
SALT TYPHOON INQUIÈTE TOUJOURS PLUS

NOV.
DE FAUX RECRUTEURS IRANIENS CIBLENT DES SECTEURS SENSIBLES

DÉC.
LE DÉPARTEMENT DU TRÉSOR AMÉRICAIN PIRATÉ PAR UN SOUS-TRAITANT

JUIL.

10 MILLIARDS DE MOTS DE PASSE DIVULGUÉS

VULNÉRABILITÉ : Fuite de mots de passe

IMPACT : Attaques par bourrage d'identifiants (credential stuffing) et par force brute

La découverte de RockYou2024 : la plus grande fuite de mots de passe de l'histoire, contenant le nombre vertigineux de 9 948 575 739 mots de passe différents en clair. Cet imposant fichier, publié sur un forum de piratage bien connu, suscite de vives inquiétudes car il contient des mots de passe accumulés au cours des deux dernières décennies. Cela pourrait exposer de nombreux utilisateurs à des attaques par bourrage d'identifiants ainsi qu'à d'autres menaces de sécurité.

SEPT.

LES PLATEFORMES D'ÉCHANGE DE CRYPTOMONNAIES ASIATIQUES VICTIMES DE VOLS

VULNÉRABILITÉ : Violation du réseau

IMPACT : Plus de 70 millions de dollars américains de préjudice

Des attaques sur deux plateformes d'échange de cryptomonnaies, BingX basée à Singapour et Indodax basée en Indonésie, ont essuyé d'importantes pertes suite à des violations bien distinctes. Indodax, basée à Jakarta, a promis d'indemniser ses utilisateurs après une perte de 22 millions de dollars, tandis que BingX a déclaré une perte de 44 millions de dollars. Aux États-Unis, le département de la Justice a également annoncé l'arrestation de deux personnes impliquées dans le vol de 230 millions de dollars en cryptomonnaie d'un citoyen américain.

VIOLATION D'INTERNET ARCHIVE

VULNÉRABILITÉ : Inconnue

IMPACT : Informations sur 31 millions de comptes uniques exposés

Internet Archive, l'organisme américain à but non lucratif consacré à l'archivage du web, a subi plusieurs violations sur une période de 22 jours. Aux alentours du 28 septembre dernier, un hacker a réussi à s'emparer du fichier de base de données de la Wayback Machine d'Internet Archive, compromettant les noms d'utilisateur, les adresses e-mail et les mots de passe chiffrés. Bien que le fondateur du site ait déclaré avoir depuis nettoyé ses systèmes et amélioré ses défenses de sécurité, de multiples attaques par déni de service ainsi qu'une deuxième vague de violations se sont de nouveau produites en octobre.

OCT.

SALT TYPHOON INQUIÈTE TOUJOURS PLUS

VULNÉRABILITÉ : Cyberespionnage des réseaux de télécommunications américains

IMPACT : Des cybercriminels chinois obtiennent un vaste accès aux communications américaines

Salt Typhoon, un groupe de cybercriminels probablement affilié à la Chine, a pu accéder à des informations hautement sensibles sur des citoyens et des fonctionnaires américains en compromettant les principaux fournisseurs américains de services de télécommunications et d'Internet, parmi lesquels Verizon et AT&T. Pas moins de neuf fournisseurs différents auraient été touchés, permettant notamment au groupe d'accéder à l'infrastructure d'écoute électronique autorisée par les tribunaux chez certains fournisseurs. Cet épisode a été qualifié d'« échec cuisant du contre-espionnage américain ».

NOV.

DE FAUX RECRUTEURS IRANIENS CIBLENT DES SECTEURS SENSIBLES

VULNÉRABILITÉ : Ingénierie sociale, utilisation abusive de LinkedIn

IMPACT : Les secteurs de l'aérospatiale, de l'aéronautique et de la défense, particulièrement en Israël et aux Émirats arabes unis. La Turquie, l'Inde et l'Albanie ont également été ciblées.

Des pirates présumés iraniens ont utilisé de faux sites de recrutement pour publier des offres d'emploi sur LinkedIn, ciblant ainsi les entreprises des secteurs de l'aérospatiale, de la défense et de l'aéronautique en Israël, aux Émirats arabes unis, en Turquie, en Inde et en Albanie. En se faisant passer pour des recruteurs sur LinkedIn, les cybercriminels ont semé des malwares sur les appareils de leurs victimes par le biais de fausses offres d'emploi rémunératrices. Leur but ? Espionner des cibles potentielles et commencer à voler des données sensibles dès 2023. Les malwares et les tactiques employés sont similaires à ceux d'un groupe de pirates nord-coréens qui avait ciblé des fonds de cryptomonnaies cotés en bourse.

DÉC.

LE DÉPARTEMENT DU TRÉSOR AMÉRICAIN PIRATÉ PAR UN SOUS-TRAITANT

VULNÉRABILITÉ : Prestataire externe, rôle essentiel des logiciels de sécurité

IMPACT : Les pirates ont pu accéder à des données non classifiées sur certains postes de travail

Le département du Trésor des États-Unis a annoncé qu'une violation de leur fournisseur de sécurité d'identité BeyondTrust s'était répercutée sur ses propres systèmes, entraînant ainsi l'exposition de plusieurs postes de travail et de données non classifiées. Alors que l'enquête est toujours en cours, les États-Unis ont accusé un groupe de pirates affilié à la Chine d'avoir accédé à une clé d'API utilisée pour l'assistance à distance. BeyondTrust n'a pas encore précisé comment les cybercriminels ont pu se procurer ladite clé.

UNE ATTAQUE DE PHISHING CIBLANT DES DÉVELOPPEURS PERMET LA COMPROMISSION D'UNE EXTENSION DE CHROME

VULNÉRABILITÉ : Une attaque de spear phishing entraînant des autorisations élevées sur les extensions du navigateur Chrome de Google

IMPACT : Des extensions malveillantes collectent des identifiants et des informations d'utilisateurs finaux

Au cours de l'année 2024, des groupes cybercriminels sont parvenus à compromettre plus de 30 extensions de navigateur en envoyant des e-mails de spear phishing semblant provenir de Google et ciblant des extensions du navigateur Chrome. En cliquant sur l'e-mail frauduleux, les développeurs étaient invités à accorder des privilèges à une application apparemment anodine, alors qu'en réalité ils permettaient aux attaquants de remplacer leur extension par du code malveillant. Cyberhaven, un éditeur de logiciels de sécurité des données, a signalé cette tactique pour la première fois en décembre, après qu'un de ses développeurs ait été victime de l'attaque et ait accordé des autorisations à l'application « Privacy Policy Extension ». On estime que pas moins de 2,6 millions d'utilisateurs pourraient avoir été touchés par cette attaque.

RECOMMAN-DATIONS

05

CONTRE-MESURES SPÉCIFIQUES

BONNES PRATIQUES ET CONSEILS

RECOMMANDATIONS POUR LES CLIENTS DE MIMECAST

CORBEAUX

ESPÈCE :

Reconnus pour leurs capacités à résoudre des problèmes ainsi que pour leurs aptitudes pédagogiques, ils sont toujours en train d'éduquer et d'**agir**. Votre référence en matière de stratégies d'atténuation des risques liés à la cybersécurité.

CONTRE-MESURES SPÉCIFIQUES AUX MENACES

05.1

Les entreprises devraient prendre des mesures spécifiques pour améliorer leurs défenses et ainsi augmenter les coûts opérationnels pour les cybercriminels.

GESTION DES RISQUES HUMAINS

Les entreprises doivent mettre en œuvre une politique de gestion des risques humains permettant d'aligner leurs objectifs de sécurité avec leurs objectifs métier. En cartographiant les facteurs de risque humain et les dommages potentiels, les entreprises peuvent développer un système de réponse multi-niveaux permettant de distinguer les erreurs involontaires des actions malveillantes. Parmi les principales préoccupations, notons la perte de propriété intellectuelle ou d'autres informations concurrentielles, l'exfiltration de données sensibles et l'utilisation abusive des ressources de l'entreprise.

Les entreprises devraient progressivement mettre en œuvre à la fois des mesures d'incitations à la vigilance et des mesures de remédiation correctives. Pour appliquer de telles mesures, les entreprises doivent constituer des groupes de travail pluridisciplinaires pour garantir l'adhésion des parties prenantes et une gestion efficace du changement, tout en maintenant des canaux de communication clairs avec la direction concernant les indicateurs de risque, les incidents potentiels et les stratégies d'atténuation.

SENSIBILISER LE PERSONNEL AUX RISQUES CYBER VIA UN PROGRAMME DE FORMATIONS ADÉQUATES

Dans le contexte actuel où les tensions géopolitiques se manifestent volontiers sous forme de cybermenaces, une formation complète de sensibilisation des collaborateurs aux risques cyber devient indispensable. Les salariés doivent être informés non seulement des cyber risques généraux, mais également de la manière dont les événements mondiaux peuvent influencer les campagnes de phishing, les menaces internes et les tentatives d'ingénierie sociale visant leur entreprise. En mettant en œuvre des programmes de formation et de sensibilisation adéquats ainsi que des plateformes de gestion des risques humains pour encadrer les utilisateurs, les entreprises parviennent à renforcer leur « pare-feu humain » contre les cyberattaques conventionnelles et celles motivées par des raisons géopolitiques. Cette approche de la sécurité centrée sur l'humain permet aux équipes de sécurité d'identifier et de répondre efficacement aux cyber menaces, qu'elles soient véhiculées par des e-mails, des réseaux sociaux, des outils collaboratifs ou d'autres procédés exploitant la psychologie humaine.

EXIGER DAVANTAGE DE SÉCURITÉ DE LA PART DES PRESTATAIRES EXTERNES

Les attaques perpétrées contre des entreprises des secteurs de la fabrication, du transport, de la logistique, ainsi que du commerce de détail et de gros, représentent un risque important de compromission de la chaîne d'approvisionnement pour les sous-traitants. Les entreprises devraient revoir leurs accords de niveau de service pour fixer des niveaux minimaux de sécurité des données et de cybersécurité et trouver ainsi les moyens de surveiller leurs fournisseurs de plus près : elles pourraient par exemple, utiliser des services de notation externes et soumettre les contrats à un examen préalable plus minutieux.

BLOQUER LES IMAGES CONTENUES DANS LE CORPS DES E-MAILS

Les cybercriminels utilisent de plus en plus de fichiers sous forme d'images pour introduire des leurres de phishing et des codes malveillants, tout en échappant à toute détection. L'étude menée par Mimecast a permis d'identifier des pirates utilisant également du chiffrement ou du texte en langue étrangère inséré dans des images afin de brouiller les pistes. Les entreprises doivent absolument configurer les clients de messagerie pour empêcher le chargement d'images dans les messages et isoler toutes les images que les utilisateurs signalent explicitement. Remarque : les utilisateurs de CyberGraph doivent faire appel à des sites de confiance pour s'assurer que les bannières se chargent correctement.

SCRUTER L'INFRASTRUCTURE D'ENTREPRISE POUR DÉTECTER LES ERREURS DE CONFIGURATION OU LES PORTS RÉSEAUX EXTERNES NON SÉCURISÉS

Les entreprises devraient passer en revue régulièrement leur infrastructure à la recherche d'itinéraires exploitables connus, tels que des ports réseau externes ouverts et non sécurisés ou bien des environnements de cloud public. Grâce à des outils tels que Cloud Security Posture Management, elles pourraient identifier rapidement les erreurs de configuration dans leur cloud public afin de s'assurer que tous les ports serveur publiquement accessibles sont bien fermés ou correctement sécurisés et protégés.

A titre d'exemple, Mimecast a observé une augmentation constante des attaques contre les ports du protocole RDP, attaques représentant 80 % des compromissions effectuées par ransomware. Nul doute qu'à l'avenir, les cybercriminels continueront à chercher des ports RDP ouverts pour infiltrer les réseaux d'entreprises.

SEGMENTER LE RÉSEAU D'ENTREPRISE ET ENREGISTRER LE TRAFIC INTERNE

Lors d'une attaque par ransomware, il n'est pas rare que les cybercriminels se déplacent latéralement au sein d'un réseau d'entreprise. La segmentation du réseau interne et le confinement d'actifs critiques dans leurs propres enclaves permet de réduire considérablement la portée des cyberattaques par ransomware ou autre. La surveillance du trafic interne, en particulier des communications vers des segments réseaux spécifiques, peut permettre une détection plus précoce des cybermenaces.

RENFORCER LES IDENTIFIANTS DES UTILISATEURS, DÉPLOYER L'AUTHENTIFICATION MULTI-FACTEURS

De nombreux malwares utilisent les mots de passe courants pour s'infiltrer dans les réseaux ciblés. Les récentes attaques montrent à quel point les mots de passe simples contribuent aux violations de données. Renforcer n'importe quel réseau commence par appliquer des mots de passe complexes, en particulier pour les comptes utilisateurs privilégiés.
La sécurité informatique doit impérativement changer les mots de passe administrateur par défaut. Exiger une authentification multi-facteurs peut réduire considérablement la compromission des comptes ou le vol d'identifiants.

05.2

BONNES PRATIQUES ET CONSEILS

AVIS APT40 : TECHNIQUES DÉPLOYÉES PAR LE MINISTÈRE DE LA SÉCURITÉ D'ÉTAT (MSS) DE LA RÉPUBLIQUE POPULAIRE DE CHINE

8 juil. 2024 EN SAVOIR PLUS >

Organisations : ASD, CISA, FBI, NSA, CCCS, NCSC-NZ, NCSC-UK, BND et autres

Les agences gouvernementales responsables de la cybersécurité et de l'application de la loi en Australie, au Canada, en Nouvelle-Zélande, en Allemagne, en Corée du Sud, au Royaume-Uni et aux États-Unis ont décrit les tactiques utilisées par APT40, le groupe cybercriminel affilié au ministère chinois de la sécurité d'état (également connu sous le nom de Gingham Typhoon), qui « a ciblé à plusieurs reprises les réseaux australiens, y compris les réseaux gouvernementaux et privés dans la région ». Le groupe est capable de rapidement utiliser, adapter et exploiter le code de preuve de concept pour de nouvelles vulnérabilités afin de mener des cyberattaques et déployer ces outils via des campagnes ciblées.

DÉTECTION ET ATTÉNUATION DES COMPROMISSIONS D'ACTIVE DIRECTORY

sept. 2024 EN SAVOIR PLUS >

Organisations : ASD, CISA, FBI, NSA, CCCS, NCSC-NZ, NCSC-UK

Les agences de cybersécurité des pays membres de l'alliance « Five Eyes » (Australie, Canada, Nouvelle-Zélande, Royaume-Uni et États-Unis) ont répertorié pas moins de 17 techniques différentes pour attaquer Microsoft Active Directory, la solution de gestion des identités et des accès la plus fréquemment utilisée dans les entreprises. Grâce à son rôle central dans les opérations d'authentification et d'autorisation et grâce aussi à sa vulnérabilité en raison de son installation complexe et de ses paramètres par défaut, Active Directory est souvent une cible privilégiée pour les cybercriminels.

LES MILITAIRES RUSSES CIBLENT INDIRECTEMENT LES INFRASTRUCTURES CRITIQUES DES ÉTATS-UNIS ET DU MONDE ENTIER

5 sept. 2024 EN SAVOIR PLUS >

Organisations : les agences gouvernementales américaines CISA, FBI, NSA

Plusieurs groupes de menaces affiliés à des instances militaires russes ont ciblé les agences gouvernementales ukrainiennes et d'autres cibles alliées de l'OTAN à l'aide du malware destructeur WhisperGate. Lors de cette attaque, les cybercriminels ont exploité des vulnérabilités dans différents appareils connectés pour infiltrer les réseaux ennemis.

PRINCIPALES VULNÉRABILITÉS RÉGULIÈREMENT EXPLOITÉES EN 2023

12 nov. 2024 EN SAVOIR PLUS >

Organisations : ASD, CISA, FBI, NSA, CCCS, NCSC-NZ, NCSC-UK

Les principales agences des pays membres de l'alliance Five Eyes ont publié, sans doute trop tard, des informations sur les 15 vulnérabilités les plus fréquemment exploitées en 2023. 11 d'entre elles ont été exploitées dans des attaques de type zero-day, contre seulement 2 problèmes de type zero-day sur la dizaine de vulnérabilités répertoriées en 2022.

RENFORCER LA CYBER RÉSILIENCE : ENSEIGNEMENTS TIRÉS DE L'ÉVALUATION PAR LA RED TEAM DE LA CISA D'UNE INFRASTRUCTURE CRITIQUE AUX ÉTATS-UNIS

21 nov. 2024 EN SAVOIR PLUS >

Organisations : CISA

L'Agence gouvernementale américaine de cybersécurité et de sécurité des infrastructures (CISA) a identifié d'importantes failles de sécurité au sein d'une organisation d'infrastructure critique lors d'une évaluation par sa Red Team. L'équipe est parvenue à infiltrer l'organisation en utilisant un web shell datant d'une précédente évaluation et à compromettre son domaine et ses systèmes critiques en raison de son réseau insuffisamment protégé et trop lentement défendu.

DES GROUPES CYBERCRIMINELS EN LIEN AVEC L'IRAN CIBLENT LES AUTOMATES PROGRAMMABLES INDUSTRIELS DANS PLUSIEURS SECTEURS, NOTAMMENT LES SYSTÈMES DE TRAITEMENT ET D'ASSAINISSEMENT DES EAUX AUX ÉTATS-UNIS

18 déc. 2024 EN SAVOIR PLUS >

Organisations : FBI, CISA, NSA, US EPA, INCD, CCCS, NCSC

Les agences de cybersécurité des États-Unis, d'Israël, du Canada et du Royaume-Uni ont récemment mis à jour un bulletin décrivant des cyber activités menées par des hackers iraniens liés au CGRI (Corps des Gardiens de la Révolution Islamique). Outre les infrastructures américaines, ces groupes ont proliféré des attaques à l'encontre d'automates programmables et d'infrastructures critiques au Royaume-Uni et en Israël.

RECOMMANDATIONS POUR LES CLIENTS DE MIMECAST

Nous conseillons aux utilisateurs des solutions Mimecast de suivre les recommandations suivantes afin de protéger leurs utilisateurs des menaces détaillées dans ce rapport :

PASSERELLE DE MESSAGERIE SÉCURISÉE CLOUD

1. Nous recommandons 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 la messagerie comme vecteur d'attaque.
2. 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 réglée sur Ignorer/Gérer et Expéditeurs autorisés permet de contourner efficacement tout e-mail légitime rejeté/mis en quarantaine en raison d'échecs DMARC.
3. Renforcez la protection contre l'usurpation d'identité conformément aux meilleures pratiques, à savoir 2 occurrences définies comme sujet/corps, et définissez une politique distincte pour les cadres dirigeants sur la base de la correspondance des noms devant être approuvée par un administrateur. Par ailleurs, créez une autre politique pour toutes les détections de 3 occurrences ou plus avec l'approbation d'un administrateur.
4. Mettez en œuvre une protection avancée contre les BEC avec trois politiques : application modérée pour la détection des menaces, contournement de l'expéditeur pour les sources fiables et contournement du destinataire pour les exclusions internes.
5. La mise en place d'une procédure de réécriture systématique des URL garantira que toutes les URL seront analysées au moment du clic, sans oublier que tout ce qui s'apparentera à une URL sera réécrit, y compris les adresses IP et les liens internes.
6. Utilisez les intégrations prédéfinies avec la majorité des fournisseurs de solutions SIEM et XDR pour assurer l'enregistrement et l'analyse des journaux afin de se conformer aux politiques de sécurité en vigueur.
7. Exploitez vos propres informations sur les menaces pour rejeter automatiquement tout flux externe présentant les mêmes caractéristiques que d'autres flux de menaces préalablement identifiés.
8. Les utilisateurs finaux doivent signaler à notre SOC, tout message potentiellement malveillant, via les outils de Mimecast, pour une analyse plus approfondie.

SÉCURITÉ DE LA MESSAGERIE INTÉGRÉE DANS LE CLOUD

1. Activez l'isolation du navigateur pour minimiser le risque que les utilisateurs accèdent à des sites potentiellement suspects.
2. Personnalisez vos règles d'autorisation et de blocage pour déterminer précisément quels utilisateurs sont autorisés à accéder à votre environnement.
3. Consultez les rapports hebdomadaires pour obtenir des informations sur les menaces détectées dans votre environnement.
4. Les utilisateurs finaux doivent signaler à notre SOC, tout message potentiellement malveillant, via les outils de Mimecast, pour une analyse plus approfondie.

Pour toute précision supplémentaire concernant l'une des recommandations énumérées ci-dessus, veuillez contacter votre partenaire Mimecast ou directement notre service d'assistance.

CONCLUSION

Au cours du second semestre 2024, l'analyse des menaces cyber a révélé une intensification des campagnes de désinformation sophistiquées et des opérations de piratage coordonnées, coïncidant avec un regain des tensions géopolitiques mondiales. Cela a permis aux groupes cybercriminels d'utiliser les événements mondiaux comme prétexte pour lancer des cyberattaques ciblées. Parmi ces tactiques toujours plus évoluées, notons l'exfiltration systématique de données, le déploiement ciblé de ransomwares et les attaques DDoS orchestrées. Tout en exploitant les vulnérabilités humaines par le biais de campagnes d'ingénierie sociale sophistiquées et inspirées par les changements géopolitiques majeurs, cette nouvelle génération de cyberattaques présente des risques importants pour la disponibilité des systèmes et le maintien de l'activité économique des entreprises. L'identification des activités malveillantes est devenue techniquement complexe, car les pirates prennent soin d'alterner actions malveillantes et opérations légitimes utilisant des services de confiance et des systèmes réputés comme fiables. Les cybercriminels s'appuient de plus en plus sur des outils légitimes de la Red Team, rendant encore plus complexes les contrôles de sécurité devant faire la distinction entre activités autorisées et non autorisées. Cela nécessite des capacités de surveillance sans cesse améliorées, y compris des systèmes avancés d'analyse comportementale et de détection des anomalies.

Dans d'autres domaines du champ des menaces, les attaques par ingénierie sociale maintiennent des taux de réussite élevés, notamment grâce à l'intégration de technologies pilotées par l'IA. Les menaces persistantes avancées utilisent désormais des technologies sophistiquées de Deepfake et des contenus générés par l'IA pour lancer des attaques ciblées, compliquant considérablement la tâche des mécanismes traditionnels de détection et de prévention. Cette course à la technologie des récentes cyberattaques témoigne des recherches approfondies menées par les cybercriminels dans les domaines de l'ingénierie sociale et des modes de communication de la chaîne d'approvisionnement.

La défense du périmètre de sécurité de l'entreprise demeure une préoccupation essentielle. En effet, les cybercriminels exploitent régulièrement les vulnérabilités de l'infrastructure périphérique, y compris les appareils VPN, les pares-feux et les services web. L'exploitation des failles de type zero-day combinée à une mise en œuvre tardive des correctifs crée des fenêtres de vulnérabilité prolongées, notamment dans les environnements à haute disponibilité nécessitant des tests de correctifs approfondis. Ce défi est amplifié par la complexité des architectures réseau et l'expansion de la surface d'attaque due à la migration vers l'infrastructure cloud et à l'évolution des technologies opérationnelles. Les entreprises ont besoin de capacités dédiées de réponse aux incidents, y compris des outils d'investigation avancés, des systèmes d'analyse du réseau et des mécanismes de détection automatisés.

Vulnérabilités susceptibles d'être exploitées cette année :

VPN

Comme le montre l'ajout récent du CVE 2025 0282 Ivanti Connect Secure VPN au catalogue des vulnérabilités exploitables connues de la CISA.

AUTHENTIFICATION

Plus récemment observée dans des vulnérabilités exploitant un contournement via un chemin ou un canal alternatif, et un code d'authentification manquant.

DÉNI DE SERVICE (DOS)

Une activité malveillante de plus en plus fréquente visant à perturber l'activité des entreprises (par exemple, l'attaque par déni de service (DoS) sur le pare-feu PAN OS CVE 2024 3393).

RESSOURCES :

Webinaire :
Traduire les renseignements sur les menaces en stratégies de sécurité pratiques

Rapport de recherche :
État de la sécurité des e-mails et de la collaboration

T I HUB :

Mimecast Threat Intelligence hub

Communauté des utilisateurs Mimecast :

Mimecast Central

mimecast