SOPHOS

Rapport Sophos 2024 sur les menaces :
« Cybercrime on Main Street »

Les ransomwares restent la plus grande cybermenace ciblant les petites entreprises, mais d'autres se développent également.

Sophos X-Ops

Table des matières

Contexte

La cybercriminalité touche des personnes de tous horizons, mais elle frappe plus durement les petites entreprises. Alors que les cyberattaques contre les grandes entreprises et les agences gouvernementales sont, en général, largement relayé par les médias, les petites entreprises (au sens large, à savoir les organisations de moins de 500 employés) sont généralement plus vulnérables aux cybercriminels et souffrent proportionnellement plus des conséquences de ces cyberattaques. Le manque de personnel expérimenté pour gérer les opérations de sécurité, le sous-investissement dans la cybersécurité et la réduction globale des budgets IT (Information Technology) contribuent à ce niveau de vulnérabilité. De plus, lorsque ces organisations sont touchées par des cyberattaques, les dépenses liées à la récupération peuvent même contraindre de nombreuses petites entreprises à déposer le bilan.

Les petites entreprises sont loin d'être concernées uniquement par de petits problèmes. Selon la Banque Mondiale (World Bank), plus de 90 % des organisations dans le monde sont des petites et moyennes entreprises, et elles représentent plus de 50 % des emplois au niveau mondial. Aux États-Unis, les petites et moyennes entreprises représentent plus de 40 % de l'activité économique globale. (Dans ce rapport, nous utiliserons les termes petites et moyennes entreprises ou organisations de manière équivalente, reflétant leur similarité dans nos données.)

En 2023, plus de 75 % des cas client en matière de réponse aux incidents traités par le service X-Ops Incident Response de Sophos concernaient des petites entreprises. Les données collectées à partir de ces cas, en plus des données télémétriques collectées auprès des clients de notre logiciel de protection pour petites et moyennes entreprises, nous donnent un aperçu supplémentaire et unique des menaces qui ciblent quotidiennement ces organisations.

Résumé

Sur la base de ces données et des recherches menées par Sophos sur les menaces, nous constatons que les ransomwares continuent d'avoir le plus grand impact sur les petites organisations. Mais d'autres dangers constituent également une véritable menace pour les petites entreprises :

- Le vol de données est l'objectif de la plupart des malwares ciblant les petites et moyennes entreprises : les voleurs de mots de passe (password stealers), les enregistreurs de frappe (keyboard loggers) et d'autres spywares représentent près de la moitié des détections de malwares. Le vol d'identifiants via le phishing et les malwares peut exposer les données des petites entreprises présentes sur les plateformes Cloud et chez les fournisseurs de services, et les violations de réseau peuvent également être utilisées pour cibler les clients de ces derniers.
- Les attaquants ont intensifié la diffusion de malwares sur le Web, via le malvertising ou le SEO malveillant (« SEO poisoning »), pour contourner les difficultés créées par le blocage de macros malveillantes dans les documents, en plus d'utiliser des images disque pour saturer les outils de détection des malwares.
- Les appareils non protégés connectés aux réseaux des entreprises (notamment les ordinateurs non gérés et sans logiciel de sécurité installé, les ordinateurs mal configurés et les systèmes exécutant des logiciels non pris en charge par les fabricants) constituent le point d'entrée principal pour tous les types d'attaque cybercriminelle contre les petites entreprises.
- Les attaquants se tournent de plus en plus vers l'abus de pilotes (qu'il s'agisse de pilotes vulnérables provenant d'entreprises légitimes ou bien de pilotes malveillants signés avec des certificats volés ou obtenus frauduleusement) pour échapper et désactiver les défenses contre les malwares sur les systèmes gérés.
- Les attaques par email ne sont plus maintenant de simples ingénieries sociales, mais se tournent de plus en plus vers des techniques plus actives pour cibler leurs victimes via des emails, en utilisant un fil d'emails et de réponses pour rendre leurs appâts plus convaincants.
- Les attaques contre les utilisateurs d'appareils mobiles, notamment les escroqueries basées sur l'ingénierie sociale et liées à l'abus de services tiers et de plateformes de réseaux sociaux, ont connu une croissance exponentielle, affectant les particuliers et les petites entreprises. Celles-ci vont de la compromission de la messagerie professionnelle et des services Cloud aux escroqueries de type pig butchering (shā zhū pán (殺豬盤)).

Quelques précisions sur nos données

Les données utilisées dans notre analyse proviennent des sources suivantes :

- Rapports client : télémétrie de détection du logiciel de protection Sophos exécuté sur les réseaux des clients, qui donne une vue d'ensemble des menaces rencontrées et analysées au sein des SophosLabs (dans ce rapport, elle sera appelée 'Dataset Labs') ;
- Données MDR (Managed Detection and Response), collectées suite aux remontées provoquées par la détection d'activités malveillantes sur les réseaux des clients MDR (dans ce rapport, elles seront appelées 'Dataset MDR') ;
- Données de l'équipe Incident Response (IR), extraites d'incidents sur les réseaux clients d'entreprises de 500 employés ou moins où il y avait peu ou pas de protection MDR (Managed Detection and Response) en place (dans ce rapport, elles seront appelées 'Dataset IR').

Pour un examen plus approfondi des données extraites concernant uniquement des cas traités par notre équipe IR externe (notamment les cas impliquant des clients de plus de 500 employés), veuillez consulter nos publications associées concernant les rapports Active Adversary (AAR). Les conclusions de ces rapports sont basées, sauf indication contraire, sur des datasets combinés avec une normalisation appropriée.

Les données sont la principale cible

Le plus grand défi en matière de cybersécurité auquel sont confrontées les petites entreprises (et les organisations de toutes tailles) est la protection des données. Plus de 90 % des attaques signalées par nos clients impliquent un vol de données ou d'identifiants d'une manière ou d'une autre, qu'il s'agisse d'une attaque de ransomware, d'une extorsion de données, d'un accès à distance non autorisé ou bien simplement d'un vol de données.

Les attaques de type BEC (Business Email Compromise), dans lesquelles les comptes de messagerie sont piratés par un cybercriminel à des fins de fraude ou à d'autres fins malveillantes, constituent un problème important dans l'univers des petites et moyennes entreprises Nous ne couvrons pas actuellement les attaques BEC dans le rapport Active Adversary, mais les auteurs de ces rapports estiment qu'en 2023, les compromissions de messagerie professionnelle ont été identifiées par notre équipe IR plus souvent que tout autre type d'incident, à l'exception des ransomwares.

Les identifiants volés, notamment les cookies de navigateur, peuvent être utilisés pour compromettre la messagerie professionnelle, accéder à des services tiers tels que des systèmes financiers basés dans le Cloud et accéder à des ressources internes qui peuvent être exploitées à des fins de fraude ou pour générer divers gains financiers. Ils peuvent également être vendus par des « courtiers d'accès (access brokers) » à quiconque souhaiterait les exploiter ; Sophos a repéré des offres sur des forums underground prétendant donner accès à un certain nombre de réseaux de petites et moyennes entreprises.

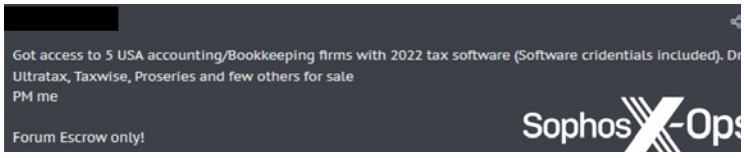


Figure 1 : Un message sur un forum faisant la promotion de l'accès à un petit cabinet comptable américain

Figure 2 : Un message sur un forum faisant la promotion de l'accès à une petite entreprise en Belgique

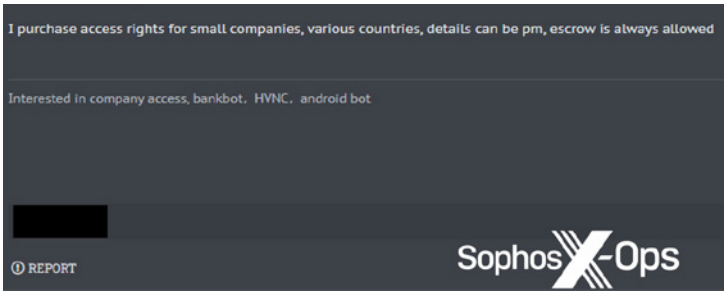


Figure 3 : Une offre cybercriminelle pour acheter l'accès à des petites entreprises

Figure 4 : Accès à une petite entreprise en Italie proposé à la vente sur un forum cybercriminel

Par catégorie, près de la moitié des malwares détectés en 2023 ciblaient les données de leurs victimes potentielles. La majorité d'entre eux sont des malwares que nous avons spécifiquement classés comme « voleurs (stealers) » : des malwares qui récupèrent les identifiants, les cookies du navigateur, les frappes au clavier et d'autres données qui peuvent être soit transformés en cash sous la forme d'un accès vendu, soit utilisés pour une exploitation ultérieure.

Cependant, en raison de la nature modulaire des malwares, il est difficile de les catégoriser uniquement et totalement par fonctionnalité : presque tous les malwares ont la capacité de voler une certaine forme de données sur les systèmes ciblés. Ces détections n'incluent pas non plus d'autres méthodes de vol d'identifiants, telles que le phishing par email, SMS et autres attaques par ingénierie sociale. Ensuite il existe d'autres cibles, telles que macOS, les appareils mobiles, où les malwares, les PUA (applications potentiellement indésirables) et les attaques par ingénierie sociale ciblent les données des utilisateurs, notamment celles de nature financière.

Catégories de malware en fonction du volume de mises à jour des signatures en 2023

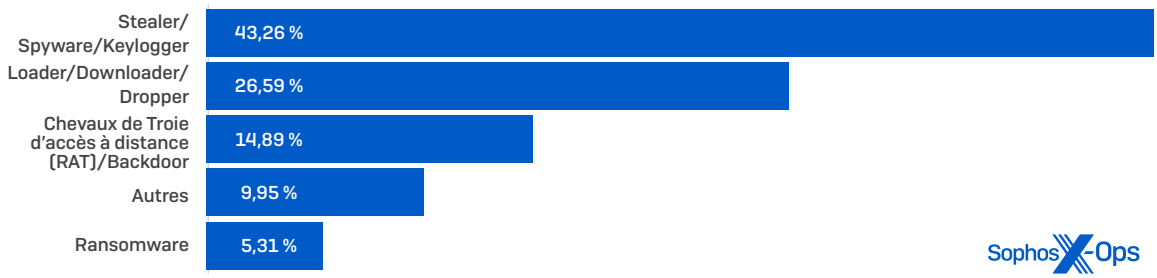


Figure 5 : Détections de malware par type pour l'année 2023, comme le montre nos datasets MDR et Labs

Près de 10 % des malwares détectés n'appartiennent pas aux quatre grandes catégories indiquées ci-dessus. Cette catégorie « autres » comprend les malwares qui ciblent les navigateurs pour injecter des publicités, rediriger les résultats de recherche afin de gagner de l'argent en échange de quelques clics, ou encore modifier ou collecter des données de toute autre manière au profit du développeur du malware en question, entre autres.

Certains voleurs sont très précis dans leur ciblage. Les voleurs de « token (jeton) » Discord, destinés à voler les identifiants du service de messagerie associé, sont souvent exploités pour diffuser d'autres malwares via des serveurs de chat ou via le réseau de diffusion de contenu (CDN : Content Delivery Network) de Discord. Mais d'autres stealers de premier plan : Strela, Raccoon Stealer et l'incontournable famille de stealers RedLine, sont beaucoup plus agressifs dans leur ciblage, collectant les magasins de mots de passe du système d'exploitation et des applications ainsi que les cookies du navigateur et d'autres données d'identification. Raccoon Stealer a également déployé des « clippers » de crypto-monnaie qui échangent les adresses de portefeuille crypto copiées dans le presse-papiers avec une adresse de portefeuille contrôlée par l'opérateur du malware.

Principaux voleurs/stealers en fonction du nombre de rapports clients uniques en 2023

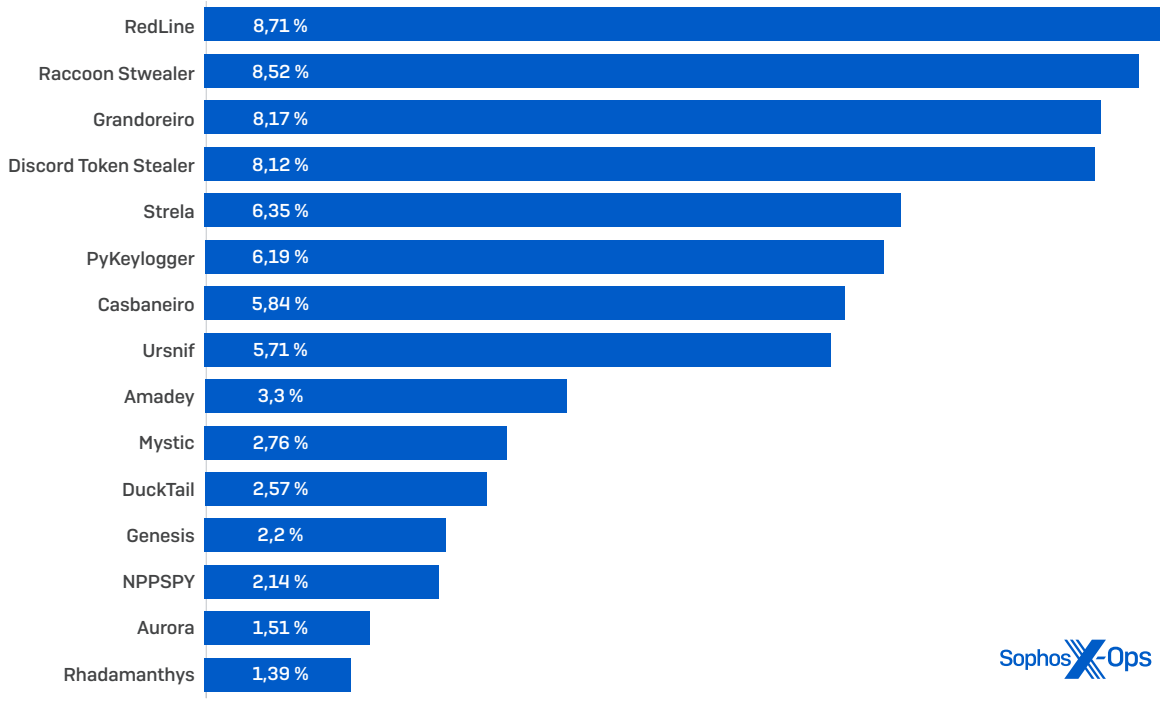


Figure 6 : Détections de malwares de type voleurs d'informations (information stealer) en 2023, tirées de la télémétrie des clients Sophos dans le Dataset des SophosLabs

Sophos a constaté une augmentation du nombre de malwares volant des informations et ciblant macOS, et nous pensons que cette tendance va se poursuivre. Ces stealers, dont certains sont vendus sur des forums underground et sur des chaînes Telegram, à des prix pouvant atteindre 3 000 dollars, peuvent collecter des données système, des données de navigateur et des portefeuilles Crypto.

Les ransomwares restent une menace majeure pour les petites entreprises

Même si les ransomwares ne représentent qu'un pourcentage relativement faible du total des détections de malwares, ils restent ceux qui ont la plus grande importance en termes d'impact. Les ransomwares touchent les entreprises de toutes tailles et dans tous secteurs, mais nous avons constaté qu'ils touchaient le plus souvent les petites et moyennes entreprises. En 2021, la Task Force sur les ransomwares de l'Institute for Security and Technology a constaté que 70 % des attaques de ransomware ciblaient les petites entreprises. Même si le nombre total d'attaques de ransomware varie d'une année sur l'autre, ce pourcentage se reflète au niveau de nos propres mesures.

Le ransomware LockBit était la principale menace dans les cas de sécurité impliquant des petites entreprises et traités par Sophos Incident Response en 2023. LockBit est un Ransomware-as-a-Service, utilisé par un certain nombre d'affiliées, et a été le ransomware le plus déployé en 2022 selon la figure 7.

Incidents de ransomware ayant ciblé les petites entreprises et traités par Sophos Incident Response en 2023

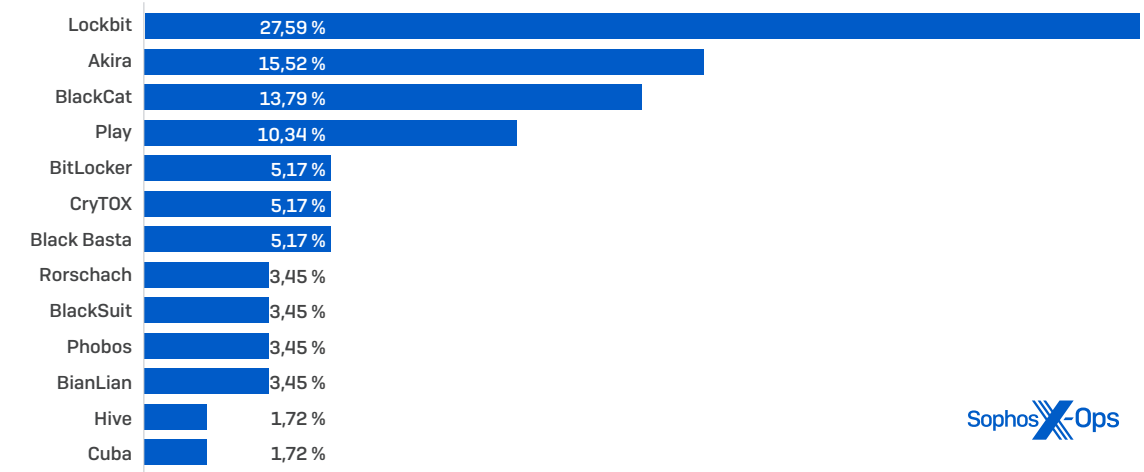


Figure 7 : Une répartition des auteurs de ransomware à l'origine des incidents ayant ciblé les petites entreprises et que Sophos Incident Response a investigués en 2023 ; ces chiffres reflètent le Dataset des interventions manuelles menées par l'équipe IR chez les clients qui n'avaient généralement pas mis en place de protections Sophos auparavant.

Principaux ransomwares en fonction du nombre de rapports clients uniques en 2023

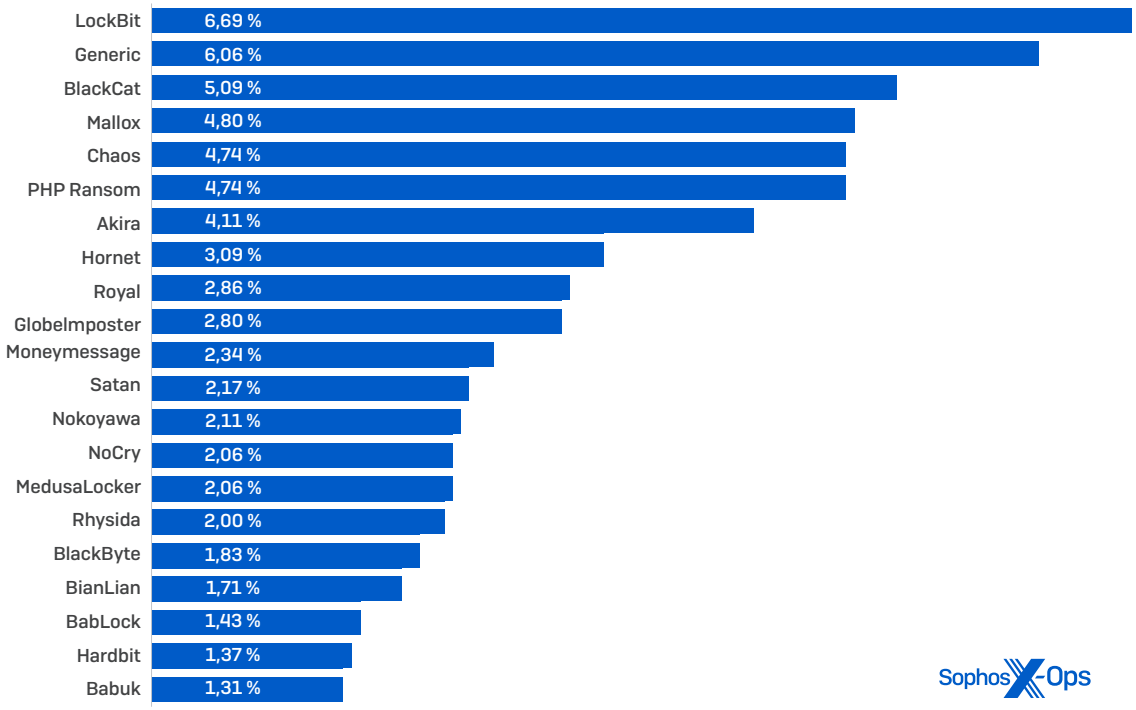


Figure 8 : Les principales tentatives de déploiement de ransomwares détectées par le logiciel de protection Endpoint de Sophos et présentes dans notre Dataset Labs chez tous les clients en 2023, en pourcentage de tous les ransomwares détectés ; « Generic » représente plusieurs types de ransomware détectés avec une signature 'fourre-tout' qui n'ont pas été détectés avec une autre désignation.

LockBit est le malware le plus observé par le groupe MDR (Managed Detection and Response) de Sophos (qui comprend l'équipe IR et ses données), avec près de trois fois plus d'incidents dans lesquels le déploiement d'un ransomware a été tenté en comparaison avec son homologue le plus proche, Akira.

Principales marques de malware observées lors des incidents traités par l'équipe MDR en 2023, en fonction du nombre d'incidents

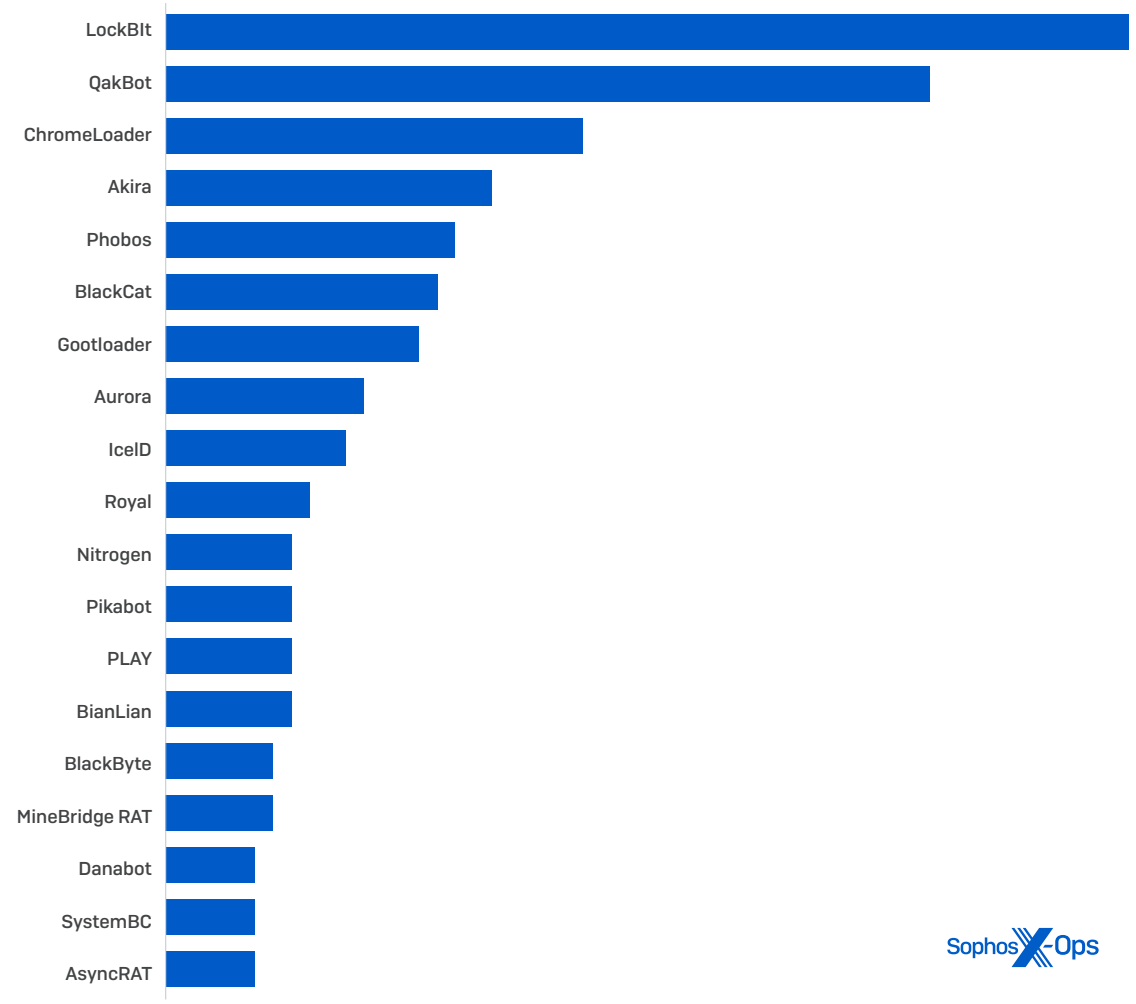


Figure 9 : Il s'agit du malware le plus souvent observé lors d'incidents pris en charge par Sophos Managed Detection and Response en 2023, comme le montre le Dataset MDR. Notez les différences entre ce graphique et celui de la figure 8. Outre la domination de LockBit en 2023, nous constatons qu'il existe un large éventail de familles de ransomware qui tentent d'infecter les systèmes. Seule une partie d'entre elles, un sous-ensemble, atteint le stade qui nécessite une assistance/intervention manuelle en matière de MDR. Notons également que plus d'une détection peut se produire au cours d'un seul incident.

Au fil de l'année 2023, nous avons constaté une augmentation de l'exécution à distance de ransomwares, en utilisant un appareil non géré sur les réseaux des entreprises pour tenter de chiffrer des fichiers sur d'autres systèmes via l'accès aux fichiers réseau.

Incidents de ransomware distant, 2022-2023

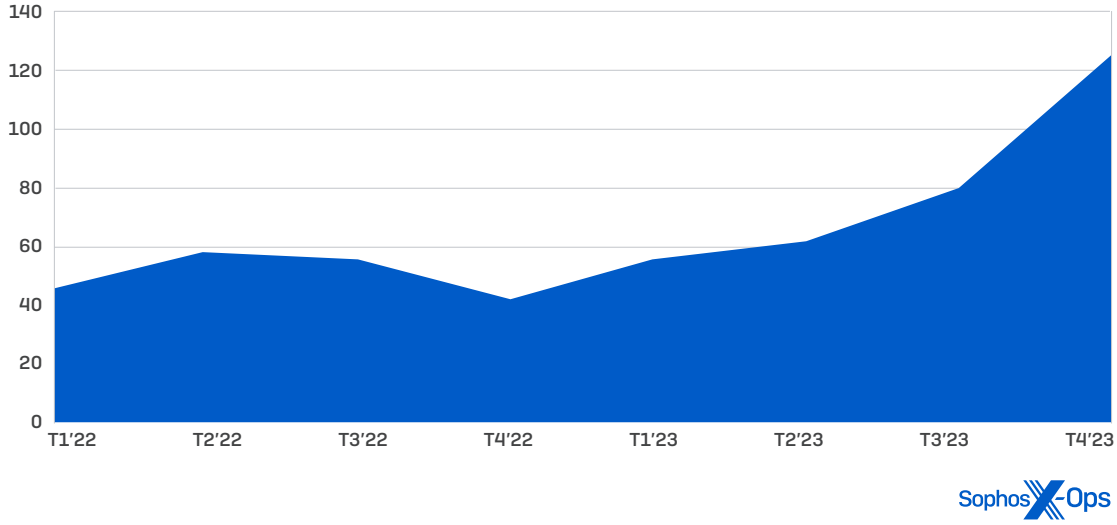


Figure 10 : Les données de télémétrie client recueillies par Sophos au cours des deux dernières années montrent une augmentation globale du volume de tentatives d'attaques de ransomware impliquant des ransomwares à distance : un problème persistant qui a pris un nouvel élan, en particulier au cours du second semestre 2023.

Ces types d'attaque parviennent à pénétrer au sein de l'organisation en exploitant des serveurs, des appareils personnels et des appareils réseau non protégés qui se connectent aux réseaux Windows des entreprises concernées. Une défense en profondeur peut empêcher ces attaques de mettre hors ligne des entreprises entières, mais elles peuvent néanmoins rendre les organisations vulnérables à la perte et au vol de données.

Les systèmes Windows ne sont pas les seuls visés par les ransomwares. De plus en plus, les développeurs de ransomwares et d'autres malwares utilisent des langages multiplateformes pour créer des versions ciblant les systèmes d'exploitation macOS et Linux ainsi que les plateformes matérielles prises en charge. En février 2023, une variante Linux du ransomware ClOp a été découverte, elle avait été utilisée lors d'une attaque de décembre 2022 ; depuis lors, Sophos a observé des versions Leaked du ransomware LockBit ciblant macOS sur le propre processeur d'Apple et Linux au niveau de plusieurs plateformes matérielles.

Cybercrime as a Service

Le monde des malwares continue d'être dominé par ce que nous appelons le « Malware as a Service » (MaaS) : l'utilisation de frameworks de diffusion de malwares fournis par les cybercriminels via des marketplaces underground à d'autres cybercriminels. Mais un certain nombre d'améliorations de la sécurité des plateformes associées à des opérations de démantèlement menées par le secteur et les forces de l'ordre a eu un certain impact sur la typologie du paysage MaaS.

Après une décennie de domination dans le domaine de la diffusion des malwares, Emotet a perdu son statut depuis son démantèlement par Europol et Eurojust en janvier 2021. Il en va de même, dans une moindre mesure, pour Qakbot et Trickbot, après avoir été perturbés par les forces de l'ordre en août 2023. Bien que Qakbot soit revenu sous une forme limitée, il a été largement supplanté par ses successeurs potentiels : Pikabot et DarkGate.

Rien de tout cela n'a eu d'impact sur le vénérable cheval de Troie d'accès à distance (RAT) AgentTesla, qui s'est hissé au sommet du marché MaaS. Il s'agit du malware le plus souvent détecté par la protection endpoint en 2023 au niveau de l'ensemble des systèmes endpoint (en dehors des fichiers .LNK malveillants génériques et des malwares obfusqués), et il représentait 51 % des détections du framework de distribution de malware dans notre télémétrie l'année dernière.

Principaux frameworks de diffusion de ransomware en fonction du nombre de rapports clients uniques en 2023

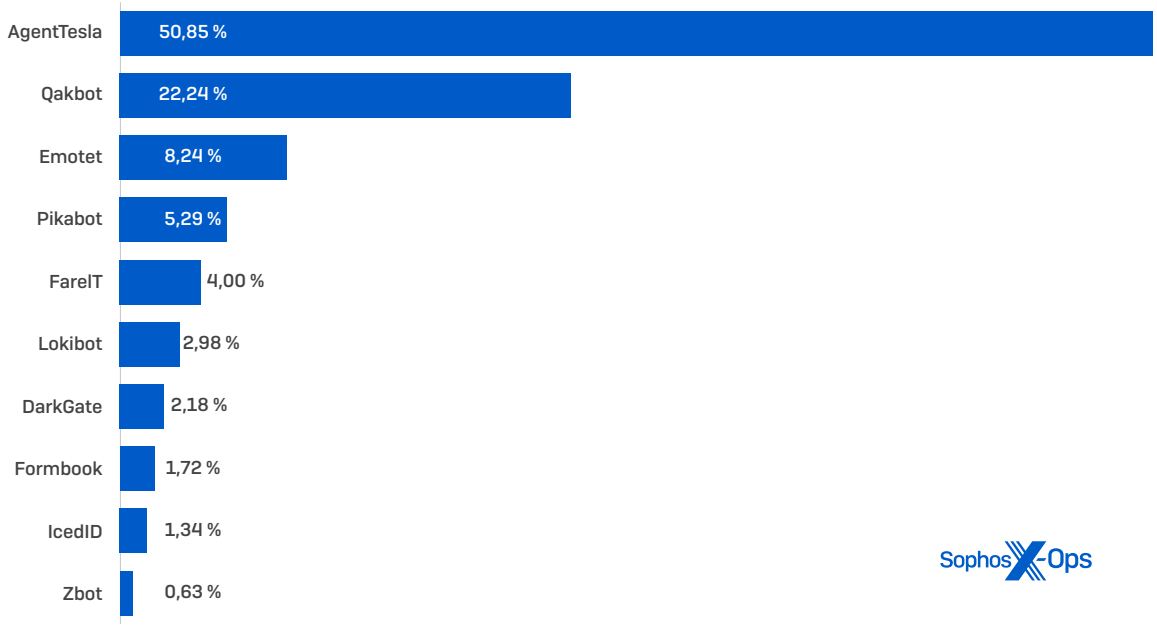


Figure 11 : Une analyse des frameworks courants utilisés pour diffuser des malwares par les attaquants, en fonction du nombre de détections endpoint sur les réseaux des clients protégés par Sophos. Les chiffres de Qakbot représentent les détections antérieures à l'opération internationale lancée par les forces de l'ordre en août 2023 contre son infrastructure.

Trouver une autre voie de diffusion

Les attaques de malware nécessitent une certaine forme d'accès initial. Généralement, cela implique l'un des éléments suivants :

- Emails de phishing
- Pièces jointes malveillantes
- Exploitations de vulnérabilités dans les systèmes d'exploitation et les applications
- Fausses mises à jour logicielles
- Exploitation et abus du RDP (Remote Desktop Protocol).
- Vol d'identifiants

Par le passé, les opérateurs MaaS s'appuyaient largement sur des pièces jointes malveillantes pour l'implantation initiale. Mais les modifications apportées à la sécurité par défaut de la plateforme Microsoft Office ont eu un impact sur le marché du MaaS. Alors que Microsoft a déployé des modifications dans les applications Office qui bloquent par défaut les macros VBA (Visual Basic For Applications) dans les documents téléchargés depuis Internet, il est devenu plus difficile pour les opérateurs MaaS d'utiliser leur méthode préférée de diffusion des malwares.

Cette tendance a conduit à certains changements dans les types de pièce jointe utilisés par les attaquants : les attaquants se sont tournés presque exclusivement vers les pièces jointes au format PDF. Il y a cependant quelques exceptions notables. Début 2023, les opérateurs de Qakbot se sont mis à utiliser des documents OneNote malveillants pour contourner les modifications au niveau de Excel et Word, dissimulant ainsi dans le document des liens vers des fichiers de script activés lorsque la cible clique sur un bouton au niveau du fichier bloc-notes OneNote.

En 2021, nous avons constaté que les offres de type « malware-as-a-service » telles que la backdoor RaccoonStealer avaient commencé à s'appuyer fortement sur la diffusion Web, utilisant souvent des astuces SEO (Search Engine Optimization) pour inciter les cibles à télécharger leurs malwares. En 2022, nous avons vu un « SEO poisoning » utilisé dans le cadre d'une campagne de vol d'informations SolarMarker. Ces méthodes sont à nouveau en hausse et les acteurs qui les développent sont devenus plus sophistiqués.

Nous avons vu plusieurs campagnes notables utilisant de la publicité Web malveillante et du SEO poisoning pour cibler les victimes. L'une d'entre elles était le fait d'un groupe d'activités utilisant un malware que nous avons surnommé « Nitrogen » ; le groupe a utilisé des publicités Google et Bing liées à des mots-clés spécifiques pour inciter les cibles à télécharger un programme d'installation de logiciel à partir d'un faux site Web, en utilisant l'image de marque d'un développeur de logiciel légitime. La même technique de malvertising a été utilisée avec un certain nombre d'autres malwares d'accès initial, notamment l'agent botnet Pikabot, le voleur d'informations (information stealer) IcedID et les familles de malware backdoor Gozi.

Dans le cas de Nitrogen, les publicités ciblaient les généralistes IT, proposant des téléchargements comprenant des logiciels de bureau à distance bien connus pour l'assistance aux utilisateurs finaux et des utilitaires de transfert de fichiers sécurisés. Les installateurs fournissaient bien ce qui avait été annoncé, mais ils venaient accompagnés d'une charge virale Python malveillante qui, une fois lancée par l'installateur, déployait un shell distant Meterpreter et des balises (beacons) Cobalt Strike. D'après les conclusions d'autres chercheurs, il s'agissait probablement de la première étape d'une attaque de ransomware BlackCat.

Des outils « à double usage »

Cobalt Strike, le kit logiciel bien connu de « simulation d'adversaires et d'opérations red team », continue d'être utilisé par de vrais adversaires ainsi que par des organismes légitimes de tests de sécurité. Mais ce n'est en aucun cas le seul logiciel développé commercialement utilisé par les attaquants, et ce n'est plus aujourd'hui le plus courant.

Les outils de bureau à distance, les outils de compression de fichiers, les logiciels de transfert de fichiers courants, d'autres utilitaires et les outils de test de sécurité open source sont couramment utilisés par les attaquants pour les mêmes raisons que les petites et moyennes entreprises : à savoir faciliter leur travail.

Sophos MDR a observé que ces utilitaires, que nous appelons « outils à double usage », étaient utilisés de manière abusive par des attaquants dans le cadre du processus de post-exploitation :

- **Découverte :** Advanced IP Scanner, NetScan, PCHunter, HRSword
- **Persistance :** Anydesk, ScreenConnect, DWAgent
- **Accès aux identifiants :** Mimikatz, Veeam Credential Dumper, LaZagne
- **Mouvement latéral :** PsExec, Impacket, PuTTy
- **Collecte et exfiltration de données :** FileZilla, winscp, megasync, Rclone, WinRar, 7zip

AnyDesk et PsExec ont tous deux été vus dans plus d'incidents par Sophos MDR que Cobalt Strike, comme indiqué ci-dessous :

Principaux outils à « double usage » observés lors des incidents traités par l'équipe MDR en 2023, en fonction du nombre d'incidents

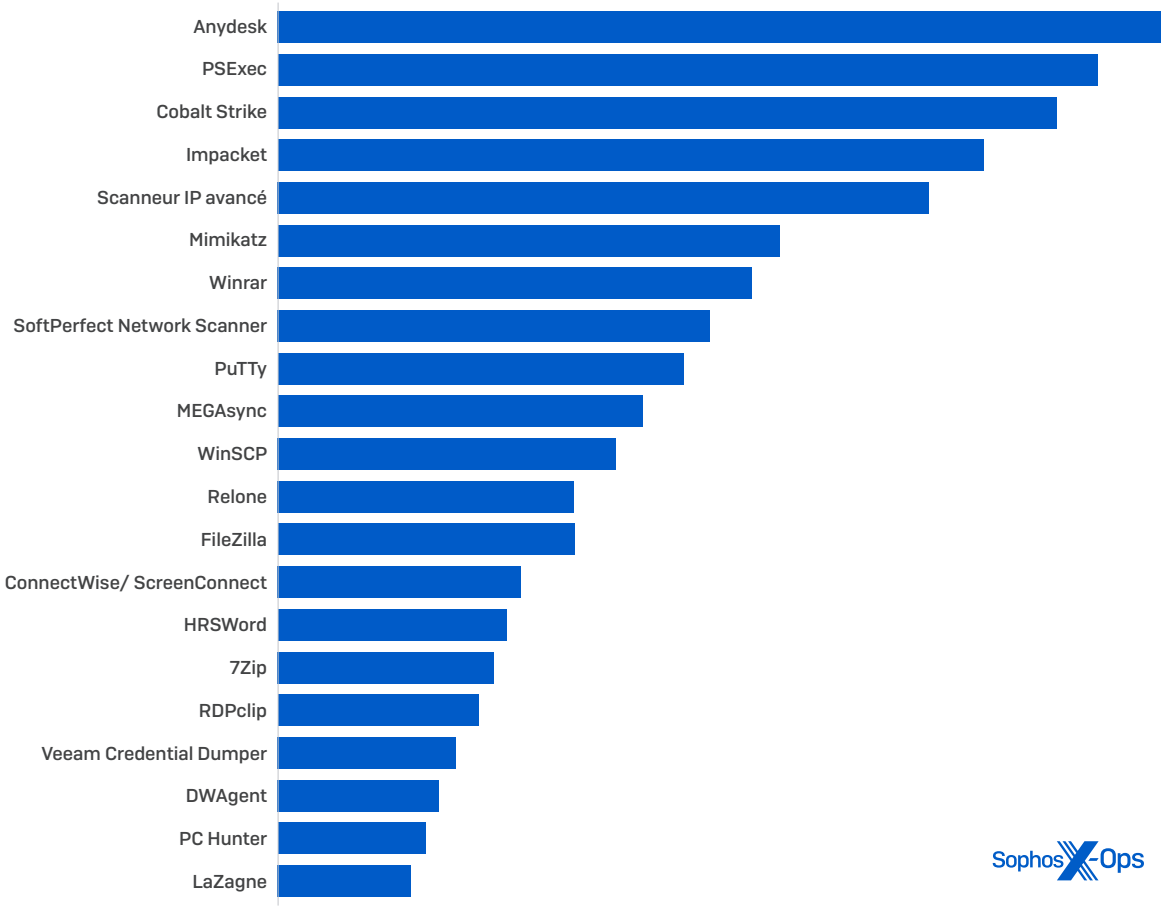


Figure 12 : Les outils à « double usage » les plus fréquemment rencontrés dans les incidents de cybersécurité, en fonction du nombre de cas où chacun a été observé dans le Dataset Sophos MDR

Attaques zero-day et attaques non zero-day

En mai 2023, Progress Software a signalé une vulnérabilité au niveau de sa plateforme de transfert de fichiers managée et sécurisée, et largement utilisée, à savoir MOVEit, dont une qui avait été exploitée par au moins un ensemble d'acteurs malveillants. Plus tard, cette dernière révélera plusieurs vulnérabilités supplémentaires et publiera plusieurs correctifs pour les traiter.

Les attaques ont été attribuées à des acteurs associés au groupe de ransomware Cl0p. Les attaquants ont utilisé cette vulnérabilité pour déployer des Web shells sur les interfaces Web publiques des serveurs MOVEit Transfer : des Web shells qui, dans certains cas, ont persisté après que les vulnérabilités ont été corrigées par les clients Progress

MOVEit n'était que l'une des nombreuses vulnérabilités « zero day » qui ont défié les défenseurs en 2023. GoAnywhere, un autre système de transfert de fichiers managé, a révélé en février une vulnérabilité qu'un autre groupe affilié à CL0p a tenté d'exploiter. Ensuite, une vulnérabilité d'exécution de code à distance dans les produits logiciels de serveur d'impression PaperCut MF et NG a été exploitée par le groupe de ransomware Bl00dy en mars et avril, après avoir été signalée aux développeurs en janvier.

Dans certains cas, ces vulnérabilités ne peuvent tout simplement pas être corrigées. Par exemple, une vulnérabilité dans les appliances Barracuda Email Security Gateway, découverte en juin, était si grave qu'elle n'a pas pu être corrigée et a nécessité le remplacement complet des appliances physiques ou virtuelles. Un groupe malveillant chinois a continué d'exploiter les appareils vulnérables jusqu'à la fin de l'année 2023.

Il n'est pas nécessaire que les vulnérabilités des logiciels et des appareils soient nouvelles pour être exploitées par des attaquants. Les acteurs malveillants recherchent fréquemment des logiciels qui ne sont plus pris en charge, tels que les anciens pare-feu réseau et les logiciels de serveur Web, sachant qu'aucun correctif ne sera disponible.

Attaques de la supply chain et malwares signés numériquement

Les petites entreprises doivent également se préoccuper de la sécurité des services dont elles dépendent pour gérer leur activité et leur infrastructure informatique. Les attaques contre la supply chain ne concernent pas uniquement les acteurs de type État-nation ; nous avons vu les attaques contre les MSP (Managed Service Providers) devenir un élément durable des playbooks de ransomware.

En 2023, Sophos MDR a traité cinq cas dans lesquels des clients de type petites entreprises ont été attaqués via un exploit au niveau du logiciel de surveillance et de gestion à distance (RMM : Remote Monitoring and Management) d'un fournisseur de services. Les attaquants ont utilisé l'agent NetSolutions RMM exécuté sur les ordinateurs des organisations ciblées pour créer de nouveaux comptes administratifs sur les réseaux en question, puis ont déployé des outils commerciaux de bureau à distance, d'exploration de réseau et de déploiement de logiciels. Dans deux des cas, les attaquants ont réussi à déployer le ransomware LockBit.

Il est difficile de se défendre contre les attaques qui exploitent des logiciels fiables, en particulier lorsque ces logiciels donnent aux attaquants la possibilité de désactiver la protection endpoint. Les petites entreprises et les fournisseurs de services qui les assistent doivent surveiller les alertes indiquant que la protection endpoint a été désactivée sur les systèmes de leurs réseaux, car cela peut indiquer qu'un attaquant a obtenu un accès privilégié via une vulnérabilité de la supply chain ou via d'autres logiciels qui, à première vue, peuvent sembler légitimes.

Par exemple, en 2023, nous avons constaté un certain nombre de cas d'attaquants utilisant des pilotes de noyau (kernel) vulnérables issus de logiciels plus anciens qui possédaient encore des signatures numériques valides, et de malwares intentionnellement créés utilisant des signatures numériques obtenues frauduleusement, notamment des pilotes de noyau malveillants signés numériquement via le programme WHCP (Windows Hardware Compatibility Publisher) de Microsoft : l'objectif était d'échapper à la détection par les outils de sécurité et d'exécuter du code qui désactivait la protection contre les malwares.

Les pilotes du noyau fonctionnent à un niveau très bas dans le système d'exploitation et sont généralement chargés avant les autres logiciels lors du démarrage du système d'exploitation. Cela signifie qu'ils s'exécutent dans de nombreux cas avant que le logiciel de sécurité ne puisse démarrer. Les signatures numériques agissent comme un permis de conduire, pour ainsi dire : dans toutes les versions de Windows depuis Windows 10 version 1607, les pilotes du noyau doivent avoir une signature numérique valide, sinon les systèmes d'exploitation Windows avec Secure Boot activé ne les chargeront pas.

En décembre 2022, Sophos a informé Microsoft de la découverte de pilotes noyau malveillants contenant des certificats signés par Microsoft. Étant donné que ces pilotes disposaient de certificats signés par Microsoft, ils étaient par défaut acceptés comme logiciels inoffensifs, leur permettant ainsi d'être installés, puis de désactiver la protection endpoint sur les systèmes où ils se trouvaient. Microsoft a publié un avis de sécurité, puis a révoqué en juillet 2023 une multitude de certificats de pilotes malveillantsobtenus via WHCP.

Il n'est pas nécessaire que les pilotes soient malveillants pour être exploités. Nous avons vu de nombreux cas de pilotes et d'autres bibliothèques de versions anciennes, voire actuelles, de produits logiciels exploités via des attaques par "chargement latéral (side load)" des malwares dans la mémoire système.

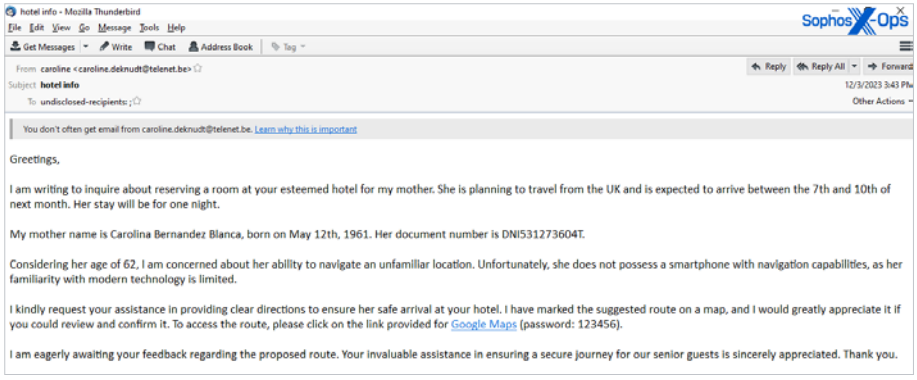
Nous avons également vu les propres pilotes de Microsoft utilisés dans des attaques. Une version vulnérable d'un pilote pour l'utilitaire Process Explorer de Microsoft a été utilisée à plusieurs reprises par des opérateurs de ransomware dans le but de désactiver les produits de protection endpoint ; en avril 2023, nous avons signalé un outil dénommé « AuKill » qui a utilisé ce pilote dans plusieurs attaques visant à déployer les ransomwares Medusa Locker et LockBit.

Parfois, nous avons de la chance et identifions les pilotes vulnérables avant qu'ils ne puissent être exploités. En juillet, les règles comportementales de Sophos ont été déclenchées par l'activité d'un pilote concernant le produit de sécurité d'une autre entreprise. L'alerte a été déclenchée par un test de simulation d'attaquant réalisé par un client, mais notre investigation de l'événement a révélé trois vulnérabilités que nous avons signalées à l'éditeur du logiciel et qui ont ensuite été corrigées.

Les spammeurs repoussent les limites de l'ingénierie sociale

Les emails peuvent sembler être une méthode de communication à l'ancienne à l'ère des discussions mobiles chiffrées de bout en bout, mais les spammeurs ne semblent pas en avoir conscience (ou du moins s'en soucier). Alors que la méthode traditionnelle du BEC consistant simplement à se faire passer pour un employé et à demander à un autre employé d'envoyer des cartes cadeaux est toujours d'actualité, les spammeurs sont devenus beaucoup plus créatifs.

Au cours de l'année écoulée, l'équipe sécurité de la messagerie de Sophos a découvert une multitude de nouvelles astuces et techniques d'ingénierie sociale conçues pour échapper aux contrôles de messagerie conventionnels. Les messages dans lesquels l'attaquant envoie par email une pièce jointe ou un lien au hasard sont désormais dépassés : Les spammeurs les plus efficaces sont plus susceptibles d'initier d'abord une conversation, puis de se lancer ensuite dans les emails de suivi.


hotel info - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address Book Tag

From caroline <caroline.deknudt@telenet.be>

Subject hotel info

To undisclosed-recipients:;

Reply Reply All Forward

12/3/2023 3:43 PM

Other Actions

You don't often get email from caroline.deknudt@telenet.be. Learn why this is important

Greetings,

I am writing to inquire about reserving a room at your esteemed hotel for my mother. She is planning to travel from the UK and is expected to arrive between the 7th and 10th of next month. Her stay will be for one night.

My mother name is Carolina Bernandez Blanca, born on May 12th, 1961. Her document number is DNI531273604T.

Considering her age of 62, I am concerned about her ability to navigate an unfamiliar location. Unfortunately, she does not possess a smartphone with navigation capabilities, as her familiarity with modern technology is limited.

I kindly request your assistance in providing clear directions to ensure her safe arrival at your hotel. I have marked the suggested route on a map, and I would greatly appreciate it if you could review and confirm it. To access the route, please click on the link provided for Google Maps (password: 123456).

I am eagerly awaiting your feedback regarding the proposed route. Your invaluable assistance in ensuring a secure journey for our senior guests is sincerely appreciated. Thank you.

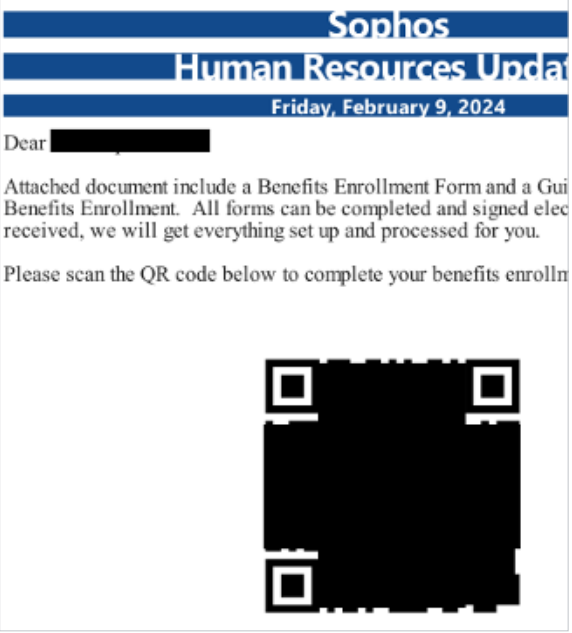
Figure 13 : Ce n'est qu'après avoir reçu une réponse de la cible que le spammeur envoie à celle-ci un email contenant un lien vers un fichier malveillant dans une archive Zip protégée par mot de passe.

Nous avons observé cette technique lors d'attaques au cours desquelles des spammeurs se faisaient passer pour des employés de sociétés de transport et appelaient ensuite des clients professionnels en leur demandant d'ouvrir un email piégé. Nous avons également vu des spammeurs envoyer dans un premier temps une sollicitation commerciale ou une réclamation, lors d'attaques ciblant divers secteurs en 2023, suivis d'un lien permettant de télécharger un fichier dissimulé et piégé après que l'entreprise a répondu au premier email.

La prévention traditionnelle contre les spams implique des processus inspectant le contenu des messages et prenant des décisions basées sur ce dernier. Les spammeurs ont expérimenté diverses méthodes pour remplacer le contenu textuel de leurs messages par des images intégrées : Parfois, les images semblaient être un message écrit, tandis que d'autres expérimentaient l'utilisation de QR codes ou d'images qui ressemblaient à des factures (avec des numéros de téléphone que les attaquants incitaient les victimes à appeler) pour échapper à la détection.

Figure 14 : Une pièce jointe PDF provenant d'un message spam intègre une vignette floue et illisible d'une facture et un lien vers un site Web hébergeant une charge virale malveillante.

Les pièces jointes malveillantes ont même repoussé les limites, les PDF piégés faisant un retour en force, renvoyant vers des scripts ou des sites malveillants, utilisant parfois des QR codes intégrés. La famille de malware Qakbot a largement abusé du format de document OneNote de Microsoft, le bloc-notes (ou fichier .one), pour diffuser des charges virales avant d'être arrêtée plus tard dans l'année lors d'une opération de démantèlement coordonnée. Les attaquants ont également utilisé le format de fichier MSIX : un type de format de fichier archive utilisé par Microsoft pour diffuser des applications via l'App Store de Windows, afin de contourner la détection.


Sophos

Human Resources Updat

Friday, February 9, 2024

Dear [redacted]

Attached document include a Benefits Enrollment Form and a Gui
Benefits Enrollment. All forms can be completed and signed elec
received, we will get everything set up and processed for you.

Please scan the QR code below to complete your benefits enrolln

Figure 15 A : Une pièce jointe PDF malveillante, envoyée par email aux employés de Sophos, intègre une image de QR code qui mène à une page de phishing

Les attaquants ont également abusé des services de Microsoft : À la fin de l'année, environ 15 % du total des spams bloqués par Sophos avaient été envoyés via des comptes de messagerie créés dans le système de messagerie de Microsoft, dédié aux entreprises, onmicrosoft.com.

Malwares mobiles et menaces utilisant l'ingénierie sociale

Les petites entreprises dépendent fortement des appareils mobiles dans le cadre de systèmes d'information approuvés ou ad hoc. Les messages texte, les applications de messagerie et de communication, ainsi que les applications se connectant aux services Cloud, notamment les applications/terminaux de paiement (point of sale) mobiles, sont des systèmes essentiels aux activités des petites entreprises distribuées. Les cybercriminels le savent et continuent de trouver des moyens de cibler les utilisateurs d'appareils mobiles pour accéder aux données ou frauder.

Les spywares et les « bankers » constituent un groupe de malwares Android particulièrement préoccupants et qui, selon nous, continueront à représenter une véritable menace. Les spywares sont utilisés pour collecter des données sur le téléphone et abonnent parfois même l'utilisateur de l'appareil à des services payants pour bénéficier d'un gain financier direct. Ils collectent des données personnelles, notamment des messages SMS et les logs d'appel de l'appareil concerné, qui sont ensuite vendues à des fraudeurs ou utilisées à des fins de chantage, ou bien les deux. Il y a eu plusieurs cas où des victimes se sont suicidées suite à des menaces émanant d'opérateurs de spyware.

Ces applications mobiles malveillantes sont diffusées de plusieurs manières. Elles peuvent se faire passer pour des applications légitimes sur l'app store Google Play ou bien sur les sites d'app store tiers, souvent comme des applications de prêt mobile. Elles sont également diffusées via des liens envoyés par messages texte.

Les bankers sont des malwares qui ciblent les applications financières, notamment les portefeuilles de crypto-monnaie, pour récolter des données de compte afin d'accéder aux fonds, en utilisant les autorisations d'accessibilité pour mettre la main sur les données sensibles du téléphone.

Ensuite, il y a le phénomène « pig butchering », ou sha zhu pan. Nous avons commencé à traquer les fausses applications sur les plateformes iOS et Android liées à une forme d'arnaque que nous avons d'abord appelée « CryptoRom » début 2021, et depuis les escroqueries sont devenues de plus en plus sophistiquées.

Les réseaux cybercriminels qui déploient ces escroqueries, lesquelles sont souvent exploitées à partir de structures frauduleuses où travaillent des personnes qui ont pour l'essentiel été kidnappées par le cybercrime organisé, ont volé des milliards de dollars à des victimes du monde entier et se concentrent souvent sur des personnes liées à de petites entreprises. En 2023, une petite banque du Kansas a fait faillite et a été prise en charge par la FDIC après que le PDG de la banque a envoyé plus de 12 millions de dollars de dépôts à des fraudeurs dans le but de récupérer les fonds qu'il aurait perdus dans l'une de ces escroqueries. Cet exemple tragique montre à quel point une arnaque habituellement observée dans la vie privée d'un individu peut avoir des ramifications et un impact sur les petites entreprises.

Les fraudeurs du Sha Zhu Pan attirent leurs victimes via les sites de réseaux sociaux, les applications de rencontres, d'autres applications et plateformes communautaires, voire même par le biais de messages SMS « accidentels ». Ils ont tendance à cibler les personnes qui recherchent une relation amoureuse ou amicale. Après avoir orienté la cible vers une application de messagerie sécurisée telle que WhatsApp ou Telegram, ils gagnent leur confiance et leur présentent alors une idée lucrative dont ils prétendent avoir une connaissance approfondie, et qui implique généralement la crypto-monnaie.

Au cours de l'année écoulée, nous avons vu les fausses applications utilisées par ces escroqueries se frayer un chemin dans les App Store Google Play et iOS. Ils échappent à la vérification de sécurité de l'app store en question en se présentant comme une application inoffensive jusqu'à la fin du processus d'examen, puis modifient le contenu à distance pour se transformer en une fausse application de trading crypto. Toute crypto-monnaie déposée via ces applications est immédiatement récupérée par les escrocs.

Récemment, nous avons également vu ces escroqueries adopter une tactique utilisant un autre style d'arnaque crypto et qui n'impliquait aucune fausse application : elles utilisaient plutôt la fonctionnalité « Web3 » des applications de portefeuille crypto mobile pour accéder directement aux portefeuilles créés par les victimes. Nous avons identifié des centaines de domaines associés à ces variantes « DeFi (Decentralized Finance) mining » de sha zhu pan, et comme pour les fausses applications que nous identifions, nous continuons à les signaler et à travailler sans relâche pour les faire supprimer.

Conclusions

Les petites entreprises sont la cible d'une multitude de menaces, et la sophistication de ces dernières est souvent comparable à celle utilisée pour attaquer les grandes entreprises et les gouvernements. Même si les sommes d'argent qui peuvent être volées sont inférieures à celles disponibles dans une entreprise plus grande, les cybercriminels seront toujours heureux de voler ce que vous avez et de compenser ensuite en jouant sur le volume.

Les syndicats cybercriminels partent du principe que les petites entreprises sont moins bien défendues et qu'elles n'ont pas déployé d'outils modernes et sophistiqués pour protéger leurs utilisateurs et leurs actifs. La clé pour réussir à se défendre contre ces menaces est de prouver que leurs hypothèses sont fausses : Formez votre personnel, déployez l'authentification multifacteur sur tous les actifs externes, les serveurs de correctifs et les appliances réseau, et ce de manière hautement prioritaire et envisagez de migrer les actifs difficiles à gérer comme les serveurs Microsoft Exchange vers des plateformes de messagerie SaaS.

Selon le rapport, la principale différence lors d'une cyberattaque entre une entreprise qui subira des effets dévastateurs et une autre qui s'en sortira avec des répercussions mineures est le temps de réponse. Disposer d'experts en sécurité pour surveiller et répondre 24 h/24 et 7 j/7 est l'enjeu d'une défense efficace en 2024. Disposer d'une sécurité efficace n'est pas impossible ; il vous suffit, tout simplement, d'adopter une approche globale et de mettre en œuvre des défenses à plusieurs niveaux pour vous donner le temps de répondre tout en minimisant les dommages.

Sophos France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

24-04-11 FR (NP)

SOPHOS