CONÇU POUR LES ENVIRONNEMENTS Microsoft 365

2024

RAPPORT SUR LA CYBERSÉCURITÉ

UNE ANALYSE APPROFONDIE DU PAYSAGE DES MENACES DE MICROSOFT 365

HORNETSECURITY

HORNETSECURITY

RAPPORT SUR LA CYBERSÉCURITÉ 2024

À propos de Hornetsecurity

Hornetsecurity offre aux entreprises et aux organisations de toutes tailles des solutions leur permettant de se concentrer sur leurs activités essentielles en protégeant non seulement les communications par courriel, mais aussi en sécurisant les données en plus d'assurer la continuité des activités et la conformité aux solutions infonuagiques de prochaine génération.

Notre produit phare, 365 Total Protection, est la solution de sécurité infonuagique la plus complète pour Microsoft 365 sur le marché et comprend la sécurité des courriels, la conformité et la sauvegarde.

Qu'est-ce que le Rapport sur la cybersécurité (Cyber Security Report)?

Le Rapport sur la cybersécurité (anciennement Rapport sur les cybermenaces – Cyber Threat Report) est une analyse annuelle du paysage actuel des cybermenaces fondée sur des données réelles recueillies et étudiées par l'équipe dédiée du Security Lab de Hornetsecurity. Hornetsecurity traite plus de 3,5 milliards de courriels chaque mois. En analysant les menaces identifiées dans ces communications, combinées à une connaissance détaillée du paysage des menaces au sens large, le Security Lab révèle des tendances majeures. Il peut faire des projections éclairées sur l'avenir des menaces de sécurité de Microsoft 365, ce qui permet aux entreprises d'agir en conséquence. Ces constatations et ces données figurent dans ce rapport.

Qu'est-ce que le Security Lab?

Le Security Lab est une division de Hornetsecurity spécialisée dans la sécurité des courriels qui effectue des analyses forensiques des menaces de sécurité les plus actuelles et les plus critiques. L'équipe multinationale de spécialistes de la sécurité possède une vaste expérience en recherche sur la sécurité ainsi qu'en génie logiciel et en sciences des données.

Pour élaborer des contre-mesures efficaces, il est essentiel de comprendre en profondeur le paysage des menaces établi par l'examen pratique des virus du monde réel, des attaques de phishing, des logiciels malveillants (aussi appelés maliciels) et plus encore. Les renseignements détaillés mis à jour par le Security Lab servent de fondement aux solutions de cybersécurité de prochaine génération de Hornetsecurity.

Comment utiliser le présent rapport

Ce rapport est divisé en cinq sections :

Le Chapitre 1 contient le résumé. Consultez cette section si vous n'êtes intéressé(e) que par les points saillants.

Le Chapitre 2 se concentre sur le paysage actuel des menaces de la plateforme Microsoft 365.

Le Chapitre 3 traite des préoccupations actuelles et des discussions concernant les menaces et les tendances les plus importantes à partir de 2023.

Le Chapitre 4 contient les prévisions du Security Lab sur les menaces à la cybersécurité en 2024, ainsi que des conseils et des lignes directrices pour vous aider à protéger votre entreprise.

Le Chapitre 5 répertorie toutes les références, les liens connexes et les ensembles de données utilisés dans le présent rapport.

Table des matières

Chapitre 1 – Résumé

Grâce à sa vaste base de données utilisateurs, l'entreprise Hornetsecurity est particulièrement bien placée pour passer au crible les menaces par courriel et en tirer des conclusions importantes pour les professionnels de la sécurité des technologies de l'information (TI). Le courriel reste un canal de communication essentiel. Cependant, selon notre analyse portant sur plus de 45 milliards de courriels, 36,4 % sont considérés comme « indésirables ». 96,4 % des courriels indésirables sont des pourriels ou rejetés purement et simplement suivant des indicateurs externes, et un peu plus de 3,6 % ont été signalés comme malveillants.

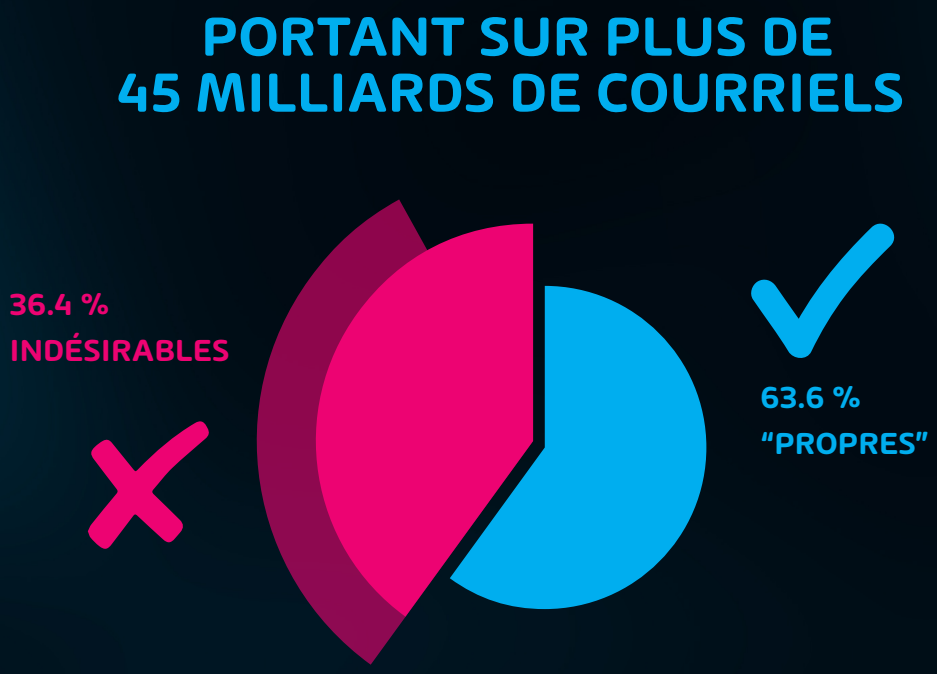


Tableau 1 : Classification des courriels analysés par Hornetsecurity

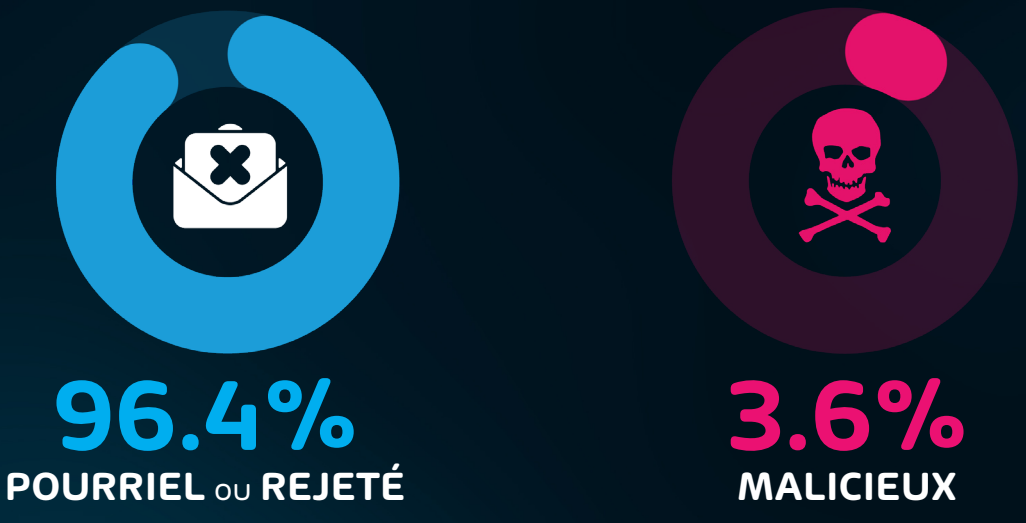


Tableau 2 : Classification des courriels indésirables

Le type d'attaque figure parmi les autres statistiques générales sur les attaques par courriel que nous examinons. Nos conclusions pour cette période de référence montrent que l'hameçonnage occupe toujours la première place, représentant 43,3 % des attaques par courriel. Cela représente une augmentation de près de 4 % par rapport à l'année précédente. Le deuxième type d'attaque le plus courant en 2023 était l'utilisation d'URL malveillantes dans les courriels (30,5 %), soit une augmentation significative de 18 % comparée au rapport de l'année dernière.

43,3 % DES ATTAQUES PAR COURRIEL

Tableau 3 : Attaques par courrier électronique

Parallèlement aux types d'attaques, nous surveillons les types de pièces jointes qui sont actuellement utilisées par les pirates pour diffuser des charges utiles malveillantes. Les fichiers HTML (37,1 %) et PDF (23,3 %) ont été observés le plus fréquemment au cours de la période de référence, les fichiers Archive (20,8 %) arrivant en troisième position. L'utilisation des fichiers HTML a connu une augmentation de 16,1 % par pirates tout au long de la période de référence, ainsi qu'une augmentation de 11 % de l'utilisation des fichiers PDF. Cette évolution est due en grande partie à des menaces, telles que Qakbot et des réseaux de zombies similaires (aussi appelés botnets) qui utilisent ces types de fichiers pour faciliter la diffusion de leurs logiciels. Il convient également de

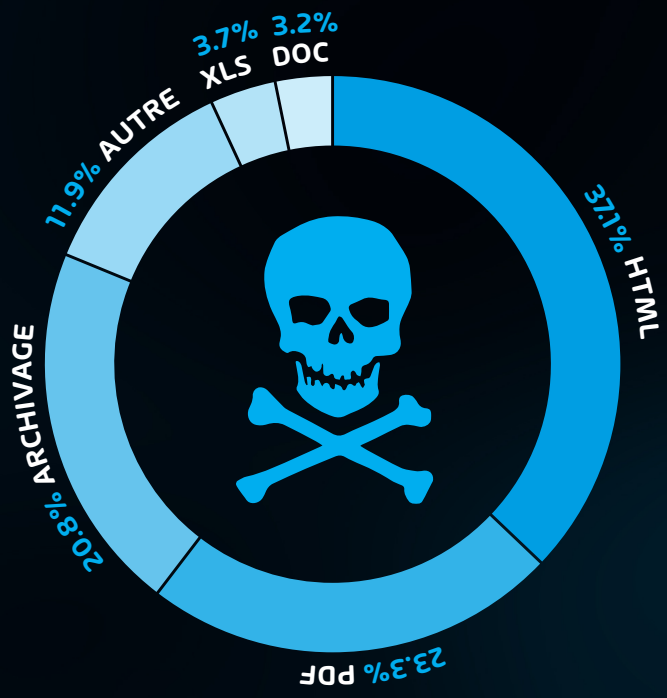


Tableau 4 : Types de fichiers les plus utilisés dans les courriels malveillants

noter une diminution notable de l'utilisation des fichiers DOCX (9,5 %) et des fichiers XLSX (6,7 %). Ces types de fichiers étaient autrefois très utilisés par les pirates. Depuis que Microsoft a désactivé les macros par défaut dans Office, l'utilisation de ces types de fichiers a chuté de façon spectaculaire.

L'indice de menace par courriel de l'industrie était à peu près le même dans la plupart des secteurs verticaux au cours de la période de référence. L'indice de menace par courriel est un indicateur que nous suivons et qui mesure le nombre de tentatives de menaces par courriel par rapport au nombre de courriels sans risque envoyés, en fonction du secteur vertical. Il donne une bonne idée des types d'entreprises qui sont actuellement ciblées par les pirates. Tout comme l'année dernière, nos données montrent que presque tous les types d'entreprises sont actuellement menacés. En bref, si votre organisation a la capacité de payer une rançon, vous êtes une cible. Cela dit, les organisations de recherche, le secteur du divertissement et le secteur manufacturier se situent au sommet du spectre, et ces types d'organisations font l'objet d'un peu plus d'attaques que d'autres.

Un dernier aspect de la sécurité des courriels que nous suivons est l'utilisation d'usurpations d'identité. Cela nous permet d'informer nos équipes de produits, nos clients et la communauté sur les types d'hameçonnage axés sur la marque qui sont actuellement utilisés dans l'écosystème. Les données recueillies dans le cadre de ce rapport montrent que les marques d'expédition restent un choix populaire. Par exemple, DHL (26,1 %), Amazon (7,7 %) et FedEx (2,3 %) figurent toutes parmi les 10 premières. Les autres noms importants figurant dans la liste sont Microsoft (2,4 %), LinkedIn (2,4 %) et Netflix (2,2 %). Dans la plupart des cas, les pirates recherchaient les identifiants des utilisateurs finaux, soit pour les vendre, soit pour les utiliser dans d'autres attaques.

26.1%	DHL
7.7%	AMAZON
2.4	LINKEDIN
2.4	MICROSOFT
2.2	NETFLIX
2.3	FEDEX

Tableau 5 : Marques ou organisations exploitées

La question de la sécurité des données dans l'écosystème infonuagique de Microsoft Cloud continue d'occuper une place importante dans les discussions sur le nuage aujourd'hui. Plusieurs récentes atteintes à la sécurité, dont une imputable à des pirates appartenant à l'État-nation chinois, ont amené de nombreuses entités (y compris le gouvernement américain) à réévaluer leur posture de sécurité à l'ère du nuage. Cette nouvelle donne a également soulevé la question de la dépendance excessive à l'égard des fournisseurs et du degré de confiance que les organisations devraient accorder à un fournisseur exclusif.

Microsoft a également modifié sa position de longue date sur la nécessité de sauvegarder les données M365. Pendant une longue période, leur position était simple : « les sauvegardes ne sont pas nécessaires », le fournisseur de services d'informatique en nuage s'appuyant uniquement sur les capacités de conservation intégrées à M365. Cependant, Microsoft semble avoir abandonné cette posture en annonçant soudainement l'arrivée d'une nouvelle application de sauvegarde M365 et une API connexe au cours de l'été. Cela dit, à l'heure où nous écrivons ces lignes, aucune information supplémentaire n'a été communiquée concernant ce produit de sauvegarde nouvellement annoncé.

La bonne définition des autorisations de partage et d'objet dans M365 est un sujet que nous abordons également dans ce rapport. Avec la facilité de partage et de collaboration qu'offre M365, des données sensibles peuvent s'échapper facilement des locataires M365, par totale inadvertance ou de manière malveillante. SharePoint Online et OneDrive Entreprise ont été les « serveurs de fichiers » de l'ère du nuage pendant un certain temps maintenant, de sorte que de nombreuses organisations sont confrontées à la dure réalité d'essayer de gérer le partage et les autorisations dans M365 APRÈS qu'ils soient devenus incontrôlables. Ce sera toujours un problème sur lequel les entreprises devront se pencher en 2024 et il est probable que cette solution devienne une source de fuite de données à l'avenir.

Le courriel reste l'un des principaux canaux utilisés par les pirates pour lancer des attaques. Une solide stratégie de sécurité des courriels est donc essentielle pour naviguer dans le paysage des menaces croissantes et renforcer la résilience en matière de sécurité en 2023.

Chapitre 2 – Le paysage actuel des menaces de Microsoft 365

Chaque année, le Security Lab de Hornetsecurity examine la base de données complète de l'entreprise et analyse l'état des menaces par courriel ainsi que des statistiques des communications à l'échelle mondiale. En outre, l'équipe mène régulièrement des exercices de réflexion prospective et fournit des renseignements sur les menaces potentielles. Le présent chapitre porte sur l'examen des données du 1er novembre 2022 au 1er novembre 2023, qui constituent la base des projections du paysage changeant des menaces décrites au Chapitre 4.

Tendances en matière de sécurité des courriels

Malgré l'utilisation croissante de logiciels de collaboration et de messagerie instantanée, tels que Microsoft Teams, le courriel reste un sujet de préoccupation majeure en ce qui concerne les cyberattaques. Bien que nous ayons constaté une légère diminution du nombre de courriels classés dans la catégorie Menaces simples/menaces sophistiquées – 3,6 % cette année, contre 5,48 % l'année dernière (en ce qui concerne les courriels « non désirés »), le risque pour les entreprises du monde entier reste élevé. Les attaques sont de plus en plus sophistiquées et, avec l'augmentation des attaques basées sur l'intelligence artificielle (IA), les entreprises doivent rester vigilantes et ne pas se reposer sur leurs lauriers en matière de sécurité. Des données plus détaillées sont présentées ci-dessous.

En examinant plus de 45 milliards de courriels recueillis pendant la période de référence en cours (du 1ernovembre 2022 au 1er novembre 2023), le Security Lab a fait les constatations suivantes :

Pourriels, logiciels malveillants, mesures concernant les menaces sophistiquées

Le courriel reste l'un des principaux canaux utilisés par les pirates pour lancer des attaques. C'est ce que montrent nos données, qui classent 36,4 % des courriels comme « indésirables », ce qui signifie qu'il ne s'agit pas de communications authentiques souhaitées par le destinataire. Le graphique ci-dessous montre la répartition des courriels indésirables et des courriels sans risque.

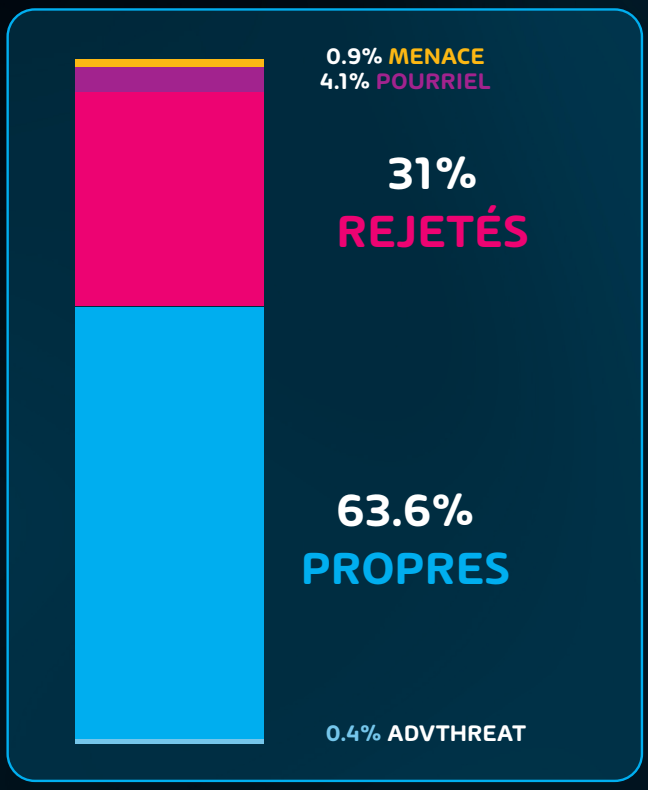


Tableau 6 : Courriels indésirables et des courriels sans risque

Ces données contrastent avec celles de l'année dernière, où 40,5 % de tous les courriels étaient classés comme « indésirables », ce qui montre une diminution (bien que légère) du nombre de courriels indésirables d'une année à l'autre en pourcentage. Si nous considérons que nous n'avons traité que 25 milliards de courriels pour le rapport de l'année dernière, contre 45 milliards cette année, la menace actuelle que représentent les menaces par courriel reste ÉLEVÉE.

Au cours de la période de référence de cette année, nous avons constaté que les courriels **indésirables** se répartissaient comme suit :

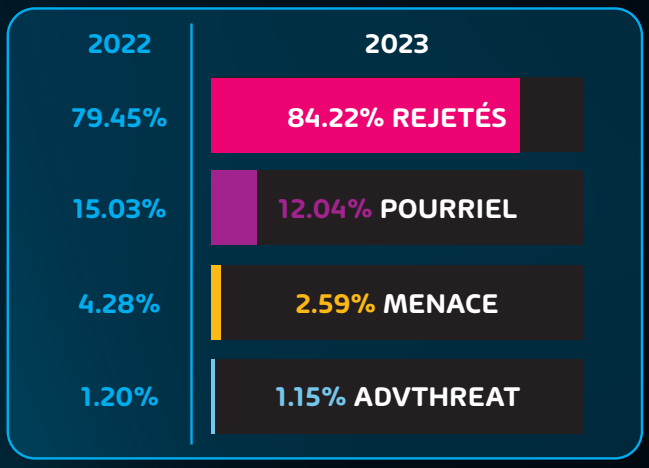


Tableau 7 : Courriels indésirables par catégorie en 2023

CATÉGORIE	DESCRIPTION
Pourriel	Ces courriels sont indésirables et sont souvent promotionnels ou frauduleux. Les courriels sont envoyés simultanément à un grand nombre de destinataires.
Menace	Ces courriels ont du contenu nuisible, comme des pièces jointes ou des liens malveillants, ou ils sont envoyés pour commettre des actes délictuels comme l'hameçonnage.
AdvThreat	La solution Advanced Threat Protection (protection avancée contre les menaces) a détecté une menace dans ces courriels. Les courriels sont utilisés à des fins illégales et nécessitent des moyens techniques sophistiqués qui ne peuvent être repoussés qu'en utilisant des procédures dynamiques avancées.
Rejeté	Notre serveur de courriel rejette ces courriels directement pendant le dialogue SMTP en raison de caractéristiques externes, comme l'identité de l'expéditeur, et les courriels ne sont pas analysés en profondeur.

REMARQUE : Pour fournir un peu plus de détails, la catégorie « Rejeté » fait référence aux courriels que les services de Hornetsecurity ont rejetés au cours du dialogue SMTP en raison de caractéristiques externes, telles que l'identité ou l'adresse IP de l'expéditeur. Si un expéditeur est déjà identifié comme compromis, le système ne poursuit pas l'analyse. Le serveur SMTP refuse le transfert du courriel dès le point de connexion initial en raison de la réputation négative de l'IP et de l'identité de l'expéditeur.

Techniques d'attaque utilisées dans les attaques par courriel

Notre analyse des courriels de la période de référence nous a permis d'observer la répartition suivante des types d'attaques utilisés dans les attaques par courriel :

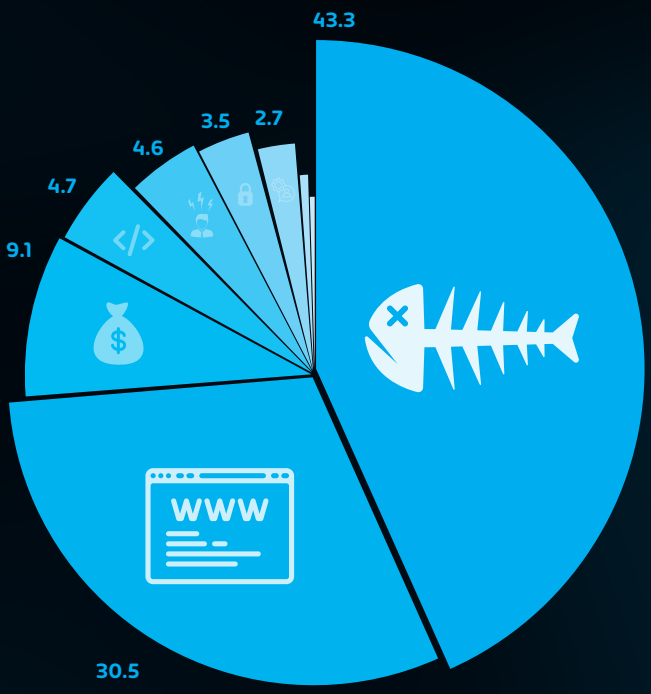


Tableau 8 : Techniques utilisées dans les attaques par courriel 2023

Sans surprise, l'hameçonnage et l'utilisation d'URL malveillantes restent en tête de liste et continuent d'être des types d'attaques populaires (et très efficaces) pour les pirates. L'examen des données de l'année dernière (voir ci-dessous) permet de faire plusieurs comparaisons :

2022 %	2023 %	TECHNIQUES D'ATTAQUE
39.6	43.3	**Hameçonnage**
12.5	30.5	**URL**
8.2	9.1	**Arnaque des avances de frais**
1.8	4.7	**HTML**
3.7	4.6	**Extorsion**
3.5	3.5	**Archives/images disques**
1.1	2.7	**Impersonation**
2.8	1.0	**Maldoc (pièce jointe malveillante)**
0.4	0.6	**PDF**

Tableau 9 : Techniques d'attaque utilisées dans les attaques par courriel 2022 et 2023

L'ingénierie sociale et les menaces par courriel restent l'une des principales méthodes utilisées par les pirates pour prendre pied dans une organisation cible. Nous avons également constaté une augmentation des cas où les utilisateurs cibles sont incités par ingénierie sociale à interagir avec un lien malveillant, de sorte que l'utilisation d'URL malveillantes va de pair avec l'augmentation générale de l'hameçonnage.

Types de pièces jointes et leur utilisation dans les attaques

Les pièces jointes aux courriels demeurent l'une des méthodes les plus fréquemment utilisées pour livrer une charge utile malveillante en 2023. Les pirates continuent d'utiliser des pièces jointes pour cacher des maliciels et donner un air d'authenticité à leurs communications malveillantes. De plus, certains filtres rudimentaires de pourriels/maliciels peuvent être incapables d'analyser les pièces jointes compressées, ce qui accroît le risque dans certaines organisations.

La répartition des types de fichiers utilisés pour la livraison de charges utiles malveillantes au cours de la période de référence est indiquée ci-dessous :

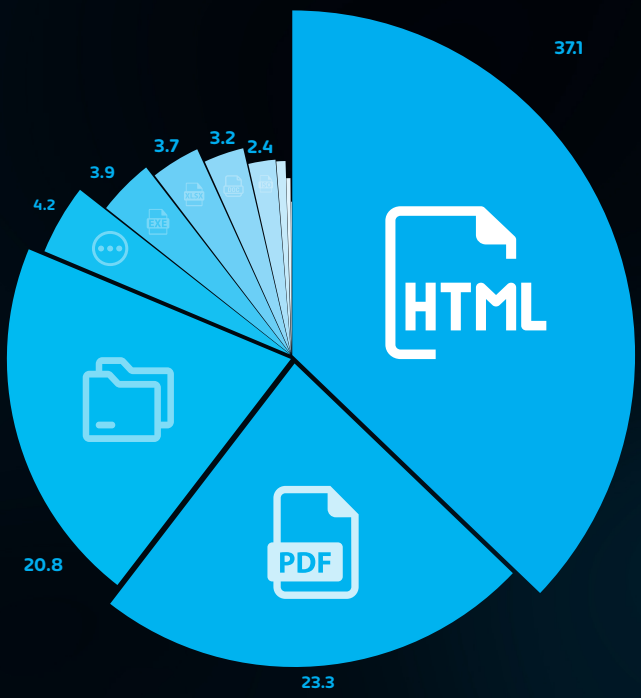
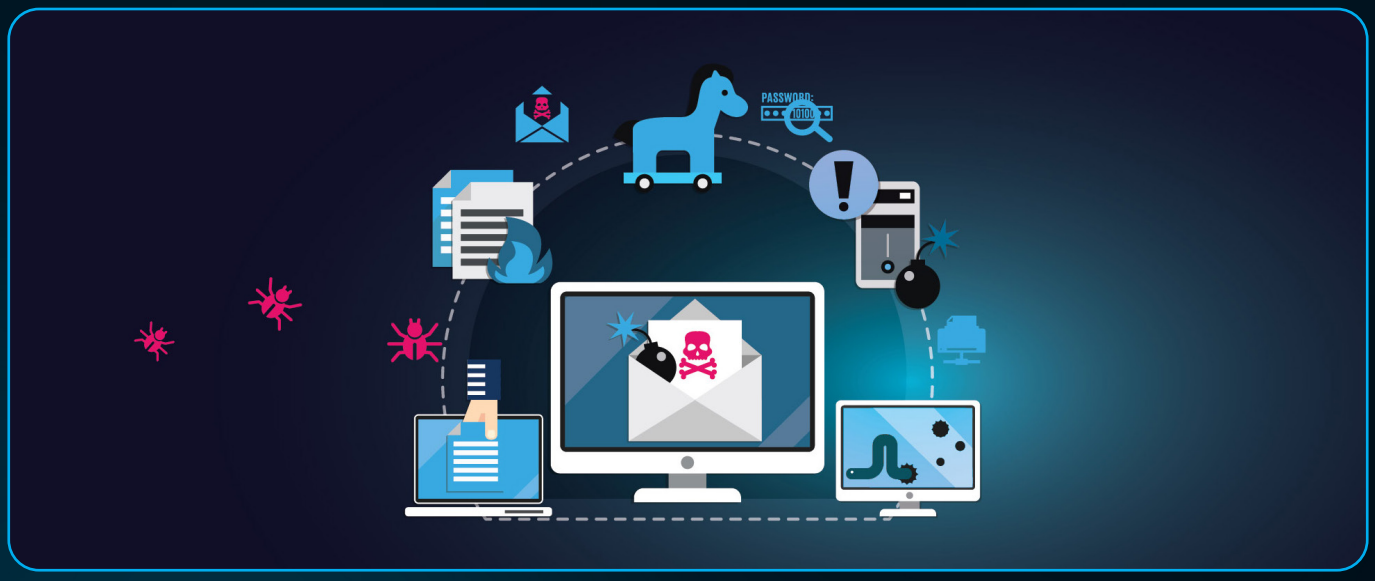


Tableau 9 : Types de fichiers pour les charges utiles malveillantes 2023

Malgré la diminution des fichiers HTML utilisés dans les attaques par courriel dont nous avons parlé précédemment, le HTML est le premier type de fichier joint utilisé par les pirates, le PDF arrivant en deuxième position, suivi des archives en troisième position. Le fait que le langage HTML occupe la première place n'est pas en soi une surprise, car il s'agit d'un type de fichier qui peut être lu et utilisé sur pratiquement toutes les plateformes. Quel que soit le système d'exploitation de l'utilisateur cible, le fichier HTML pourra être ouvert, ce qui augmente les chances de succès du pirate.



Si nous comparons les données ci-dessus avec celles de l'année dernière (voir ci-dessous), un certain nombre de différences ressortent.

	2022	2023	
HTML	21.0	37.1	HTML
PDF	12.4	23.3	PDF
	28.0	20.8	ARCHIVE
	4.8	4.2	OTHER
EXE	4.3	3.9	EXECUTABLE
XLSX	10.4	3.7	EXCEL
DOC	12.7	3.2	WORD
ISO	5.4	2.4	DISK IMAGE FILES
	0.7	0.8	SCRIPT FILE
	0.0	0.4	ONENOTE
	0.1	0.1	EMAIL
LNK	0.1	0.0	LNK FILE
PPTX	<0.1	0.0	POWERPOINT

Tableau 11 : Types de fichiers pour les charges utiles malveillantes 2022 et 2023

Au cours de l'année écoulée, les groupes de cybercriminels et l'industrie ont connu une certaine activité qui peut expliquer ces changements. En ce qui concerne l'augmentation des fichiers HTML et PDF, nous pouvons l'attribuer en partie à Qakbot. Malgré l'interruption de Qakbot par les autorités mondiales au cours de l'été 2023, Qakbot a connu une certaine activité cette année. Qakbot était connu pour utiliser des documents HTML et PDF pour faciliter l'infection des machines cibles. Cela dit, ce mécanisme de déploiement restera populaire pour les futurs exploitants de logiciels malveillants et de réseaux de zombies.

La forte diminution de l'utilisation des fichiers DOCX et XLSX par rapport à l'année dernière peut être attribuée à la nouvelle pratique de Microsoft consistant à bloquer par défaut les macros dans Office. Ces types de fichiers sont donc moins attrayants pour les pirates.

Indice des menaces par courriel pour les secteurs verticaux

L'un des domaines clés que nous examinons chaque année (et chaque mois) est le nombre de menaces qui pèsent sur les différents secteurs verticaux. Cela nous permet de déterminer s'il y a des campagnes données ou des attaques ciblées sur certaines entreprises. Elle fournit également des informations que les entreprises peuvent utiliser pour déterminer si elles sont exposées à un risque accru d'attaque ou non.

L'un des principaux changements observés dans les données de l'année dernière est le fait que l'indice de menace de l'industrie était à peu près le même dans tous les secteurs. Ces données ont permis de conclure que le secteur d'activité n'a pas d'importance. Si votre organisation a la capacité de payer une rançon, vous ÊTES une cible. Nos données pour cette année (ci-dessous) montrent que la tendance se poursuit. L'indice de menace est pratiquement le même pour les dix principaux secteurs verticaux.

Cela dit, certains secteurs ont été un peu plus ciblés que d'autres.

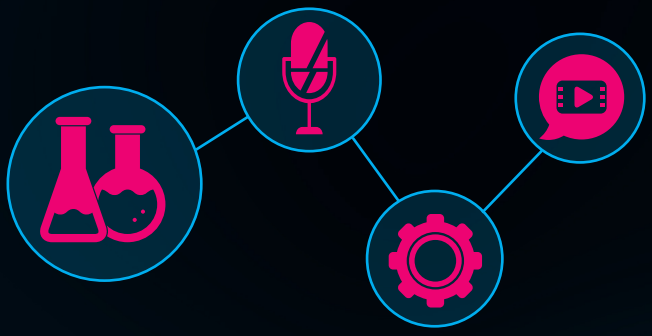
- **Secteur de la recherche** – Nous constatons que les organismes de recherche deviennent des cibles simplement en raison de la propriété intellectuelle qu'ils gèrent généralement.
- **Secteur du divertissement** – Les organisations de ce type relèvent généralement du secteur des jeux d'argent, de la vente de billets, etc. Ces organisations deviennent une cible en raison de l'importance des sommes d'argent en jeu. Comme exemple, nous pouvons mentionner l'attaque de 2023 contre MGM et Caesars Entertainment.
- **Secteur manufacturier** – Le secteur manufacturier est depuis longtemps la cible fréquente des pirates.

Il s'agit généralement de pirates qui s'en prennent à la propriété intellectuelle. Beaucoup considèrent ce secteur comme une cible facile pour les rançongiciels et les interruptions de production en raison de la nature de la sécurité de leur réseau et du fait qu'ils utilisent souvent un grand nombre de dispositifs IdO (Internet des objets) non sécurisés.

Le tableau ci-dessous montre l'indice des menaces pour les principaux secteurs verticaux.

3.0	INDUSTRIE DE LA RECHERCHE
3.0	INDUSTRIE DU DIVERTISSEMENT
3.0	INDUSTRIE DE LA FABRICATION
2.9	INDUSTRIE DES MÉDIAS
2.9	INDUSTRIE DES SOINS DE SANTÉ
2.7	INDUSTRIE DU TRANSPORT
2.6	INDUSTRIE HOSPITALIÈRE
2.6	INDUSTRIE AUTOMOBILE
2.5	UTILITAIRE
2.5	TECHNOLOGIE DE L'INFORMATION
2.5	INDUSTRIE DE L'ÉDUCATION
2.4	INCONNUE
2.4	INDUSTRIE DE LA CONSTRUCTION
2.4	INDUSTRIE MINIÈRE ET MÉTALLURGIQUE
2.4	INDUSTRIE FINANCIÈRE
2.4	INDUSTRIE AGRICOLE
2.3	SERVICES PROFESSIONNELS
2.3	COMMERCE DE DÉTAIL
2.2	INDUSTRIE IMMOBILIÈRE
1.8	INDUSTRIE DE LA LOGISTIQUE
2.4	MOYENNE GLOBALE
99.3	MAXIMUM GLOBALE

Tableau 12 : Indice annuel des menaces pour l'industrie



REMARQUE : La valeur de l'indice de menace est déterminée en utilisant la formule de calcul suivante :

Pourcentage de l'indice de menace = nombre de courriels malveillants (Menace+Menace sophistiquée/(le nombre de courriels malveillants (Menace+Menace sophistiquée) + le nombre de courriels sans risque) multiplié par 100 – Pourriels et courriels d'information non inclus.

Remarque sur la méthodologie

Des organisations (de taille) différentes reçoivent un nombre absolu de courriels différents. Par conséquent, nous calculons le pourcentage de courriels de menace de chaque organisation et de courriels sans risque pour comparer les organisations. Nous calculons ensuite la médiane de ces valeurs en pourcentage pour toutes les organisations d'une même industrie afin d'établir la note de menace finale de l'industrie.

Usurpation d'identité de marque

L'usurpation d'identité de marque demeure une technique d'attaque majeure par courriel ciblant les utilisateurs finaux en 2023.

Les usurpations d'identité de marque au cours de la période de référence continuent de suivre les tendances habituelles. Les entreprises DHL, Amazon et FedEx sont restées parmi les dix premières. Cette tendance est à la hausse et se répète depuis un certain temps. La pandémie de COVID a entraîné une forte augmentation des achats en ligne, et cette pratique est restée dans l'esprit des consommateurs depuis lors. Les pirates le savent, et s'ils parviennent à placer un message d'hameçonnage convaincant lié à l'expédition dans la boîte aux lettres de la cible au bon moment, ils ont de grandes chances de réussir.

Il importe de noter également l'inclusion de Microsoft, LinkedIn et Netflix parmi les dix premières. La présence de Microsoft ici est principalement due aux tentatives d'accès aux identifiants des services infonuagiques de Microsoft Cloud par les attaques populaires actuelles de type « adversaire au milieu » au moyen de trousses d'outils de serveur mandataire inverse (reverse proxy), comme la trousse d'hameçonnage W3II. Ces types d'attaques sont capables de contourner les dispositifs de protection de l'authentification multifactorielle (AMF) et il peut être assez difficile de s'en protéger.

L'usurpation d'identité des marques LinkedIn et Netflix est un peu plus nuancée pour les pirates. Les comptes LinkedIn compromis permettent aux pirates d'accéder à de vastes quantités d'informations concernant le compte qu'ils ont compromis, ainsi qu'aux connexions du compte compromis. Nous avons également vu des cas où des pirates utilisent un compte LinkedIn compromis pour attaquer un autre utilisateur de LinkedIn en se faisant passer pour une relation professionnelle de confiance. L'usurpation de la marque Netflix est principalement considérée comme un moyen de s'approprier des comptes et de les vendre ou de tenter d'utiliser ces mêmes identifiants dans le cadre d'attaques par saturation d'identifiants.

Les données que nous avons recueillies sur ce point au cours de la période couverte par le rapport sont présentées ci-dessous :

26.1	DHL
18.5	OTHER
7.7	AMAZON
5.7	POSTBANK
2.5	STRATO
2.4	LINKEDIN
2.4	MICROSOFT
2.3	FEDEX
2.2	NETFLIX
2.1	1&1

Tableau 13 : Dix premières marques dont l'identité est usurpée

Remarque : les données sur l'usurpation d'identité de marque sont fortement touchées par les variations régionales. Plusieurs marques allemandes sont énumérées ici en raison de notre vaste clientèle en Allemagne.

Sécurité des données dans le nuage

En ce qui concerne l'état de la sécurité dans l'espace Microsoft 365, c'est beaucoup plus que le courriel, n'est-ce pas? M365 a changé la façon dont les organisations mènent leurs opérations. De plus en plus souvent, les entreprises utilisent les fonctionnalités supplémentaires de M365, et la discussion sur l'état de la sécurité de M365 doit donc dépasser les frontières du courrier électronique.

Les autres sections de ce rapport abordent de nombreux aspects de la sécurité au sein des services infonuagiques de Microsoft Cloud mais il convient d'examiner l'état général et la culture de la sécurité actuelle de Microsoft. En d'autres termes, ce n'est pas bon pour l'instant. Microsoft a connu plusieurs problèmes de sécurité au cours des dernières années. Il s'agit notamment de multiples atteintes de sécurité, telles que la situation de Storm-0558, de multiples vulnérabilités d'Exchange Server sur site et la fuite de données de 32 téraoctets à partir d'un compte de stockage en nuage.

Remarque

Pour une discussion plus approfondie sur les récents problèmes de sécurité liés à **Microsoft Cloud**, veuillez consulter cet épisode du balado dans lequel Andy Syrewicze et Paul Schnackenburg en parlent de façon détaillée.

Tout cela remet en question l'idée du rôle de Microsoft dans la sécurisation de votre entreprise. Actuellement, la culture de Microsoft en matière de sécurité est remise en question par de nombreux acteurs du secteur, ce qui met en lumière l'idée d'une dépendance excessive à l'égard d'un fournisseur.

Qu'est-ce que la dépendance excessive à l'égard d'un fournisseur?

La dépendance excessive à l'égard d'un fournisseur est la pratique qui consiste à confier à un partenaire fournisseur exclusif un grand nombre ou la quasi-totalité des processus et procédures de base de l'entreprise. Le problème de ce genre d'ententes est que si le fournisseur a des problèmes, l'entreprise en souffre de manière disproportionnée.

Quelques exemples :

1. Les sauvegardes hors site font depuis longtemps partie des meilleures pratiques informatiques. Cela s'applique également aux données stockées dans M365. S'appuyer sur les capacités de rétention de M365 ou tirer parti du produit de sauvegarde M365 de Microsoft (lorsqu'il sera enfin disponible) revient à stocker les sauvegardes sur la même plateforme de stockage que le système de production. Si les services infonuagiques de Microsoft Cloud ne sont pas disponibles, il est possible que les méthodes de récupération des données le soient aussi.

2. La taille et la portée des services infonuagiques de Microsoft Cloud en font une cible pour les pirates. Les pirates savent que s'ils parviennent à déjouer Exchange Online Protection pour un client, ils l'ont probablement fait pour TOUS les clients M365. Il s'agit d'un cas où une solution de sécurité tierce peut offrir de meilleures capacités que le fournisseur natif, en particulier contre les attaques très graves.

3. C'est rare, mais il est arrivé que les services infonuagiques de Microsoft Cloud deviennent indisponibles pendant un certain temps. L'année dernière, plusieurs pannes d'Azure Active Directory (désormais appelé Azure Entra) ont empêché les clients d'accéder à leurs données dans M365.

Microsoft détient actuellement une part de marché extrêmement importante avec Microsoft 365. De nombreux acteurs du secteur remettent en question la pratique consistant à utiliser le même fournisseur pour les logiciels de productivité/collaboration et la sécurité. Il existe un conflit d'intérêts potentiel dans la mesure où, en cas de défaillance ou de problème avec l'un des produits de sécurité de ce fournisseur, celui-ci peut NE PAS divulguer ou résoudre ce problème de manière adéquate en raison du risque de perdre des marchés dans le domaine de la productivité/collaboration.

Là encore, chaque organisation doit prendre sa propre décision en la matière. Néanmoins, compte tenu des récentes préoccupations en matière de sécurité et, en fin de compte, de la responsabilité de Microsoft en ce qui concerne vos données, le choix se révèle important.

De quoi Microsoft est-elle responsable?

La question ci-dessous revient très souvent : « Si Microsoft ne s'occupe pas de mes données et de ma sécurité, de quoi est-elle vraiment responsable? » La position actuelle de Microsoft sur cette question est restée la même en 2023. Pour bien comprendre, vous devez connaître le modèle de responsabilité partagée de Microsoft.

Le point crucial est que le modèle de responsabilité partagée stipule que « la responsabilité incombe toujours au client en ce qui concerne » :

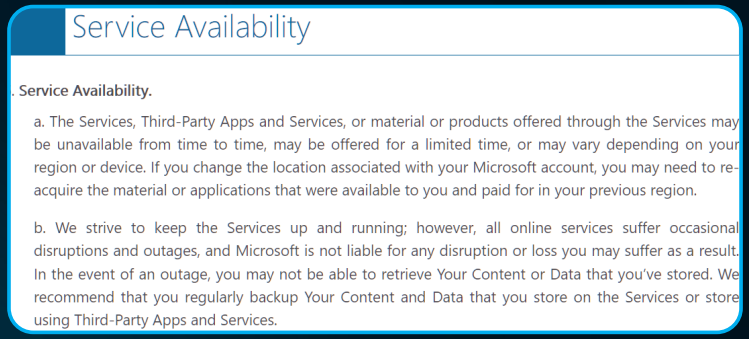
- Les informations et les données
- Les appareils (mobiles et ordinateurs de bureau)
- Les comptes et les identités

En principe, le client est responsable de la sécurité et de la protection de ses renseignements et données. Microsoft ne l'est pas. À mesure que les organisations se tournent vers le nuage, elles doivent en tenir compte lors de la mise en œuvre de stratégies de protection.

Cela dit, Microsoft a modifié en 2023 une position de longue date sur l'utilisation d'applications de sauvegarde avec M365. Lors d'une conférence Microsoft en début d'année, Microsoft a annoncé l'arrivée de la solution Microsoft 365 Backup. Un service a été présenté pour fournir des capacités de sauvegarde de base pour M365. Malgré cela, très peu d'informations supplémentaires ont été publiées depuis cette annonce restreinte dans sa portée. La partie la plus importante de cette annonce n'est pas le service lui-même, mais le changement de la position historique de Microsoft selon laquelle « vous n'avez pas besoin de sauvegarder vos données dans M365 ». De nombreux acteurs du secteur considèrent que cette évolution est due à l'une des raisons suivantes :

1. Microsoft a finalement cédé et admet désormais qu'une attention uniquement axée sur la conservation des données N'EST PAS suffisante dans M365.
2. Microsoft veut simplement s'approprier une partie du marché de la sauvegarde M365, maintenant que l'entreprise a constaté qu'il existait un vaste marché pour ce type de service.

Les deux options semblent probables, la deuxième étant renforcée par le fait qu'ils ont également publié une API de sauvegarde que les fournisseurs peuvent également utiliser, moyennant paiement. Quoi qu'il en soit, le message est plus clair que jamais. Les entreprises **SONT** responsables de la protection de toutes les données qu'elles sauvegardent en utilisant les services infonuagiques de Microsoft Cloud.



Service Availability

Service Availability.

a. The Services, Third-Party Apps and Services, or material or products offered through the Services may be unavailable from time to time, may be offered for a limited time, or may vary depending on your region or device. If you change the location associated with your Microsoft account, you may need to re-acquire the material or applications that were available to you and paid for in your previous region.

b. We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.

Les difficultés d'une bonne gestion des autorisations dans M365

Le partage des autorisations dans les sites SharePoint et OneDrive Entreprise constitue un autre défi particulièrement pernicieux pour les services informatiques. L'environnement professionnel d'aujourd'hui est constitué d'équipes virtuelles collaboratives, souvent dans des entreprises distinctes, qui partagent des documents de diverses manières. Il n'est pas possible de verrouiller ce système (cela ne ferait qu'inciter les utilisateurs à recourir à des formes non autorisées de partage de documents dans le nuage, ce qui aurait un impact sur la visibilité des services informatiques). De même, vous ne pouvez pas non plus laisser la porte grande ouverte avec des liens vers des données sensibles qui sont partagées sans discernement. Les outils intégrés pour gérer cela dans Microsoft 365 sont fragmentés dans divers portails et difficiles à gérer à grande échelle, ce qui fait de la gestion des permissions dans Microsoft Cloud un grand sujet de préoccupation en ce qui a trait à l'état de sécurité dans M365. Cela dit, le 365 Permission Manager de Hornetsecurity, unique en son genre, facilite la gestion des politiques de partage entre des milliers de comptes, notamment en permettant de vérifier qui a accès à quoi et en conciliant l'accès aux différents sites avec les exigences de la gestion des risques de l'entreprise.

Chapitre 3 – Analyse des principaux incidents de sécurité et de l'actualité de la cybersécurité en 2023

Plusieurs attaques et problèmes de sécurité notables ont eu lieu en 2023 et sont directement liés aux données recueillies pour le présent rapport. La présente section porte sur ces attaques.

Storm-0558

Au cours des 12 derniers mois, plusieurs incidents de sécurité très médiatisés ont affecté le service infonuagique de Microsoft 365, mais l'attaque Storm-0558 est sans conteste celle qui a eu le plus d'impact. En résumé, le groupe de pirates informatiques parrainé par l'État chinois et désigné par Microsoft sous le nom de Storm-0558 a compromis le compte d'un ingénieur en 2021. Bien que l'environnement de production soit isolé du réseau de l'entreprise, en avril 2021, un système de signature des consommateurs (partie d'Azure AD, maintenant Entra ID) a cessé de fonctionner et produit un vidage d'incident.

Il a été transféré sur le réseau de production à des fins de débogage et le système automatisé conçu pour détecter les identifiants dans les dumps a connu une défaillance. Ainsi, lorsque les pirates ont pénétré dans ce compte, ils ont eu accès au dump et à la clé.

Cette intrusion leur a permis de créer leurs propres clés, même si la clé dans le dump avait expiré, et en raison d'une incapacité à séparer les clés des consommateurs (Hotmail, Xbox, etc.) des clés d'entreprise (M365, Azure), le système de validation n'a pas été mis en œuvre, mais seulement documenté que ces clés étaient valides. Cela a permis aux pirates d'obtenir une « clé de porte dérobée » pour accéder à tous les locataires M365 (et à tous les locataires Azure, bien qu'il n'y ait aucune preuve que cela ait été utilisé). À l'heure où nous écrivons ces lignes, cette atteinte à la sécurité a « seulement » entraîné la violation de quelques dizaines de comptes de courrier électronique au département d'État américain et le vol de 60 000 courriels.

Il s'agit probablement de l'atteinte à la sécurité la plus grave jamais survenue dans le nuage, qui compromet la plateforme d'identité d'une manière qui ébranle clairement la confiance à l'égard du nuage et de la ou des plateformes de Microsoft. Pour être clair, il a été très difficile de détecter cette activité malveillante par des entreprises utilisant M365, et ce n'est qu'en juin 2023 qu'un analyste de la sécurité d'un organisme fédéral américain a détecté des événements suspects « MailItemsAccessed » (Accès à des courriels) et les a signalés à Microsoft et à la CISA (Cybersecurity and Infrastructure Security Agency – Agence pour la cybersécurité et la sécurité des infrastructures). Cette agence ne disposait de ces journaux que parce qu'elle avait payé le forfait E5, l'unité de licence M365 la plus élevée de Microsoft.

Cette atteinte à la sécurité a engendré les conséquences suivantes : Microsoft a finalement modifié son approche de la disponibilité des journaux pour les différents niveaux de licence, et toutes les unités de licence d'entreprise disposent désormais d'un accès étendu aux journaux. Cette exigence a été formulée pour la première fois en 2020, après l'attaque de Solarwinds. Par ailleurs, le prochain rapport du US Cyber Security Review Board (CSRB) sera axé sur cette atteinte à la sécurité. Il reste à voir si et dans quelle mesure cette atteinte à la sécurité obligera Microsoft à se remettre en question et à améliorer son système de sécurité global.

nOAuth

Une autre faille de sécurité, baptisée nOAuth, exploite l'utilisation courante de comptes de courrier électronique comme identifiants et d'applications enregistrées dans Entra ID (anciennement Azure AD) qui permettent de se connecter avec des comptes de consommateurs. Microsoft met explicitement en garde contre l'utilisation du courrier électronique comme identifiant dans ces demandes, mais cela ne diminue en rien la complexité et les risques associés à l'enregistrement d'applications multi-locataires dans Azure.

Les cyberattaques de MGM/ Caesars Entertainment

Les casinos Caesars et MGM ont subi deux des atteintes à la sécurité les plus marquantes au cours des 2023. Bien qu'elles ne présentent pas les mêmes symptômes, elles contiennent toutes deux des enseignements importants pour la protection de votre entreprise. Dans le cas de MGM, un pirate du groupe Scattered Spider a utilisé l'ingénierie sociale lors d'un appel téléphonique pour tromper un représentant du service d'assistance et lui demander de réinitialiser toutes les méthodes d'AMF pour son compte Okta super administrateur, qu'il a ensuite utilisé pour configurer la fédération afin d'usurper l'identité d'utilisateurs. Une fois compromises, 6 téraoctets de données auraient été exfiltrées, et les données d'entreprise ont été cryptées dans une attaque par rançongiciel.

MGM a choisi de ne pas payer et l'entreprise a indiqué qu'elle s'attend à ce que le coût global pour eux soit de 100 millions de dollars; apparemment, elle a jusqu'à 200 millions de dollars en couverture d'assurance pour la cybersécurité. L'entreprise a dû faire face à des pannes généralisées de ses systèmes pendant qu'elle travaillait à leur rétablissement, et les atteintes à sa réputation vont probablement bien au-delà de l'argent, d'autant plus que les pirates ont obtenu des données sensibles provenant d'interactions avec des clients avant mars 2019.

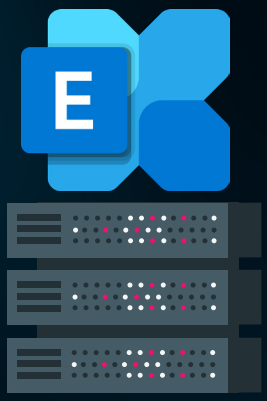
La société Caesars a été victime d'une intrusion chez un fournisseur de services informatiques tiers et a choisi de payer la rançon (à l'origine, les pirates voulaient 30 millions de dollars, mais cette somme a été négociée à 15 millions de dollars).

Plusieurs enseignements peuvent être tirés de ces atteintes à la sécurité pour améliorer la cyber-résilience de votre organisation :

- Le personnel de votre service d'assistance aurait-il été suffisamment vigilant pour repérer cette attaque? Formez vos utilisateurs et sensibilisez à tous les vecteurs d'attaque, et pas seulement aux courriels d'hameçonnage. L'hameçonnage vocal (« Vishing » ou « Voice Phishing » en anglais) est plus efficace qu'un simple courrier électronique, d'autant plus que les informations personnelles requises pour usurper l'identité d'une personne sont souvent accessibles au public sur LinkedIn, Facebook et les sites Web des entreprises. L'hameçonnage par code QR (« Qishing » ou « QR code phishing ») est une autre méthode qui gagne en popularité.
- N'autorisez pas votre service d'assistance de réinitialiser l'AMF et les mots de passe pour les comptes à privilèges élevés. Votre authentification est aussi forte que vos méthodes de réinitialisation, et si quelqu'un parvient à tromper un utilisateur du service d'assistance pour ajouter ou réinitialiser des méthodes d'AMF, alors la partie est terminée.
- Surveillez et alertez sur l'ajout d'organisations fédérées dans votre fournisseur d'identité (« IdP » ou « Identity Provider »), qu'il s'agisse d'Okta, de Ping, d'Entra ID dans Microsoft 365 ou de Google. Ce vecteur a été utilisé par les pirates dans le cas de Solarwinds en 2020 et est toujours prisé.
- Exigez des preuves de la résilience de vos fournisseurs tiers en matière de cybersécurité. Les entreprises modernes sont interdépendantes, de sorte que même si votre personnel fait tout ce qu'il faut, vous pouvez toujours être victime en raison d'une sécurité laxiste chez un fournisseur de confiance.

Vulnérabilités de Microsoft Exchange

Certaines organisations utilisent toujours des serveurs Exchange sur site, souvent dans une configuration hybride avec Microsoft 365. Ces serveurs restent une cible de choix pour les pirates. En 2021, nous avons eu ProxyShell, suivi par ProxyNotShell en 2022, puis en août 2023, des correctifs pour trois vulnérabilités d'exécution de code à distance ont été lancés. Au total, il y a eu 31 vulnérabilités Exchange Server en 2021, 18 en 2022 et 23 (jusqu'à présent) en 2023. Nous vous recommandons de mettre hors service vos serveurs Exchange sur site et d'effectuer la migration vers Exchange Online dès que possible.



ANNÉE	VULNÉRABILITÉS DU SERVEUR EXCHANGE
2023	23 jusqu'à présent
2022	18
2021	31

Tableau 14 : Vulnérabilités du serveur Exchange

L'interruption de Qakbot

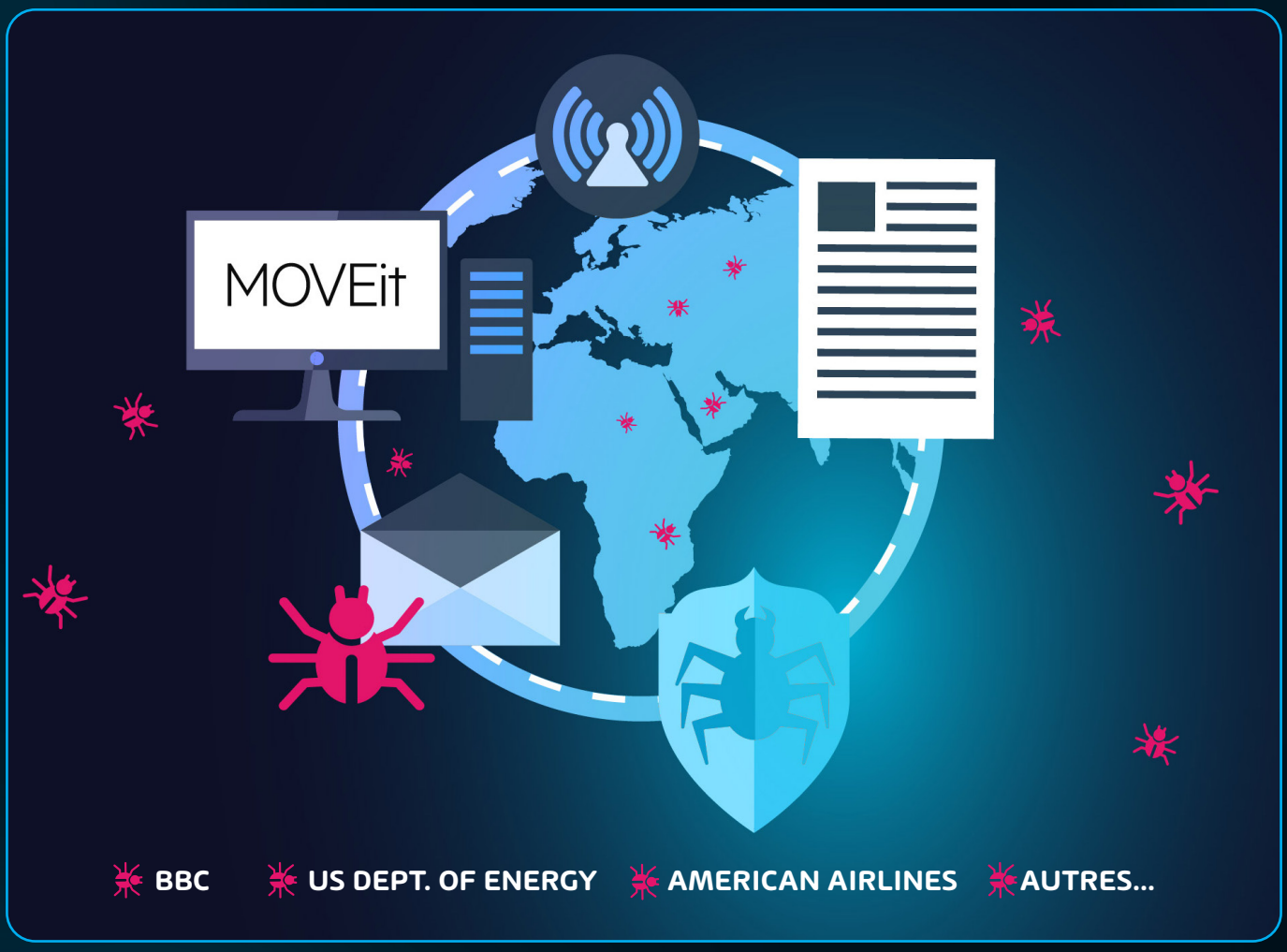
Qakbot était un réseau de zombies malveillants bien connu, utilisé par des pirates pendant une longue période. Il a été à l'origine d'innombrables attaques sur le Web et a été largement traité par les médias spécialisés en cybersécurité et des chercheurs en sécurité (dont notre entreprise!).

En août de 2023, le FBI et ses partenaires des organismes chargés de l'application de la loi du monde entier ont réussi à prendre le contrôle du réseau de zombies Qakbot et à le fermer. Il s'agit sans aucun doute d'une bonne chose, mais cela laisse néanmoins un certain vide. Les pirates associés à Qakbot ne vont pas renoncer à leurs attaques. Ils s'efforceront de rétablir Qakbot ou se tourneront vers d'autres outils. Comme nous l'avons évoqué dans un épisode du Balado Security Swarm, le logiciel malveillant DarkGate semble être une alternative éventuelle pour combler le vide laissé par Qakbot. Les équipes de sécurité devront être à l'affût de ce logiciel malveillant et d'autres à l'approche de 2024.

L'attaque de la chaîne d'approvisionnement MOVEit

L'année ne serait pas bouclée en matière de cybersécurité sans qu'il n'y ait d'importantes attaques de type « chaîne d'approvisionnement ». Plusieurs attaques de ce type ont eu lieu en 2023, mais l'attaque de la chaîne d'approvisionnement MOVEit a été de loin la plus grave. MOVEit est une application logicielle qui fournit des services de transfert de fichiers à un grand nombre d'entreprises dans le monde entier. L'attaque consistait en l'exploitation de plusieurs vulnérabilités (principalement des vulnérabilités par injection SQL) dans le code base MOVEit et a été utilisée pour voler les informations personnelles d'un nombre incalculable de victimes. Parmi les victimes figuraient des organisations, telles que la BBC, le US Dept. of Energy (ministère américain de l'Énergie), la compagnie American Airlines pour n'en nommer que quelques-unes.

Ce type d'attaques continue de souligner la nécessité de disposer de processus de correction efficaces et souples au sein des services informatiques des entreprises. Malgré la publication de mesures d'atténuation et de correctifs, de nombreuses organisations sont restées trop longtemps vulnérables à ces attaques, et le secteur de la sécurité et les fournisseurs de logiciels doivent continuer à travailler sur des solutions permettant d'atténuer l'impact des futures



Les prédictions de l'année dernière étaient-elles justes?

Dans le rapport sur la cybersécurité de l'année dernière, nous avons prédit le type d'attaques que nous verrions en 2023, et nous avions en grande partie raison.

Certains groupes criminels se sont tournés vers les cibles gouvernementales de l'hémisphère sud, perçues comme « douces », avec le Costa Rica, l'Équateur et le Chili en 2022, suivis du Brésil, des Bermudes et de la Colombie en 2023, sans oublier de nombreuses cibles dans la région de l'Asie de l'Est. Nous pensions que la compromission des courriels d'entreprise dépasserait le rançongiciel, le vecteur d'attaque le plus populaire, mais il s'avère que le « secteur des rançongiciels » se porte toujours bien et qu'il s'apprête à réaliser sa deuxième année de revenus la plus élevée en 2023, avec près de 900 millions de dollars (après 939 millions de dollars en 2021).

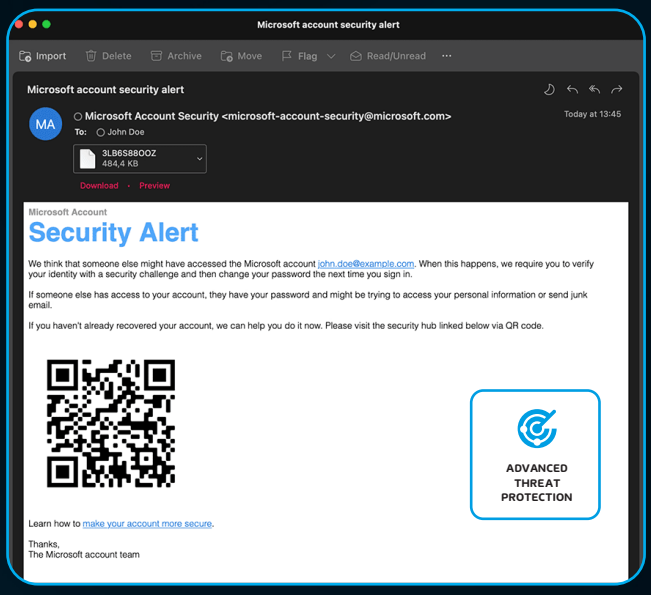
Les techniques de contournement de l'AMF sont de plus en plus sophistiquées et faciles à utiliser, comme nous l'avions prédit, compte tenu de l'augmentation du nombre d'entreprises qui protègent leur identité au moyen de l'AMF. Nous constatons que des pirates entreprenants utilisent les messages externes de Teams comme appâts d'hameçonnage, et de nombreux utilisateurs ne sont pas au courant de ce vecteur, mais le nouveau client Teams qui n'est pas intégré à Electron rendra au moins le client plus sûr.

Le vol de jetons à partir d'une machine compromise et leur réutilisation dans d'autres attaques ont augmenté, tout comme le vol général de témoins de connexion pour faciliter le vol d'identité, comme l'a montré le démantèlement par le FBI du Genesis Market en avril 2023 dans le cadre de l'opération baptisée « Cookie Monster ».

Nous avons également examiné les logiciels espions mobiles et leur importance, Predator et Pegasus étant utilisés par différents pays, non seulement pour espionner des criminels, mais aussi des dissidents, des ennemis politiques et des journalistes (la Grèce en est un exemple).

Microsoft 365 en tant que plateforme n'est pas devenue moins complexe à configurer de manière sécurisée. Comme nous l'avions prévu, le délai entre une vulnérabilité rendue publique et la mise à disposition d'un code d'exploitation est de plus en plus court, ce qui met les équipes SOC au défi de suivre le rythme.

Les opérations d'information (OI) et la désinformation représentent un risque croissant pour les entreprises et la société en général, en particulier avec l'absence de modération du contenu de X (anciennement Twitter) sous la nouvelle direction, et avec ChatGPT et d'autres grands modèles de langage de l'IA générative à grand langage qui facilitent plus que jamais la désinformation à grande échelle.



Une « prédiction » qui ne figurait pas dans le rapport sur la cybersécurité de l'année dernière, mais qui s'est révélée particulièrement pertinente récemment, est l'inclusion de l'hameçonnage par courriel au moyen de codes QR dans la plateforme de l'outil Advanced Threat Protection de Hornetsecurity. Au cours des derniers mois, ce vecteur d'attaque a connu une forte augmentation, les autres solutions d'hygiène du courrier électronique ayant du mal à protéger les utilisateurs finaux contre les liens malveillants intégrés dans les codes QR. Au cours des derniers mois, ce vecteur d'attaque a connu une forte augmentation, les autres solutions d'hygiène du courrier électronique ayant du mal à protéger les utilisateurs finaux contre les liens malveillants intégrés dans les codes QR.

Enfin, nous avions raison de prédire l'essor des solutions d'authentification sans mot de passe, bien que nous n'ayons pas vu les clés d'accès devenir aussi populaires qu'elles l'ont été dans l'espace grand public.

Les attaques contre les API augmentent également rapidement, comme nous l'avons indiqué dans le rapport de l'an dernier, et il s'agit d'un domaine sur lequel les équipes de sécurité devront se concentrer, car il s'agit souvent d'une infrastructure « cachée en arrière-plan, qui fait partie de la plomberie » et qui est peu surveillée. L'atteinte à la sécurité survenue chez Optus en Australie (10 millions de clients) fin 2022 en est un exemple, mais il y en a beaucoup d'autres.

Les prévisions du Security Lab pour 2024

Chaque année, dans le cadre de ce rapport, l'équipe du Security Lab de Hornetsecurity examine l'état du secteur, nos données, les tendances en matière d'attaques, etc. afin de faire une série de prédictions pour l'année à venir. Les entreprises sont ainsi informées des menaces potentielles auxquelles elles pourraient être confrontées au cours de l'année à venir, ainsi que de l'évolution du secteur. Voici les prévisions du Security Lab pour 2024.

L'IA continuera à stimuler le secteur de la cybersécurité

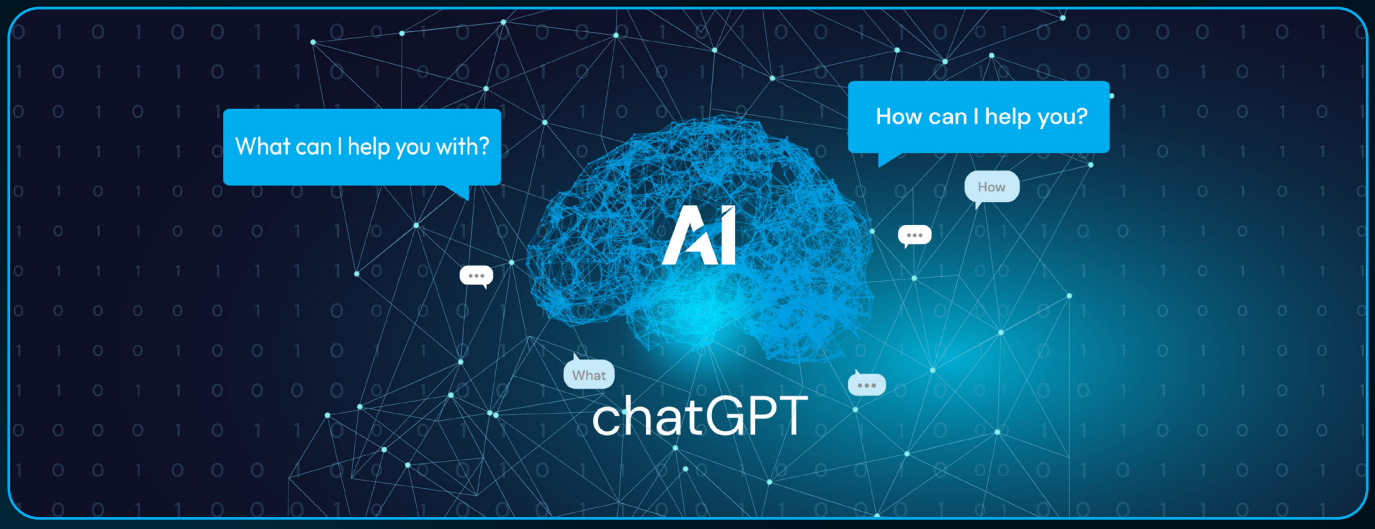
Avec le lancement de ChatGPT d'OpenAI fin 2022 et sa popularité croissante début 2023, l'IA générative a rapidement commencé à transformer le secteur de la cybersécurité. Il est devenu immédiatement évident que l'IA générative pourrait être utilisée par des pirates novices pour non seulement lancer des attaques, mais aussi apprendre COMMENT lancer des attaques. En fait, nous avons mené nos propres recherches sur ce sujet dans le Security Lab et publié certaines de nos conclusions dans le tout premier épisode du Balado Security Swarm.

Ces nouvelles capacités ont non seulement entraîné une explosion des cyber-attaques tout au long de l'année, mais continuent également d'intensifier les inquiétudes. Il reste cependant une bonne nouvelle concernant l'utilisation de l'IA générative par les pirates. Le fait est que les pirates chevronnés possédaient déjà ces compétences et que les pirates novices qui cherchent à exploiter des outils tels que ChatGPT pour lancer des attaques doivent encore consacrer un temps considérable à la compréhension de l'ensemble de la chaîne d'attaque pour une attaque donnée, car l'IA générative n'est pas en mesure de le faire à leur place.

Cela dit, l'une de nos prévisions pour l'année à venir est que les pirates continueront de développer leurs variantes Darkweb (Web invisible) de ChatGPT (comme DarkBERT et WormGPT) afin de mieux comprendre et d'être en mesure d'automatiser d'autres maillons de la chaîne d'attaque. Les pirates novices disposeront ainsi de capacités accrues, ce qui accélérera le rythme des cyberattaques dans l'industrie. La capacité des grands modèles de langage (LLM – Large Language Model) à traduire de façon crédible des textes dans d'autres langues ouvre également de « nouveaux marchés » pour les criminels, d'autant plus que bon nombre de ces pays ne sont pas culturellement aussi habitués aux attaques par hameçonnage, par exemple.

En outre, une attaque potentiellement intéressante que nous n'avons pas encore vue à grande échelle est une attaque du pirate CONTRE un service d'IA générative. L'objectif final serait de compromettre (« empoisonner ») les réponses de l'IA dans le seul but de diffuser des informations erronées. Toute attaque de ce type sera très sophistiquée et très probablement menée par un État-nation, si (et quand) elle se produit.

Alors que le cycle des nouvelles sur la cybersécurité s'est presque entièrement concentré sur les impacts négatifs de l'IA générative sur notre industrie, il y a aussi de bonnes nouvelles. Alors que la course aux armements en matière de cybersécurité se poursuit, les experts en sécurité et les fournisseurs utilisent également l'IA générative dans leurs outils de défense. Des organisations spécialisées dans l'IA, comme OpenAI, ont même créé des programmes de subvention spécialement conçus pour aider les organisations de cybersécurité à « rendre leurs offres compatibles avec l'IA ».



Nous prévoyons que cela se manifestera de plusieurs façons, par l'utilisation de l'IA pour la détection des d'anomalies, l'analyse des journaux, les attaques simulées (voir plus loin), la modélisation des menaces et plus encore.

Les entreprises devront se tenir informées de ces évolutions et adapter leur dispositif de sécurité en conséquence au cours de l'année à venir.

Partenaires d'entraînement de grands modèles de langage (LLM – Large Language Model) pour les équipes bleues

Cette prédiction s'inscrit dans le cadre de la discussion précédente sur l'IA générative, mais elle est suffisamment intéressante pour mériter sa propre section.

Une chose qui a toujours été difficile pour les équipes bleues est d'effectuer des simulations correctes de pirates. Bien sûr, vous pouvez faire appel à une organisation extérieure ou embaucher votre propre testeur de pénétration, mais sa vision de l'environnement cible risque d'être faussée par le fait qu'il connaît déjà l'environnement. Le coût pourrait également être un problème.

C'est un domaine dans lequel les grands modèles de langage (LLM) pourraient jouer un rôle important dans les opérations de sécurité. Un pirate simulé par l'IA pourrait lancer plusieurs simulations d'attaques contre votre organisation. Cela joue un rôle important non seulement pour trouver des vulnérabilités inconnues dans votre infrastructure, mais aussi pour former les membres de l'équipe à la manière de réagir en toute sécurité en cas d'attaque.

Nous prévoyons que les LLM commenceront à être utilisés dans de nouvelles solutions logicielles afin de répondre à ce besoin.

Les technologies, telles que Co-Pilot entraîneront un besoin accru d'analyse de la sécurité et de la qualité du code

Les attaques par contournement de l'AMF vont augmenter en volume avec un degré de sophistication plus élevé. Alors que les entreprises adoptent en général des formes d'authentification plus solides que le « meilleur ami » des criminels, à savoir le nom d'utilisateur et le mot de passe, les pirates s'adaptent eux aussi. Plusieurs « trousses de contournement de l'AMF » sont apparues. Elles simplifient le processus de configuration d'un serveur mandataire pour agir comme un « attaquant au milieu » – présentant une page d'ouverture de session convaincante pour l'utilisateur, et à mesure qu'il saisit ses identifiants (y compris une invite de l'authentification multifactorielle), ceux-ci sont transférés à la page d'ouverture de session réelle, en inscrivant l'utilisateur au service légitime, tandis que la trousse saisit une copie des témoins de session, ce qui permet au pirate de se faire passer pour l'utilisateur. Evilginx (source ouverte) et le panneau W3LL et les outils connexes pour faciliter la compromission des courriels d'affaires en sont des exemples. Les différentes technologies d'AMF ont des forces différentes. Assurez-vous donc que votre entreprise utilise les plus fortes pour l'accès aux données et applications sensibles.

L'adoption des produits XDR et MDR augmente

La tendance et le besoin d'une sécurité accrue dans l'industrie ne font que s'accélérer. Par conséquent, nous prévoyons une augmentation de l'adoption des solutions XDR (Extended Detection and Response – Détection et intervention étendues) et MDR (Managed Detection and Response – Gestion de la détection et des interventions) dans tous les secteurs. Compte tenu de l'omniprésence des cybermenaces, aucune solution unique ne constitue une protection adéquate. Les entreprises doivent adopter une approche à plusieurs niveaux, ce qui inclut l'enregistrement et la diffusion appropriés des événements de sécurité dans l'ensemble du patrimoine numérique d'une organisation. Sans une bonne visibilité, de nombreuses attaques passent totalement inaperçues et les responsables de la sécurité des systèmes d'information (RSSI) et les responsables des technologies commencent à donner la priorité à leur niveau de visibilité en matière de sécurité.

Augmentation des attaques contre la chaîne d'approvisionnement

Les attaques contre la chaîne d'approvisionnement ne sont pas vraiment nouvelles pour nous dans l'industrie. Un certain nombre d'attaques contre la chaîne d'approvisionnement ont eu lieu récemment, notamment une attaque contre la chaîne d'approvisionnement en mars 2023 impliquant 3CX, ainsi que l'attaque bien connue de MOVEit au début de l'été 2023. Le problème de ce type d'attaque est son impact potentiel. Les deux cas mentionnés ci-dessus ont mis en danger d'innombrables organisations et les données privées de millions de personnes.

Au fur et à mesure que les services numériques s'intègrent dans notre société, ils deviennent de plus en plus étendus et, en fin de compte, de plus en plus une cible. Les pirates savent que s'ils parviennent à s'introduire chez un fournisseur qui offre un tel service, ils ont plus de chances d'obtenir une gros pactole. Non seulement ils peuvent demander une rançon pour les données, mais beaucoup d'entre eux se retournent

ensuite pour vendre ces données sur le Web invisible dans le cadre d'une campagne de double extorsion. Mais ce n'est pas le seul risque. Dans le cas de l'attaque de la chaîne d'approvisionnement MOVEit, l'exploit – une attaque exploitant une faille de sécurité – a permis aux pirates d'accéder facilement à toutes les organisations touchées. Ainsi, au lieu de s'en prendre à une seule organisation, TOUTES les entreprises qui utilisent les logiciels concernés risquent de subir des fuites de données et des extorsions.

Par conséquent, nous pouvons facilement prédire que ce type d'attaques se poursuivra et augmentera au cours de l'année à venir.

La complexité du nuage continuera à provoquer des incidents de sécurité

L'une de nos prédictions de l'année dernière portait sur le fait que la complexité croissante du nuage entraînerait de nouveaux incidents de sécurité. Nous sommes prêts à refaire cette prédiction pour l'année à venir.

Alors que les entreprises continuent d'adopter rapidement les technologies du nuage et que les innovations dans ce domaine se multiplient, la sécurité apparaît parfois comme une préoccupation secondaire. Il existe d'innombrables exemples de compartiments S3 d'Amazon qui n'ont pas été sécurisés, et même une violation de 38 téraoctets de données directement sous le nez de Microsoft en raison d'un compte de stockage Azure mal configuré. Il ne s'agit là que d'exemples concernant le stockage en nuage. C'est sans compter l'adoption massive des API en nuage, les configurations de réseau de plus en plus complexes, une main-d'œuvre de plus en plus nombreuse qui travaille de n'importe où parmi tant d'autres facteurs. Ces complexités augmentent le risque de commettre des erreurs, ce qui entraînera d'autres atteintes à la sécurité au cours de l'année à venir.

L'adoption accrue de la 5G et la dépendance des opérateurs à l'égard du VNI (Network Slicing VNI – Découpage réseau VNI) favoriseront les attaques contre les réseaux mobiles

Les appareils mobiles sont devenus omniprésents dans la vie quotidienne. Pour tenter de répondre au besoin insatiable de la société en matière de bande passante, la plupart des opérateurs de téléphonie mobile ont déployé l'infrastructure 5G dans leurs réseaux. Afin de faciliter cette tâche, de nombreux opérateurs ont commencé à s'appuyer sur une stratégie connue sous le nom de découpage du réseau. Dans ce cas, l'opérateur divisera son réseau en plusieurs réseaux logiques à différents niveaux et s'appuiera sur le réseau défini par logiciel (SDN) pour gérer le routage, la commutation et la gestion du trafic.

Le problème des réseaux définis par logiciel est la partie « logiciel » de cette équation. Les logiciels sont (généralement) plus difficiles à sécuriser et peuvent être utilisés par les pirates pour lancer des attaques. En fait, la NSA (National Security Agency – Agence nationale de sécurité) et la CISA ont publié un rapport sur les dangers du découpage en tranches du réseau et ont fourni des conseils sur cette pratique.

Cela dit, avec l'augmentation de l'empreinte de la 5G, la dépendance croissante à l'égard des réseaux mobiles et la dépendance accrue à l'égard du SDN, nous nous attendons à voir davantage d'attaques ciblant les réseaux mobiles au cours de l'année à venir.

Des pirates plus performants et des temps de latence plus courts

Les groupes de rançongiciels devenant plus compétents et plus complexes, nous constatons qu'ils redoublent d'efforts pour exécuter les attaques en un temps record. En conséquence, le temps de latence a considérablement diminué au cours de l'année écoulée, et nous nous attendons à ce que cette tendance se poursuive. Le temps de latence est le temps pendant lequel les pirates s'attardent sur les réseaux avant de prendre des mesures offensives susceptibles d'alerter les systèmes de sécurité ou de faire connaître leur présence. Avec l'augmentation du nombre de failles de sécurité de type zero-day et un secteur de la cybersécurité qui s'efforce frénétiquement de suivre le rythme, les pirates savent qu'ils doivent exécuter leurs attaques en un temps record avant que les défenses ne soient mises en place.

Encore une fois, cela montre que nous continuons à voir des preuves que les groupes de pirates deviennent plus sophistiqués (CONTI, par exemple). Ces groupes testent activement les nouvelles vulnérabilités, étudient les applications antivirus et mettent au point des solutions de contournement et des exploits. Tout cela laisse présager une augmentation des attaques par rançongiciel ainsi qu'une volonté délibérée de supprimer les sauvegardes de données au cours de l'année à venir.

Le point sur l'informatique quantique et le chiffrement

Dans le rapport de l'année dernière, nous avons abordé un risque futur : l'informatique quantique, capable de briser facilement les normes de cryptage actuelles. Contrairement aux autres risques mentionnés dans le présent rapport, ce risque n'est pas imminent (les services d'informatique quantique disponibles dans le commerce sont encore très sujets aux erreurs), mais comme les données cryptées et le trafic réseau enregistrés aujourd'hui pourraient être facilement violés à l'avenir, il est important de commencer à planifier.

La Cybersecurity and Infrastructure Security Agency, la National Security Agency (NSA) et le National Institute of Standards and Technology (NIST) se sont mis d'accord et ont récemment publié cette brève fiche d'information. Trois des quatre normes que nous avons mentionnées l'année dernière sont maintenant à l'état de versions préliminaires et devraient être finalisées en 2024.

Quel sera le niveau de risque de mon organisation en 2024?

La réponse brève et simple est, encore une fois, que si votre organisation est capable de payer une rançon, vous **ÊTES** une cible. C'est ce que démontrent nos données concernant l'indice des menaces par courriel dans tous les secteurs. Cela dit, si votre organisation traite des données sensibles, est impliquée dans le secteur de la défense ou de l'infrastructure critique, ou détient une propriété intellectuelle de grande valeur, vous êtes une cible plus prioritaire.

Ce que les organisations devraient faire pour se défendre

Commencer par les principes de base

Les organisations ont tendance à réagir à des menaces spécifiques et à acquérir des solutions de sécurité ponctuelles pour chaque domaine, et donc à se concentrer sur les solutions technologiques, au lieu de commencer par couvrir les principes de base de l'hygiène en matière de sécurité. La grande majorité des entreprises victimes d'une atteinte à la sécurité ne le sont pas en raison d'une attaque obscure exploitant une faille de sécurité non connue (« zero-day ») ou d'une technique de piratage avancée. Leurs systèmes de défense échouent parce qu'elles n'ont pas mis en œuvre une authentification forte (MFA, de préférence du matériel résistant aux hameçonnages), autorisé des mots de passe simples, configuré les utilisateurs en tant qu'administrateurs locaux sur leurs appareils ou n'ont pas formé les utilisateurs à être prudents lorsqu'ils cliquent sur des liens dans des courriels. Ne pas valider les sauvegardes en testant les procédures de restauration peut conduire à une très mauvaise journée en cas d'attaque par rançongiciel, tout comme une politique laxiste en matière de correctifs.

En d'autres termes, il faut d'abord s'occuper de l'hygiène de base en matière de sécurité, ce qui inclut la technologie, les processus et les personnes. Commencez par adopter un état d'esprit de confiance zéro :

- **Vérifiez chaque connexion** – ce n'est pas parce qu'un appareil est géré qu'il est automatiquement sûr, et ce n'est pas parce qu'un utilisateur se connecte à partir d'un réseau connu qu'il ne s'agit pas d'un pirate utilisant des identifiants volés.
- **Utilisez le principe du moindre privilège** – n'accordez aux utilisateurs et aux identités de charge de travail que les autorisations dont ils ont besoin pour remplir leur rôle et procédez à des examens réguliers pour vous assurer que les autorisations accordées ne s'accumulent pas.
- **Supposez une atteinte à la sécurité** – renforcez vos systèmes de défense autant que votre budget le permet, mais étudiez également les scénarios possibles en cas de défaillance. Si un pirate compromet un utilisateur, comment le détecterez-vous? Comment pouvez-vous limiter la capacité d'un pirate à se déplacer latéralement dans votre environnement?

Une liste plus complète est disponible dans les commandements ZT des Groupes ouverts.

La culture mange la stratégie au petit déjeuner

Transformer votre organisation en une entreprise cyber-résiliente demandera du temps, des efforts et de la persévérance. Vous ne pouvez pas transformer votre entreprise en une cyber-forteresse bien défendue sans impliquer tout le monde et sans les aider à comprendre comment cela les affecte et pourquoi ils doivent faire partie de la solution.

Lorsqu'il s'agit de déployer l'AMF, il faut s'assurer que la direction donne l'exemple et qu'elle (et le conseil d'administration) comprend la raison de l'ajout d'une friction supplémentaire pour l'authentification. Une partie de ce changement de culture consiste à comprendre que la cyber-résilience n'est pas l'affaire des services informatiques ou des services de sécurité.

Le service informatique ne peut pas sécuriser des charges de travail dont il n'a pas connaissance, et si le service marketing déploie un site Web et une solution dite SaaS (« Software as a Service » ou logiciel en tant que service) de suivi des clients potentiels sans impliquer les services informatiques et la sécurité, le risque que cela introduit est du ressort du service marketing. Chaque choix technologique ou décision de processus qui définit le mode de fonctionnement d'une entreprise comporte des risques, et la manière dont ces risques seront gérés doit être transparente pour l'entreprise afin qu'elle puisse prendre les bonnes décisions.

Une leçon importante pour les services informatiques et de sécurité est de parler le bon langage, celui de la gestion des risques. Si vous commencez à parler de détails techniques et de fonctionnement, vous perdrez tous les autres membres de l'entreprise, mais si vous traduisez les changements de technologie et de processus en termes de risques opérationnels (ou de possibilités à exploiter pour l'entreprise), tout le monde devrait être d'accord.

Et cette cyber-résilience n'est pas statique, tout comme d'autres risques auxquels sont exposées les entreprises (géopolitiques, économiques, concurrents), elle est en constante évolution et l'entreprise doit apprendre et s'adapter en permanence. Parmi les exemples récents, on peut citer la manière dont les pirates contournent ou déjouent les formes d'AMF les « plus faibles », avec des trousses d'outils de type « attaquant au milieu » ou des attaques de fatigue de l'AMF. L'ingénierie sociale est un risque omniprésent. Votre service d'assistance aurait-il mieux réussi à défendre votre entreprise que ceux de Caesars ou de MGM?

Une stratégie de sécurité équilibrée

Il est clair que l'écosystème de la sécurité est aujourd'hui plus diversifié et plus dangereux qu'il ne l'a jamais été. Par conséquent, les entreprises doivent envisager de mettre en œuvre une approche équilibrée de la sécurité. Cela signifie qu'elles doivent être conscientes des menaces avancées qui peuvent cibler leur secteur d'activité et prendre des mesures pour les atténuer, tout en veillant à ce que les éléments de base soient également pris en compte.

Aucune organisation ne devrait s'appuyer sur une seule application ou un seul dispositif de sécurité, mais plutôt sur une approche à plusieurs niveaux qui couvre les vecteurs d'attaque courants ainsi que ceux qui sont spécifiques au secteur d'activité de l'entreprise.
Cela inclut :

- Détection de spam/malware de nouvelle génération avec ATP, Advance Threat Protection, pour l'analyse comportementale afin de se protéger contre le barrage continu de menaces basées sur le courrier électronique que nous observons dans ce secteur.
- Une formation de sensibilisation à la sécurité, Security Awareness Service, pour les utilisateurs finaux afin de les former à repérer les attaques d'ingénierie sociale et les attaques de spear-phishing.
- Des capacités de sauvegarde et de récupération des données sur site et des données hébergées dans des services en nuage tels que M365, à des fins de récupération en cas d'attaque par ransomware
- Des fonctions de conformité et de gouvernance qui aident à protéger contre les fuites accidentelles de données et à garantir que les contrôles de conformité sont respectés.

En intégrant ces fonctionnalités à leurs stratégies de sécurité, les entreprises peuvent être sûres de leur position en matière de sécurité à l'aube de l'année prochaine.

HORNETSECURITY

365 TOTAL PROTECTION

PLAN 4 - COMPLIANCE & AWARENESS

365 Total Protection couvre tous les aspects de la gestion de la sécurité et de la protection des données de Microsoft 365 d'une organisation : sécurité du courrier électronique, sauvegarde et récupération, conformité, gestion des autorisations et sensibilisation à la sécurité. La solution s'intègre de manière transparente à Microsoft 365, fournissant des couches supplémentaires de sécurité et de protection des données contre le spam, les logiciels malveillants et les menaces avancées.

PLAN 1	PLAN 2	PLAN 3	PLAN 4
BUSINESS	ENTERPRISE	BACKUP	COMPLIANCE & AWARENESS
SPAM & MALWARE PROTECTION	ADVANCED THREAT PROTECTION	BACKUP & RECOVERY OF MAILBOXES & TEAMS	PERMISSION MANAGEMENT
EMAIL ENCRYPTION	EMAIL ARCHIVING	BACKUP & RECOVERY OF ONEDRIVE & SHAREPOINT	PERMISSION ALERTS
EMAIL SIGNATURES & DISCLAIMERS	EMAIL CONTINUITY	BACKUP & RECOVERY OF ENDPOINTS	PERMISSION AUDIT

PLAN 4
PHISHING & ATTACK SIMULATION
SECURITY AWARENESS
ESI® REPORTING

PLAN 4
COMMUNICATION PATTERN ANALYSIS
AI RECIPIENT VALIDATION
SENSITIVE DATA CHECK

FONCTIONNALITÉS DE NOUVELLE GÉNÉRATION POUR UNE PROTECTION PUISSANTE ET COMPLÈTE

- Protection basée sur l'IA contre les cyberattaques les plus sophistiquées.
- Taux de détection les plus élevés du marché (99,9 % de spams et 99,99 % de virus)
- Sauvegarde et récupération de toutes les données M365, y compris les chats et les fichiers Teams
- Service automatisés de sensibilisation à la sécurité pour sensibiliser les employés aux cybermenaces
- Gestion des autorisations de fichiers, archivage des courriels à l'épreuve des audits, cryptage des courriels, signatures et clauses de non-responsabilité uniformes pour une conformité maximale.
- Services infonuagiques flexibles et évolutifs, entièrement gérés, avec une assistance 24 heures sur 24 et 7 jours sur 7
- Intégration transparente avec M365, onboarding en 30 secondes et un seul panneau de contrôle pour faciliter l'utilisation.
- Pas de matériel, pas de logiciel, pas de maintenance
- Tout est disponible dans un seul forfait, dans une seule licence

COMMENCEZ VOTRE ESSAI GRATUIT

www.hornetsecurity.com

À propos des auteurs

Appuyé par les données provenant directement de notre Security Lab

RÉDIGÉ PAR

Andy Syrewicze

Andy possède plus de 20 ans d'expérience dans la fourniture de solutions technologiques dans plusieurs secteurs verticaux de l'industrie. Il est spécialisé dans les infrastructures, le nuage et la suite Microsoft 365.

Andy est lauréat du prix MVP (Most Valuable Professional) de Microsoft dans la gestion du nuage et des centres de données et est l'un des rares à être également un expert en VMware.

Paul Schnackenburg

Paul Schnackenburg a commencé sa carrière dans le secteur des TI lorsque le DOS et les processeurs 286 étaient à la fine pointe. Il dirige Expert IT Solutions, une petite entreprise de conseil en TI sur la Sunshine Coast, en Australie. Il travaille également comme professeur de TI dans une Microsoft IT Academy.

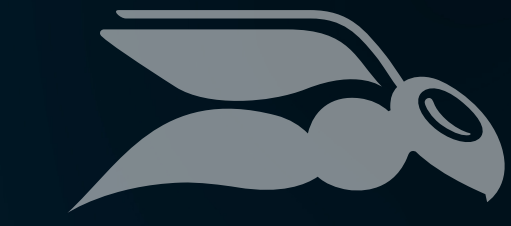
Auteur de contributions sur les technologies très respecté, Paul est actif au sein de la collectivité et a rédigé des articles techniques approfondis sur Hyper-V, le System Center, le nuage privé et hybride, Office 365 et les technologies infonuagiques publiques Azure.

Il détient les certifications MCSE, MCSA et MCT.

Chapitre 5 – Ressources

- https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked
- https://www.bleepingcomputer.com/news/security/w3ll-phishing-kit-hijacks-thousands-of-microsoft-365-accounts-bypasses-mfa/
- https://www.hornetsecurity.com/us/podcast-us/can-you-trust-microsoft-security/
- https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
- https://techcommunity.microsoft.com/t5/microsoft-syntex-blog/welcome-to-microsoft-inspire-2023-introducing-microsoft-365/ba-p/3874887
- https://www.hornetsecurity.com/us/services/365-permission-manager/
- https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/
- https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
- https://www.microsoft.com/en-us/security/blog/2023/07/19/expanding-cloud-logging-to-give-customers-deeper-security-visibility/
- https://www.descope.com/blog/post/noauth
- https://sec.okta.com/articles/2023/08/cross-tenant-impersonation-prevention-and-detection
- https://www.fbi.gov/news/stories/fbi-partners-dismantle-qakbot-infrastructure-in-multinational-cyber-takedown
- https://www.hornetsecurity.com/us/podcast-us/monthly-threat-report-discussion-october-2023/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
- https://www.chainalysis.com/blog/crypto-crime-midyear-2023-update-ransomware-scams/
- https://www.hornetsecurity.com/us/podcast-us/we-used-chatgpt-to-create-ransomware/
- https://www.zdnet.com/article/wormgpt-what-to-know-about-chatgpts-malicious-cousin/
- https://www.bleepingcomputer.com/news/security/cybercriminals-train-ai-chatbots-for-phishing-malware-attacks/
- https://www.hornetsecurity.com/us/podcast-us/generative-ai-in-defensive-tools/

- https://openai.com/blog/openai-cybersecurity-grant-program
- https://github.com/features/copilot
- https://github.com/kgretzky/evilginx2
- https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise
- https://www.bleepingcomputer.com/news/security/the-moveit-hack-and-what-it-taught-us-about-application-security/
- https://www.theregister.com/2023/05/17/another_security_calamity_for_capita/
- https://www.bleepingcomputer.com/news/microsoft/microsoft-leaks-38tb-of-private-data-via-unsecured-azure-storage/
- https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3459888/esf-members-nsa-and-cisa-publish-second-industry-paper-on-5g-network-slicing/
- https://therecord.media/ransomware-deployment-dwell-time-decreasing
- https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography
- https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers
- https://pubs.opengroup.org/security/zero-trust-commandments/
- https://salt.security/api-security-trends



HORNETSECURITY