Version française

ThreatDown™
Powered by Malwarebytes

2024
État des malwares

Des malwares aux menaces, le guide de défense complet

Contenu

1. Pourquoi vous avez besoin d'un guide

Des malwares aux menaces

Le cybercrime est un secteur florissant, et très bien organisé, un véritable miroir à plusieurs milliards de dollars de l'économie licite dont il se nourrit. Son écosystème est composé de véritables chaînes d'approvisionnement sur lesquelles s'égrainent des organisations spécialisées, telles que courtiers en accès et vendeurs de logiciels malveillants. Il dispose de publicités, de noms de marques, de services RH, de systèmes de primes et élit même des « employés du mois ».

Et à l'instar des entreprises légales, le cybercrime s'est doté d'une série d'outils efficaces. Observez les ordinateurs fixes aux États-Unis ou en Europe, vous y verrez des logiciels qui étaient déjà connus il y a 15 ans comme Microsoft Windows, Office et les navigateurs web.

La cybercriminalité, elle, possède des infostealers (virus dérobeurs d'informations), des outils d'hameçonnage et des ransomwares. Tout comme Windows et Office, ces outils sont matures et efficaces, et depuis des années, seules de légères améliorations sont apportées au fil de leurs itérations. Par conséquent, l'innovation au sein du cybercrime se tourne de plus en plus du côté des tactiques employées : les avancées se concentrent sur la manière de réussir les attaques, plus que sur ce que les malwares sont capables de faire.

À propos de ce rapport

Pour refléter la transition des malwares aux menaces, nous faisons encore une fois évoluer notre rapport État des malwares. Nous avons demandé à nos experts à quoi les équipes informatiques aux effectifs parfois réduits allaient devoir faire attention dans l'année à venir. Ceux-ci ont répertorié six menaces représentatives des tactiques de cybercrime les plus dangereuses repérées sur Windows, Mac et Android. Cette liste n'est pas exhaustive, mais si vous êtes équipé pour traiter ces menaces, alors vous serez en bonne place pour affronter tout ce que l'écosystème du cybercrime vous réserve.

Les malwares sont toujours aussi dangereux, mais lorsqu'ils sont utilisés, ils représentent simplement un maillon dans une chaîne d'attaque composée de menaces multiples et variées. Les équipes informatiques et de sécurité font désormais face à des attaques LOTL (***Living Off The Land***), des adversaires actifs, des exploits zero-day, des compromissions de comptes, de l'ingénierie sociale, et toute une palette d'autres menaces qui n'entrent pas dans la définition classique des malwares.

Dans ce contexte, les budgets alloués à la sécurité s'effritent, tandis que les services informatiques et de sécurité, qui ne disposent pas de ressources illimitées, se battent contre des environnements toujours plus complexes. Cette dynamique ne fonctionnera tout simplement pas en 2024. Pour contenir le fléau des adversaires 24 h/24, 7 j/7, et compte tenu de la pénurie de ressources qualifiées en sécurité et de la prolifération de produits de sécurité à l'intégration douteuse, une autre approche va être nécessaire en matière de sécurité.

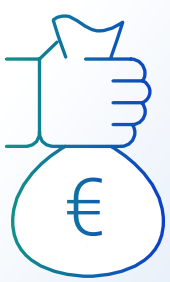
Une cyberdéfense efficace reposera sur des professionnels de sécurité compétents et expérimentés capables d'identifier et d'investiguer jour et nuit les anomalies, et qui soient soutenus par des logiciels de sécurité sophistiqués, groupés et faciles à utiliser pour démanteler non seulement les malwares, mais également les cybermenaces de tout type.

2. Leçons apprises en 2023

Les principaux changements

En ce début d'année 2024, les ransomwares restent la cybermenace la plus importante pour les entreprises. Plein aux as, l'écosystème des ransomwares a connu un emballement en 2023 tout en continuant à faire évoluer ses tactiques.

Le nombre d'attaques connues a augmenté de 47 % en France, la moyenne mondiale des demandes de rançon a grimpé de façon vertigineuse et la plus grosse demande de rançon de l'année a atteint le montant astronomique de 74 millions d'euros, exigé par le groupe LockBit suite à l'attaque contre Royal Mail, opérateur postal au Royaume-Uni.



74 M €

La plus grosse demande de rançon connue en 2023, émanant de LockBit à l'encontre de Royal Mail, s'élevait à 74 millions d'euros.

En rupture totale avec les normes établies, le groupe de ransomware CL0P a tiré parti de deux vulnérabilités zero-day pour mener deux campagnes de vol de données automatisées dévastatrices qui ont affecté des milliers d'organisations peu méfiantes en quelques jours à peine. L'approche de CL0P lui a permis de dépasser de façon significative même les groupes de Ransomware-as-a-Service les plus chevronnés, récoltant 92 millions d'euros dans cette opération. Ses tactiques semblent vouées à être reproduites par d'autres en 2024.

Des groupes moins sophistiqués ont misé sur les difficultés persistantes que rencontrent certaines organisations pour appliquer efficacement les correctifs. En février, la plus grosse attaque de ransomware connue hors Windows a compromis des milliers de serveurs VMware ESXi obsolètes en se servant d'une vulnérabilité vieille de deux ans. En mai, MalasLocker est sorti de nulle part, en prenant de court tous les autres groupes de ransomwares avec une campagne visant des serveurs Zimbra qui n'avaient pas reçu de correctif depuis six mois.

Les cybermenaces ont aussi évolué ailleurs

Suite à la décision de Microsoft de bloquer les macros dans les documents téléchargés sur Internet, les criminels ont diversifié leurs tactiques, notamment en faisant montre d'un regain d'intérêt pour la publicité malveillante (le malvertising). Sont apparues d'innombrables campagnes imitant des marques telles qu'Amazon, Zoom et WebEx pour distribuer des malwares Windows et Mac par le biais de publicités et de sites web plus vrais que nature, sans que les vendeurs de publicités semblent en mesure de pouvoir les arrêter.

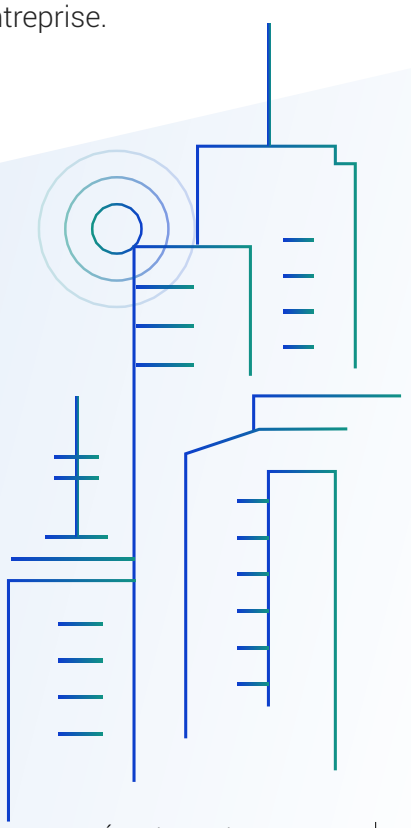
Tout n'a cependant pas été tout rose pour les cybercriminels. En août, le département de la Justice des États-Unis a annoncé le démantèlement du tristement célèbre malware

Qakbot, qu'il a décrit comme étant « le plus grand coup financier et technique porté par les États-Unis à l'encontre d'une infrastructure de botnet dirigée par des cybercriminels pour mener des attaques de ransomwares, des fraudes financières et d'autres activités cybercriminelles.

Dans une démarche que ne manqueront sans doute pas de suivre attentivement les autres pays, la Loi pour la sécurité en ligne du Royaume-Uni (***Online Safety Act***) tente de remettre en question le ***statu quo*** des entreprises de réseaux sociaux et de messageries. Cette loi a globalement été interprétée comme une demande faite aux entreprises de repérer les contenus illégaux dans les messages des utilisateurs, ce qui les aurait contraintes à débloquer le chiffrement de bout en bout (E2EE). En réponse, WhatsApp et Signal ont menacé de quitter le Royaume-Uni si la loi était adoptée. Un tour de passe-passe politique a permis à toutes les parties prenantes de garder la face, mais le libellé controversé de la loi n'a pas été modifié, et pourrait donc toujours être utilisé pour remettre en cause le chiffrement.

Menacé par endroits, le chiffrement a ailleurs permis d'améliorer significativement la sécurité. Google et Microsoft ont tenu leur promesse de faire la part belle aux clés d'accès, qui sont basées sur le chiffrement, remplacent les mots de passe et ne peuvent être volées, devinées, craquées ou hameçonnées. Ces entreprises accompagnent activement la mise en place des clés d'accès et encouragent vivement les utilisateurs à les adopter, une victoire conséquente pour la sécurité, et une dynamique qui devrait se poursuivre fortement en 2024.

L'évolution des cybermenaces au cours de l'année écoulée exige des entreprises qu'elles-mêmes fassent évoluer leur défense. Les chapitres qui suivent détaillent tout ce que vous devez savoir sur les cybermenaces les plus importantes, ainsi que les conseils, techniques et technologies dont vous avez besoin pour protéger votre entreprise.



Les ransomwares restent la menace criminelle la plus redoutable pour les entreprises.

3. Les ransomwares dirigés contre les grandes entreprises

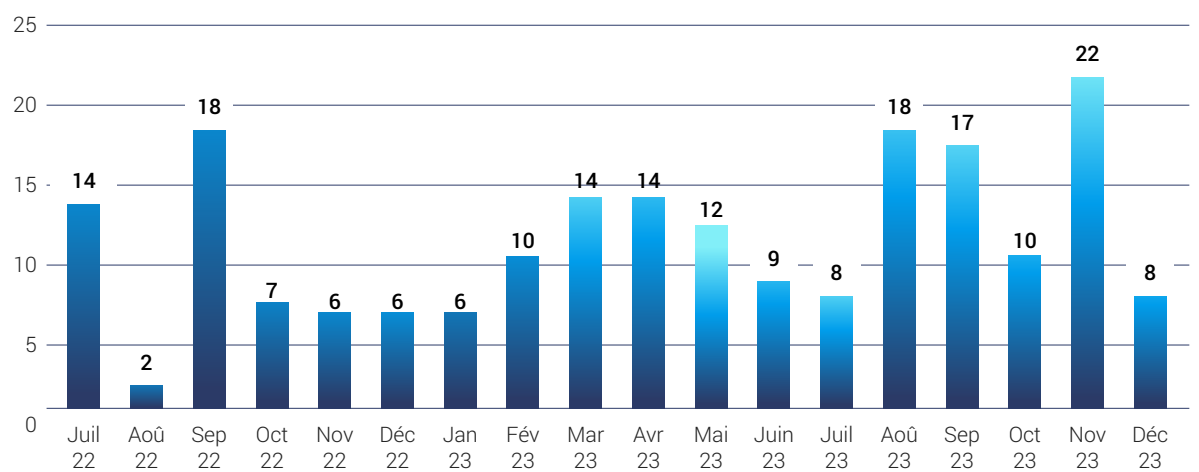
Depuis leur arrivée en 2018, les ransomwares à l'encontre du « gros gibier » (comprenez les attaques contre de grands comptes, « ***big game*** » en anglais) représentent la cybermenace la plus sérieuse pour les entreprises dans le monde. Ces attaques visent à extorquer de grosses sommes d'argent aux organisations en prenant leurs données en otage, soit en les chiffrant, soit en menaçant de les faire fuiter, voire les deux.

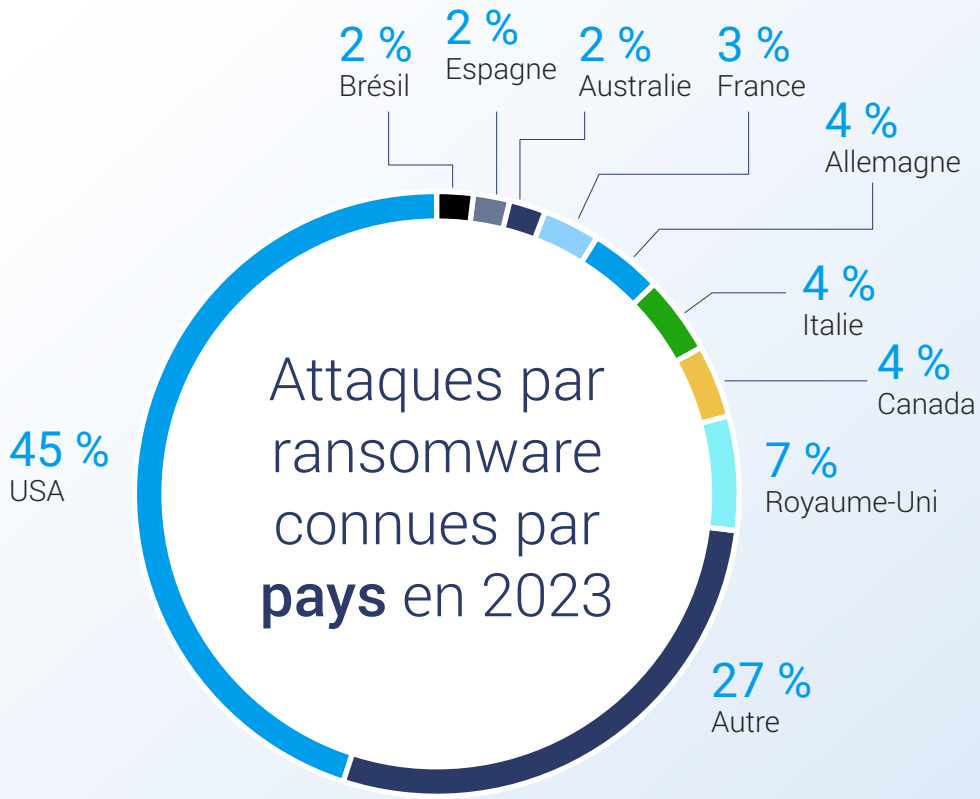
Malheureusement, le problème des attaques de ransomwares contre de grands comptes a sérieusement empiré en 2023, le nombre d'attaques connues ayant augmenté de 68 % dans le monde et de 47 % en France. Dans le monde, le montant moyen des rançons a atteint 740 000 $ au premier trimestre de l'année, d'après Coveware, une société de réponse aux attaques par ransomware, qui a également indiqué que le total des paiements de rançons en 2023 avoisinera le milliard de dollars.

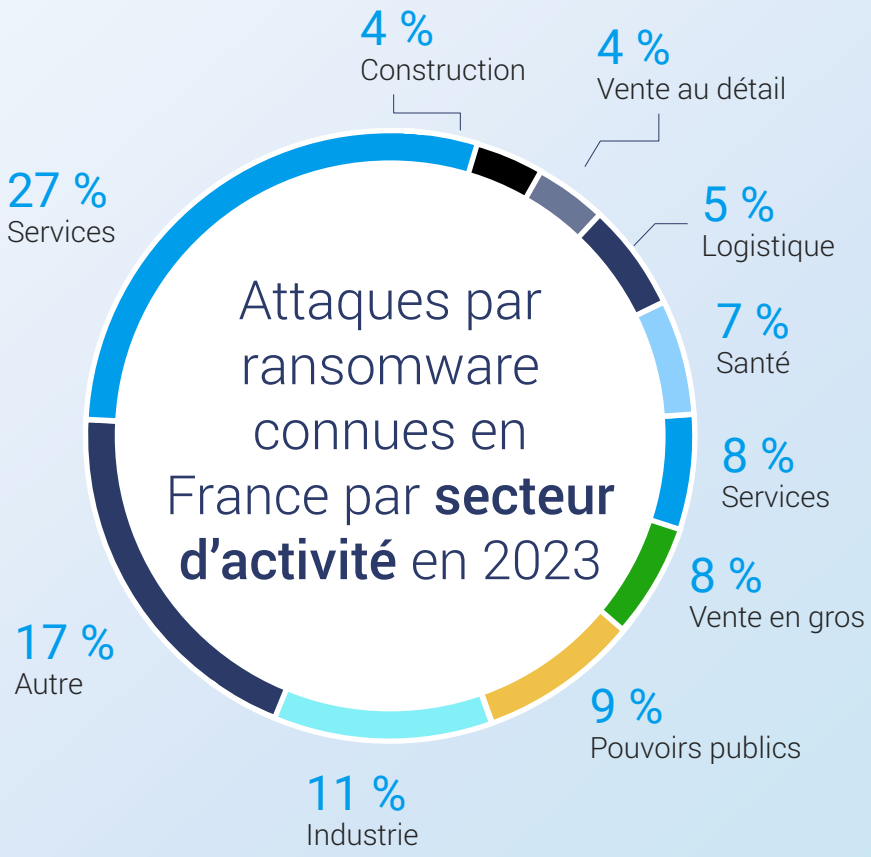
47 % Le nombre d'attaques par ransomware connues en France a augmenté de 47 % en 2023.

3 % La France représente 3 % de toutes les attaques par ransomware en 2023.

Attaques par ransomware connues en France par mois




Attaques par ransomware connues par **pays** en 2023
2 % Brésil
2 % Espagne
2 % Australie
3 % France
4 % Allemagne
4 % Italie
4 % Canada
7 % Royaume-Uni
27 % Autre
45 % USA


Attaques par ransomware connues en France par **secteur d'activité** en 2023
4 % Construction
4 % Vente au détail
5 % Logistique
7 % Santé
8 % Services
8 % Vente en gros
9 % Pouvoirs publics
11 % Industrie
17 % Autre
27 % Services

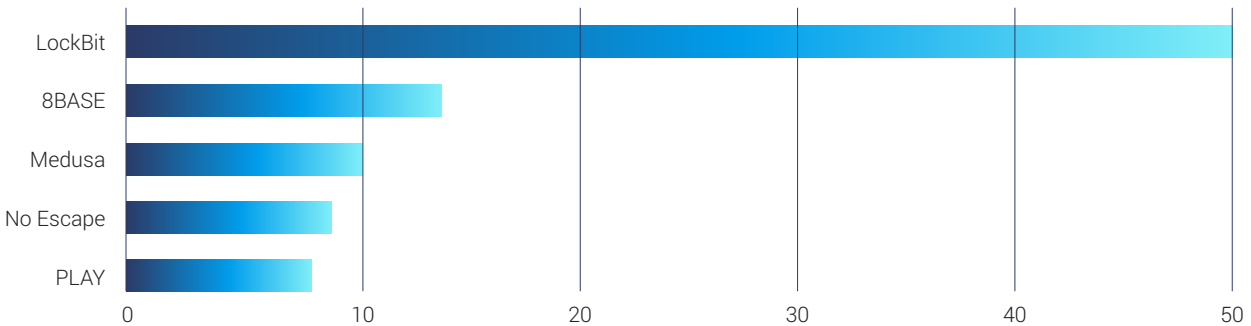
La préparation d'une attaque par ransomware peut prendre des semaines, le temps pour les pirates de s'introduire dans leur cible, d'acquérir le rôle d'administrateurs, d'explorer leur environnement, voler des données et diffuser ensuite leur ransomware dans tous les recoins du réseau. Lorsque l'attaque finit par être déclenchée, c'est au moment où la victime est le moins à même de réagir : pendant la nuit, le week-end ou les vacances. Les représentants de la cible et du groupe de ransomware négocient sur un chat du dark web pendant des jours, voire des semaines.

Les attaques contre le « gros gibier » peuvent rapporter très gros, mais demandent beaucoup de travail. La réponse des cybercriminels au problème d'échelle inhérent aux ransomwares dirigés contre les grandes entreprises tient dans le Ransomware-as-a-Service (RaaS), un type de ransomware qui voit généralement se coordonner trois types d'organisations criminelles au sein d'une seule attaque.

Les groupes criminels spécialisés dans l'infiltration des réseaux d'entreprise commencent par s'introduire. Ces groupes malveillants, appelés courtiers d'accès initiaux (ou IAB, ***Initial access broker***), disposent d'une variété de tactiques pour s'introduire dans les entreprises, telles que l'hameçonnage, les chevaux de Troie, la pulvérisation de mots de passe et l'exploitation des vulnérabilités dans une infrastructure avec Internet. Lorsqu'arrive la phase suivante de l'attaque, les courtiers vendent l'accès obtenu à des « filiales »expertes en ransomwares.

Celles-ci représentent des groupes criminels qui exécutent les attaques de ransomware. Plutôt qu'écrire leurs propres ransomwares, ces filiales les achètent auprès d'un vendeur de Ransomware-as-a-Service (RaaS) tel que LockBit, ALPHV ou Play.

Les 5 principaux groupes de ransomwares dirigés contre de grands comptes en France en 2023

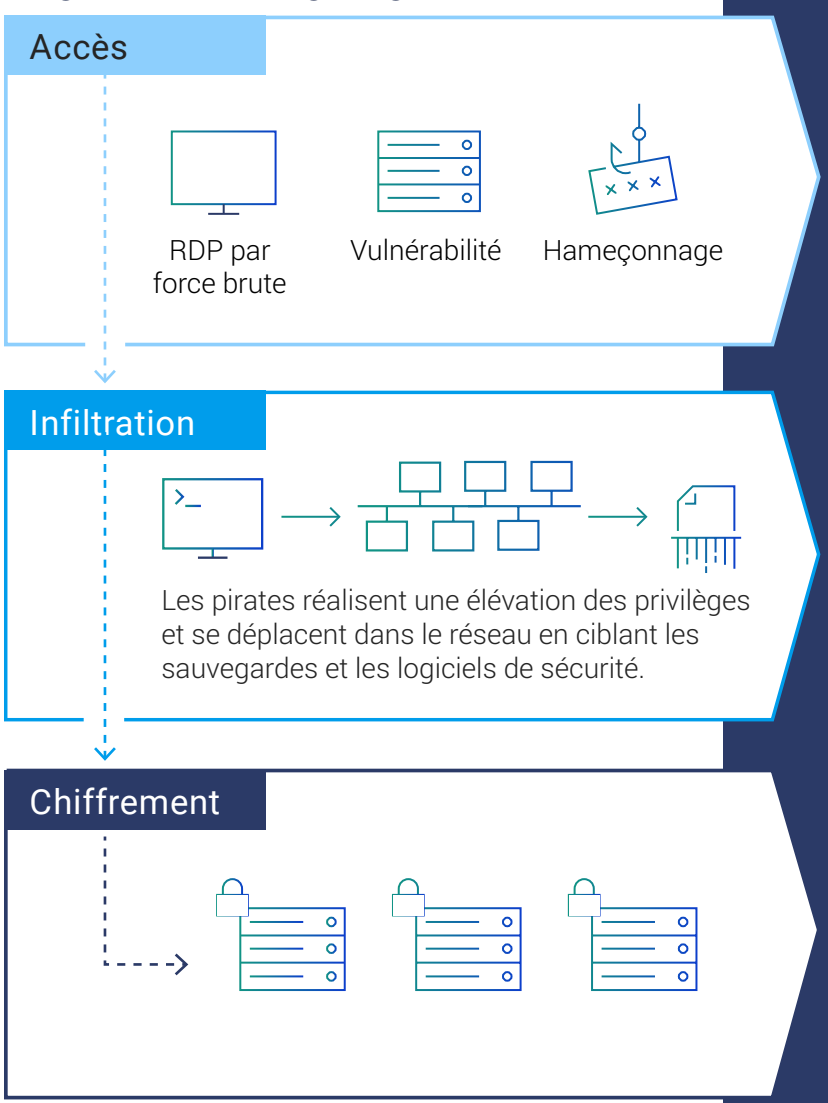


LockBit reste le RaaS le plus utilisé, mais ses concurrents s'en rapprochent.

LockBit est le Raas le plus utilisé au monde, mais aussi le plus couramment observé en France, et de loin, puisqu'il concernait trois fois plus d'attaques que son plus proche concurrent en 2023. Cependant, alors que le nombre total d'attaques LockBit a augmenté par rapport à l'année précédente, la part qu'il occupait dans le nombre d'attaques global est passée de 31 % en 2022 à 22 % en 2023, du fait de la concurrence, autre signe inquiétant de la recrudescence des ransomwares.

Les menaces d'attaques de ransomware contre de grands comptes s'accentuent, et les groupes qui en sont à l'origine sont à la fois déterminés, expérimentés et bien équipés. Se défendre contre ce type de ransomware requiert une approche intégrée de la sécurité, avec une excellente pile de sécurité combinée à des chasseurs de menaces compétents et des spécialistes de la réponse aux incidents.

Phases d'attaque des ransomwares dirigés contre le « gros gibier »



Protection avec ThreatDown

La protection contre la force brute, les fonctions Vulnerability Assessment et Patch Management, la protection contre les exploits et le filtrage des contenus de sites web stoppent différentes formes d'accès.

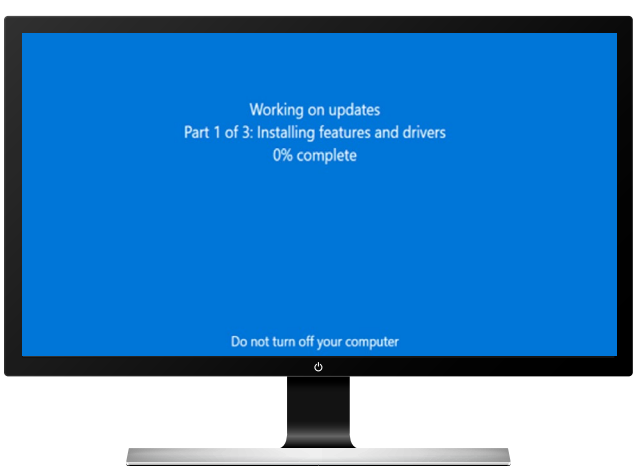
Managed Detection & Response (MDR) identifie les pirates tapis dans votre réseau avant qu'ils lancent des ransomwares ; l'antivirus nouvelle génération, le blocage des applications et la protection contre les exploits empêchent les pirates d'accéder à leurs outils ; le filtrage des contenus de sites web empêche les pirates d'accéder aux serveurs de commande et de contrôle (C&C).

Endpoint Detection & Response (EDR) stoppe les ransomwares ; le Ransomware Rollback récupère les fichiers chiffrés ; Incident Response vous offre la tranquillité d'esprit après une attaque.

4. Le malvertising

Bien que le recours aux publicités malveillantes (malvertising) pour diffuser des malwares ne soit pas nouveau, il a connu en 2023 une recrudescence qui a ciblé les entreprises comme les particuliers. L'intérêt pour cette technique est sûrement né de la décision tardive (mais nécessaire) de Microsoft de bloquer les macros dans les documents téléchargés sur Internet, l'une des voies de distribution de malwares les plus efficaces du cybercrime. Cette technique de diffusion étant désormais révolue, les cybercriminels ont dû innover ailleurs.

Le malvertising emploie souvent des techniques d'ingénierie sociale pour installer des malwares. Les cybercriminels créent des publicités Google Search imitant des marques connues et menant vers des répliques de pages web très réalistes qui trompent les utilisateurs et les amènent à télécharger des malwares.



Un site de malvertising imitant une mise à jour de système Windows.

Bien que Google et d'autres vendeurs de publicités aient lutté contre les créateurs de malvertising tout au long de 2023, les pirates ont su garder une longueur d'avance et contourner systématiquement les contrôles de vérification des publicités toute l'année.

Le malvertising ciblant les particuliers imite par exemple des marques grand public comme Amazon, des logiciels tels que les outils de conversion PDF, ou se sert de sujets populaires comme l'investissement dans les cryptomonnaies. Les entreprises sont quant à elles ciblées par des publicités incitant à télécharger des outils comme Slack, Webex, Zoom et 1Password. En 2023, les cybercriminels ont également visé les départements d'informatique avec de fausses versions d'outils comme Advanced IP Scanner.

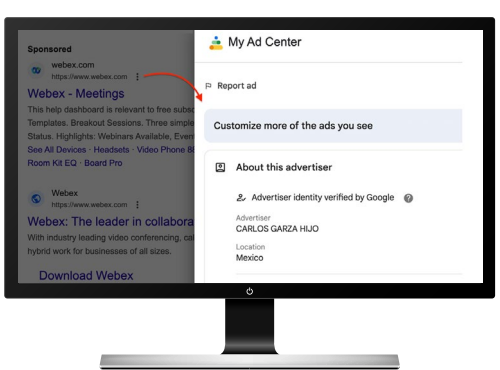
Amazon était la marque la plus usurpée en 2023.

Les publicités et sites web frappent par leur réalisme, et sont généralement plus difficiles à détecter que les e-mails malveillants. Le malvertising utilise également du code sophistiqué de collecte d'empreintes qui permet de déterminer si un visiteur est un bot, tel que le robot d'exploration de Google Search, ou un chercheur en sécurité, afin d'être sûr que seules les victimes potentielles voient les fausses pages, ce qui lui permet de rester tapi dans l'ombre pendant plus longtemps.

Top 5 des marques les plus imitées	
1	Amazon
2	Rufus
3	Weebly
4	NotePad++
5	TradingView

Même si les pages malveillantes sont rapidement identifiées et supprimées, elles sont rapidement remplacées, et il est rare que l'infrastructure qui les sous-tend soit menacée. Ainsi, la chaîne de distribution des malwares n'étant pas affectée, les acteurs malveillants ont pu en 2023 se concentrer sur la sophistication de leurs pages de leurre et de leurs charges utiles de malware.

Ces charges utiles changent à chaque nouvelle campagne, mais on y retrouve des infostealers courants comme IcedID, Aurora Stealer et BatLoader. Ces programmes volent les identifiants sur les navigateurs ou les ordinateurs des utilisateurs, préparant le terrain pour des attaques par ransomware.



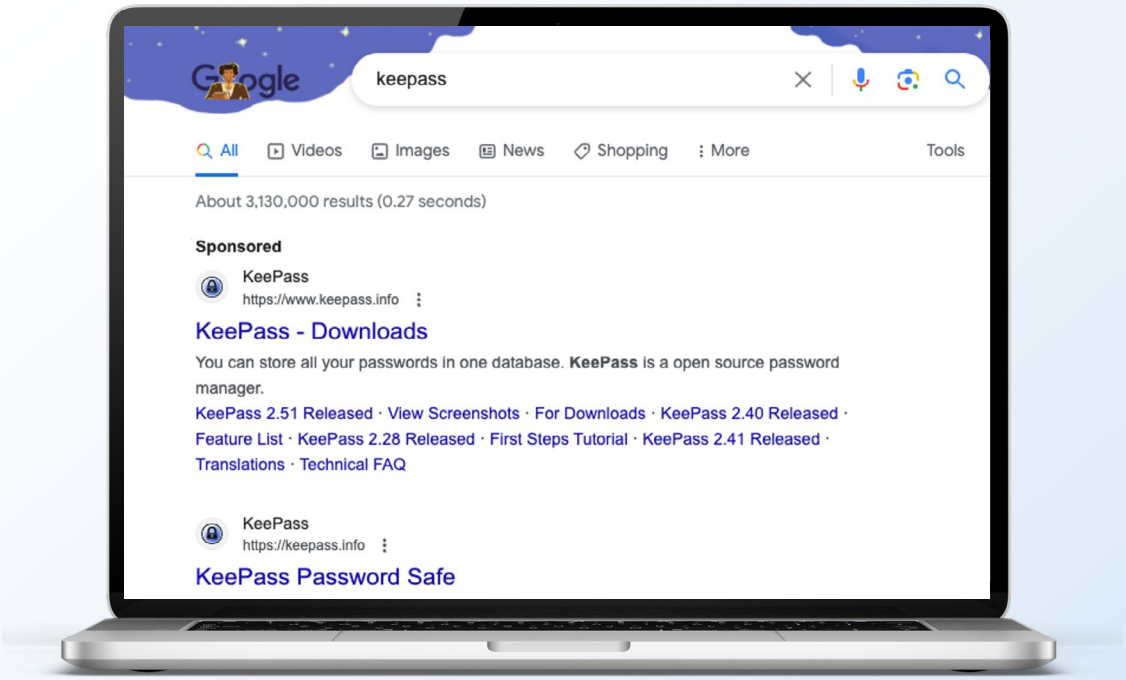
Seule la section relative aux informations sur l'annonceur peut faire penser que cette publicité Webex est fausse.

Top 5 des malwares les plus fréquemment détectés	
1	Aurora Stealer
2	Vidar
3	Redline Stealer
4	BatLoader
5	IcedID

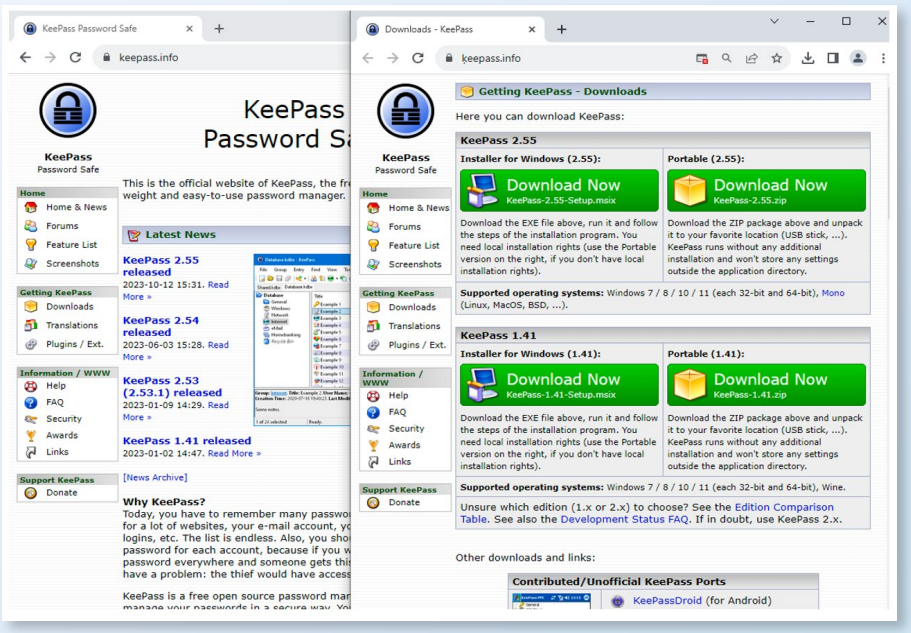
Par exemple, le groupe de ransomware Royal s'est servi d'AnyDesk comme leurre de malvertising pour distribuer BatLoader, utilisé pour déposer une balise Cobalt Strike Beacon qui a servi de précurseur à une attaque par ransomware.

Pour les cybercriminels, le malvertising présente plusieurs avantages par rapport au piège des pièces jointes contenues dans des e-mails malveillants. Les utilisateurs connaissent moins cette technique et savent rarement la détecter. Même lorsque c'est le cas, le format très normé des publicités search ne donne aux utilisateurs que très peu d'éléments à examiner. Ces publicités peuvent en outre cibler des termes de recherche, des zones géographiques et des publics spécifiques, pour que les victimes potentielles ne voient que les campagnes susceptibles d'attirer leur attention.

Top 5 des hôtes les plus piratés	
1	Dropbox
2	Discord
3	4sync
4	GitLab
5	Google



Une publicité malveillante pour le gestionnaire de mots de passe KeePass apparaît comme légitime.

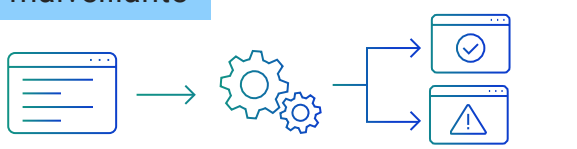


Le véritable site web KeePass (à gauche) et un site de malvertising (à droite)

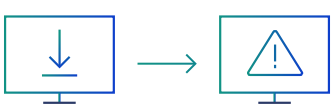
Le malvertising est en plein essor alors que les cybercriminels recherchent des alternatives aux macros pour distribuer des malwares comme des chevaux de Troie, des infostealers ou des ransomwares. Se défendre contre le malvertising implique le filtrage efficace des contenus de sites web pour stopper dans leur élan les sites qui distribuent des malwares, ainsi que la mise en place d'une excellente pile de sécurité comme filet de sécurité contre l'intensification des attaques.

Phases d'attaque du malvertising

Publicité malveillante

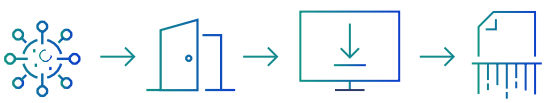


Site web malveillant



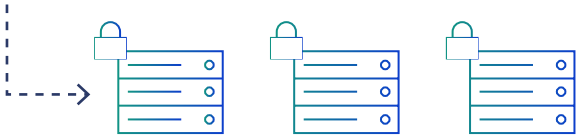
Téléchargement d'un malware imitant un logiciel légitime.

Malwares



Le malware vole des données, télécharge d'autres malwares ou ouvre une voie pour une attaque de ransomware.

Ransomwares



Protection avec ThreatDown

Le filtrage de contenus de sites web bloque les sites de malvertising, l'antivirus de nouvelle génération stoppe les malwares.

Managed Detection & Response (MDR) identifie et investigue les comportements suspects sur votre réseau ; le filtrage des contenus de sites web empêche les pirates d'accéder aux serveurs de commande et de contrôle (C&C).

Endpoint Detection & Response (EDR) stoppe les ransomwares ; le Ransomware Rollback récupère les fichiers chiffrés ; Incident Response vous offre la tranquillité d'esprit après une attaque.

5. Les ransomwares zero-day

Les attaques de ransomware dites au « gros gibier » constituent la cybermenace la plus importante pour les entreprises actuellement, en raison de leur potentiel de déstabilisation et de destruction. En parallèle de cette menace existentielle, on trouve cependant un autre type d'attaque en apparence bénin qui met en exergue le problème d'échelle des ransomwares dirigés contre les grandes entreprises. Limitées, car très dépendantes du travail humain, les attaques et négociations peuvent prendre des semaines, et plus il y a d'attaques, plus les moyens humains sont importants. Ainsi, un grand nombre de cibles potentielles passent entre les mailles du filet.

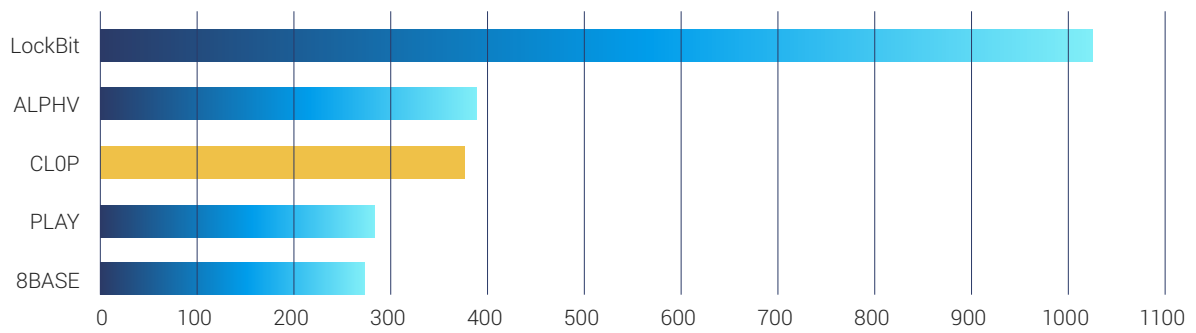
En 2023 cependant, le groupe de ransomware CL0P a vaincu la barrière de l'évolutivité et secoué le monde de la sécurité avec une série de courtes campagnes automatisées ayant frappé simultanément sans qu'elles le sachent des centaines de cibles au moyen d'attaques basées sur des exploits zero-day.

L'usage répété des « zero-day » a marqué un tournant de sophistication pour un groupe de ransomware, et en quelques semaines d'activité, CL0P est devenu le troisième ransomware le plus actif de 2023 pour les attaques dites au « gros gibier », devançant ses rivaux, pourtant actifs tous les mois de l'année.

Étant donné la nature même des vulnérabilités zero-day, les organisations n'ont pas pu appliquer de correctifs de sécurité, ni les techniques traditionnelles de détection de malwares.

Point important à signaler, ces attaques ne reposaient pas sur le chiffrement. Au cours des deux campagnes menées par CL0P, les données des victimes étaient volées et menacées d'être divulguées si aucune rançon n'était payée ; ainsi, aucun déploiement de ransomware n'a été requis.

Le top 5 des groupes de ransomware en 2023 par attaques connues



CL0P s'est hissé à la troisième place du classement des groupes les plus actifs malgré son absence une grande

Entre le 18 et le 31 janvier, CL0P a lancé une attaque automatisée contre des entreprises utilisant l'outil de transfert de fichiers sécurisé GoAnywhere MFT de Fortra. Le groupe s'est servi d'une vulnérabilité zero-day pour créer des comptes non autorisés dans les environnements des victimes, utilisés ensuite pour voler des fichiers et installer des outils malveillants. Des informations concernant 100 et quelques victimes n'ayant pas payé de rançon ont commencé à apparaître sur le site de fuite de données de CL0P en mars.

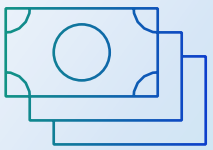
Peu de temps après, le groupe est réapparu avec une campagne encore plus vaste basée sur un zero-day dans le logiciel MOVEit Transfer de Progress. La faille a permis d'installer un shell web, qui a servi à son tour à voler des fichiers dans la base de données du logiciel.

L'exploitation a débuté le 27 mai, alors que Progress Software a alerté ses clients sur l'existence de cette faille le 31 mai. Une semaine plus tard, CL0P revendiquait ces attaques.

En raison de la nature soudaine et violente des attaques, les données volées n'ont pas été aussi soigneusement sélectionnées, et n'étaient pas aussi sensibles qu'elles auraient pu l'être si l'attaque avait été manuelle, ce qui a conduit de nombreuses victimes à refuser de payer une rançon. La société de réponse aux incidents de ransomwares Coveware a toutefois estimé que le groupe était parvenu à combler cette faille en exigeant le paiement de rançons bien supérieures à la moyenne, cette seule campagne ayant rapporté 100 millions de dollars (92 millions d'euros).

92 M €

On estime que CL0P a extorqué entre 75 M $ et 100 M $ (70 M € à 92 M €) grâce à sa campagne zero-day contre MOVEit Transfer.



Par conséquent, en ce début d'année 2024, le groupe CL0P dispose d'une fortune lui permettant de réinvestir dans l'achat ou la découverte de nouveaux zero-day, après avoir démontré que les ransomwares peuvent évoluer bien au-delà des limites qu'on leur connaissait. Il est difficile de s'imaginer que d'autres groupes de ransomware n'essaieront pas de reproduire ces tactiques en 2024.

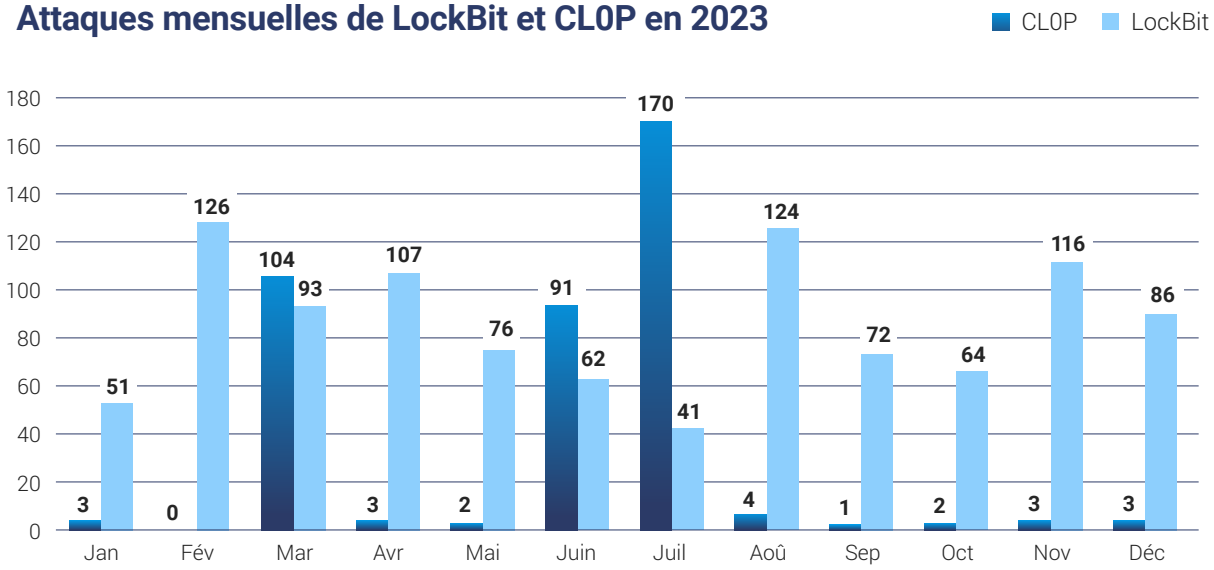
CVE-2023-0669

La première campagne de CL0P a permis d'exploiter CVE-2023-0669, une vulnérabilité d'exécution de code à distance inconnue auparavant dans GoAnywhere MFT.

CVE-2023-34362

La campagne la plus dévastatrice de CL0P exploitait CVE-2023-34362, une vulnérabilité d'injection SQL inconnue auparavant dans MOVEit Transfer.

Attaques mensuelles de LockBit et CL0P en 2023



LockBit s'est montré actif tous les mois de l'année, mais CL0P est devenu l'un de ses principaux rivaux en quelques semaines d'attaque à peine.

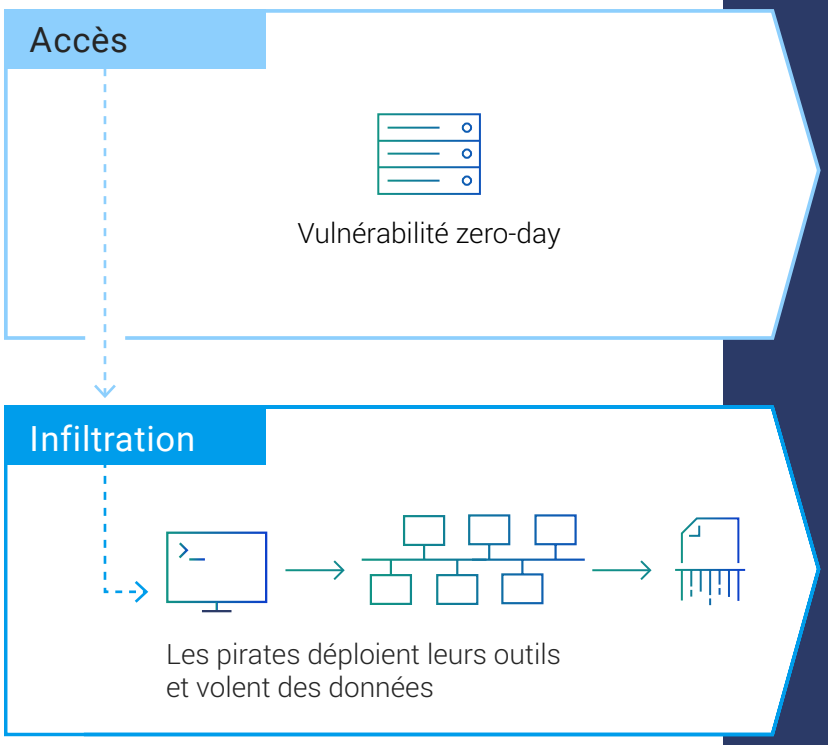
Déclaration sur le site web de CL0P

CL0P a frappé un nombre si important d'entreprises qu'il a dû publier cette déclaration sur son site web pour faciliter les négociations avec les centaines de victimes.

> WE HAVE INFORMATION ON HUNDREDS OF COMPANIES SO OUR DISCUSSION WILL WORK VERY SIMPLE
>
> ***STEP 1 - IF WE DO NOT HEAR FROM YOU UNTIL JUNE 14 2023 WE WILL POST YOUR NAME ON THIS PAGE***
> ***STEP 2 - IF YOU RECEIVE CHAT URL GO THERE AND INTRODUCE YOU***
> ***STEP 3 - OUR TEAM WILL PROVIDE 10% PROOF OF DATA WE HAVE AND PRICE TO DELETE***
> ***STEP 4 - YOU MAY ASK FOR 2-3 FILES RANDOM AS PROOF WE ARE NOT LYING***
> ***STEP 5 - YOU HAVE 3 DAY TO DISCUSS PRICE AND IF NO AGREEMENT YOU CUSTOM PAGE WILL BE CREATED***
> ***STEP 6 - AFTER 7 DAYS ALL YOU DATA WILL START TO BE PUBLICATION***
> ***STEP 7 - YOU CHAT WILL CLOSE AFTER 10 NOT PRODUCTIVE DAY AND DATA WILL BE PUBLISH***

Les ransomwares zero-day représentent une menace émergente qui pose un sérieux danger pour les entreprises. Comme ils reposent sur des vulnérabilités inconnues, ils sont difficiles à détecter. Se défendre contre ce type de ransomware requiert une approche intégrée de la sécurité, avec une excellente pile de sécurité combinée à des chasseurs de menaces compétents capables de détecter et d'investiguer les activités suspectes sur votre réseau.

Phases d'attaque des ransomwares zero-day



Protection avec ThreatDown

Avec Vulnerability Assessment et Patch Management, les systèmes sont protégés rapidement une fois les correctifs disponibles.

Managed Detection & Response (MDR) identifie et investigue les comportements suspects sur votre réseau ; le filtrage des contenus de sites web empêche les pirates d'accéder aux serveurs de commande et de contrôle (C&C) ; l'antivirus nouvelle génération stoppe les backdoors malveillants.

6. Les menaces LOTL

Les techniques de cyberattaque ***Living Off The Land*** (LOTL) consistent pour les criminels à mener des activités malveillantes en se cachant derrière des outils d'administration informatique légitimes comme Powershell, PsExec ou encore Windows Management Instrumentation (WMI).

L'usage malveillant de ces outils peut passer pour une activité de réseau normale pour un œil non averti, mais même pour les équipes informatiques, les attaques LOTL sont extrêmement difficiles à détecter.

Les groupes de ransomware comme LockBit, ALPHV et Royal emploient des techniques LOTL pour passer inaperçus lorsqu'ils préparent des attaques sur des réseaux d'entreprise, telles qu'élévation des privilèges, exécution de commandes, téléchargement de scripts, déplacement latéral, vol de données et déploiement de ransomwares.

Par exemple, les groupes affiliés au ransomware LockBit utilisent PowerShell pour télécharger du code malveillant de Google Sheets, et le planificateur de tâches Windows pour exécuter des VBScripts malveillants. Les filiales d'ALPHV utilisent elles aussi le planificateur de tâches Windows, cette fois pour configurer des stratégies de groupe (GPO, Group Policy Objects) malveillantes. Le groupe de ransomware Royal utilise quant à lui le service Volume Shadow Copy de Windows pour supprimer les sauvegardes des instantanés de Windows et ainsi saper le travail de récupération.

L'intérêt pour les attaques LOTL est grand au sein de la cybercriminalité. Des gangs de vol de données et des groupes de menaces persistantes avancées (APT) peuvent très bien n'exécuter aucun malware et utiliser des techniques LOTL pour rester tapis dans l'ombre pendant des années, tandis que des cybercriminels de tous bords se délectent d'outils d'accès à distance comme RDP et AnyDesk, car ils offrent un potentiel de contrôle énorme sans paraître suspects.

Pour se défendre contre les attaques LOTL, les équipes informatiques et de sécurité ont besoin de comprendre en profondeur leur environnement de sorte à pouvoir repérer les anomalies, telles que des outils administratifs inhabituels (ou des outils habituels entre des mains inconnues), des motifs étranges d'utilisation des données ou des horaires d'activité suspects.

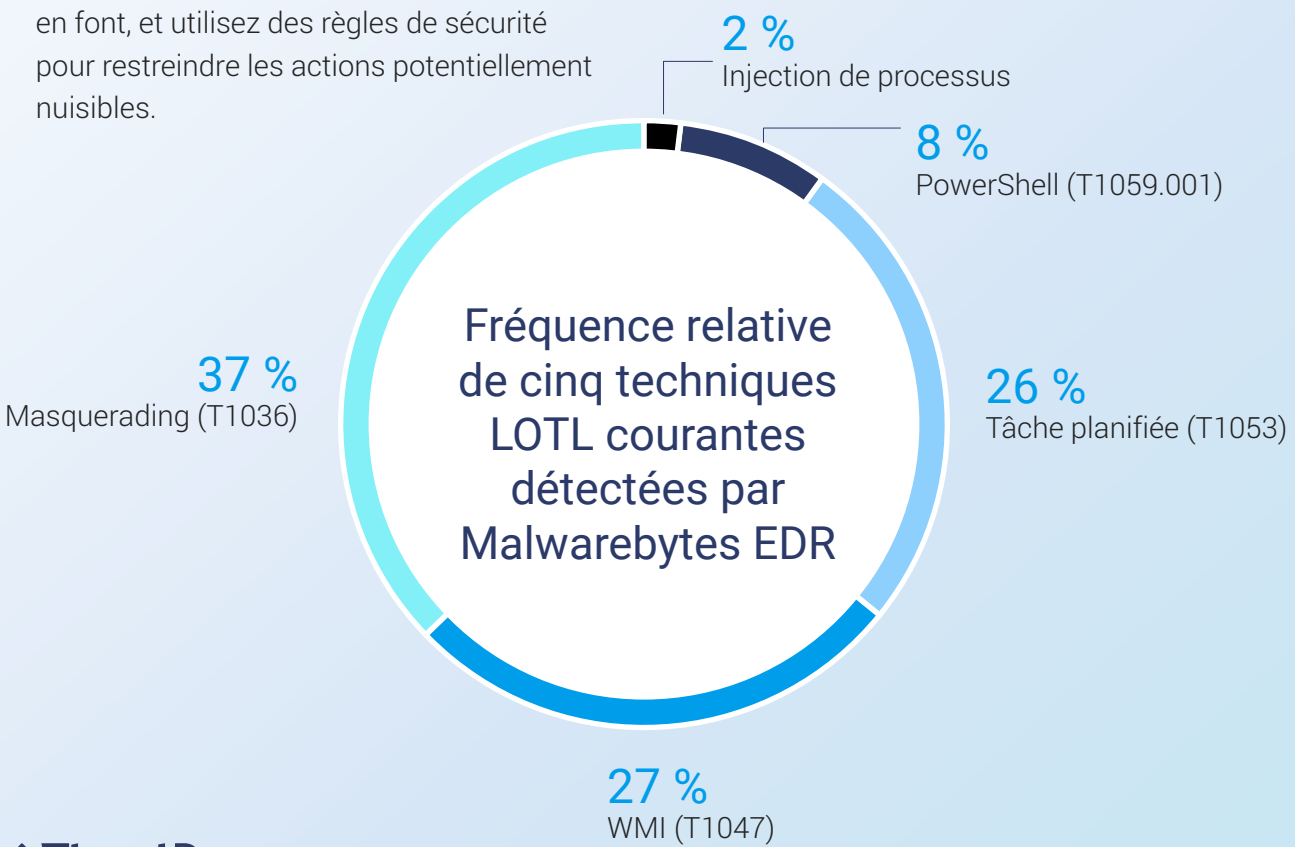
> « Pour détecter efficacement les attaques LOTL, il est essentiel de comprendre l'environnement. Armés de cette base, les analystes en sécurité peuvent identifier les anomalies ou des exceptions qui peuvent ne pas être malveillantes en soi, mais qui sortent de l'ordinaire. »
>
> **Hiep Hinh**
> Analyste MDR en chef, Malwarebytes

Se défendre contre les attaques LOTL

- **Utilisez le MDR** afin que des analystes humains experts détectent 24 h/24, 7 j/7 les motifs inhabituels, signes de compromission ou connexions sur vos terminaux.
- **Utilisez les flux de renseignement sur les menaces** pour affiner la surveillance et être capable de repérer les techniques d'attaque et les indicateurs de compromission les plus récents.
- **Implémentez des outils de surveillance avancés** focalisés sur la détection des comportements inhabituels des utilisateurs ou des systèmes.
- **Limitez l'accès aux outils couramment détournés** aux utilisateurs qui en ont vraiment besoin, surveillez l'utilisation qu'ils en font, et utilisez des règles de sécurité pour restreindre les actions potentiellement nuisibles.

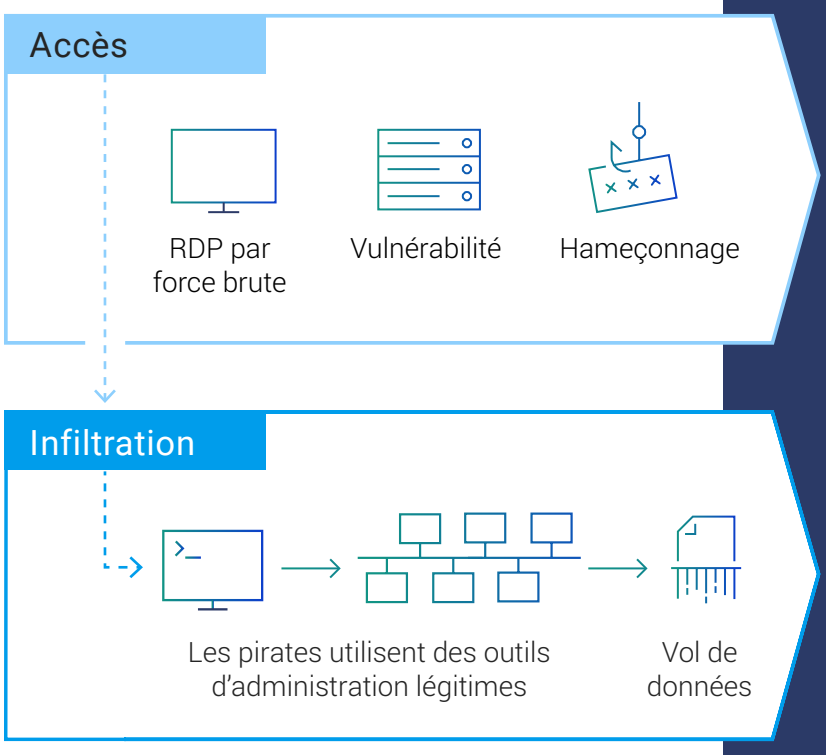
Les criminels raffolent plus que tout des logiciels de bureau à distance. Pour complexifier les attaques LOTL potentielles, désactivez le RDP et bloquez les outils de bureau à distance que votre entreprise n'utilise pas, comme Anydesk, Dameware Mini remote et Splashtop.

Dans un exemple d'attaque LOTL stoppée par l'équipe MDR de Malwarebytes, les cybercriminels utilisaient une chaîne d'outils légitimes pour tenter d'échapper à la détection. Ils se sont servi de wscript pour exécuter un fichier de script Windows (WSF), qui a lancé un script PowerShell, qui a téléchargé des fichiers malveillants ayant finalement été exécutés via rundll32.



Les cybercriminels adeptes des techniques LOTL utilisent des outils d'administration informatique légitimes plutôt que des malwares, ce qui les rend extrêmement difficiles à détecter. Lutter contre ce type d'attaques impose de faire appel à des chasseurs de menaces compétents utilisant un EDR de pointe pour trouver et investiguer les activités suspectes sur votre réseau.

Phases d'attaque « *Living Off the Land* »



Protection avec ThreatDown

La protection contre la force brute, les fonctions Vulnerability Assessment et Patch Management, la protection contre les exploits et le filtrage des contenus de sites web stoppent différentes formes d'accès.

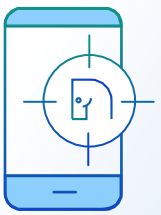
Managed Detection & Response (MDR) identifie et investigue les comportements suspects sur votre réseau ; le blocage des applications refuse aux pirates l'accès à leurs outils ; le filtrage des contenus de sites web empêche les pirates d'accéder aux serveurs de commande et de contrôle (C&C).

7. Les chevaux de Troie bancaires sur Android

Les chevaux de Troie bancaires constituent l'une des menaces les plus graves qui pèsent sur les appareils Android. Sophistiqués et discrets, ils combinent intelligemment technique et ingénierie sociale pour tromper les utilisateurs et échapper aux mécanismes de protection de Google Play, afin de voler de l'argent directement sur les comptes bancaires.

Les chevaux de Troie bancaires prennent la forme d'applications classiques comme des lecteurs de codes QR, des applications de suivi des performances sportives ou même des copies d'applications populaires comme Instagram. Une fois installées, les applications peuvent tester leur environnement pour s'assurer qu'elles se trouvent sur un véritable appareil, et non pas dans un laboratoire de recherche informatique. Les tests en question peuvent consister à rechercher la présence d'une carte SIM ou à vérifier que les pirates ne se trouvent pas sur un appareil rooté ou dans un émulateur. Si les conditions propices à l'installation du cheval de Troie bancaire sont réunies, une deuxième application malveillante est déployée.

Le malware peut regarder s'il se trouve sur un appareil rooté ou dans un environnement émulé, s'il y a une carte SIM, ou faire d'autres contrôles de son environnement pour éviter tout risque de rétro-ingénierie. Il peut aussi rester en veille pendant un moment, puis télécharger du code malveillant lors d'une mise à jour pour tenter d'échapper aux contrôles de sécurité de Google Play Protect.



88 500

Malwarebytes a détecté des chevaux de Troie bancaires 88 500 fois en 2023.

72 %

des smartphones utilisent Android, ce qui en fait le système d'exploitation le plus utilisé, devant Windows.

Parfois, l'application est téléchargée depuis un serveur externe. Pour contourner les systèmes de détection du réseau, une plateforme d'hébergement légitime peut être utilisée, telle que le CDN (Content Delivery Network) de Discord.

Il existe d'autres chevaux de Troie appelés « injecteurs », dans lesquels se trouve déjà la seconde application. Des services tiers comme Zombinder utilisent un mécanisme de liaison sophistiqué pour dissimuler une charge utile malveillante dans une application hôte bénigne.

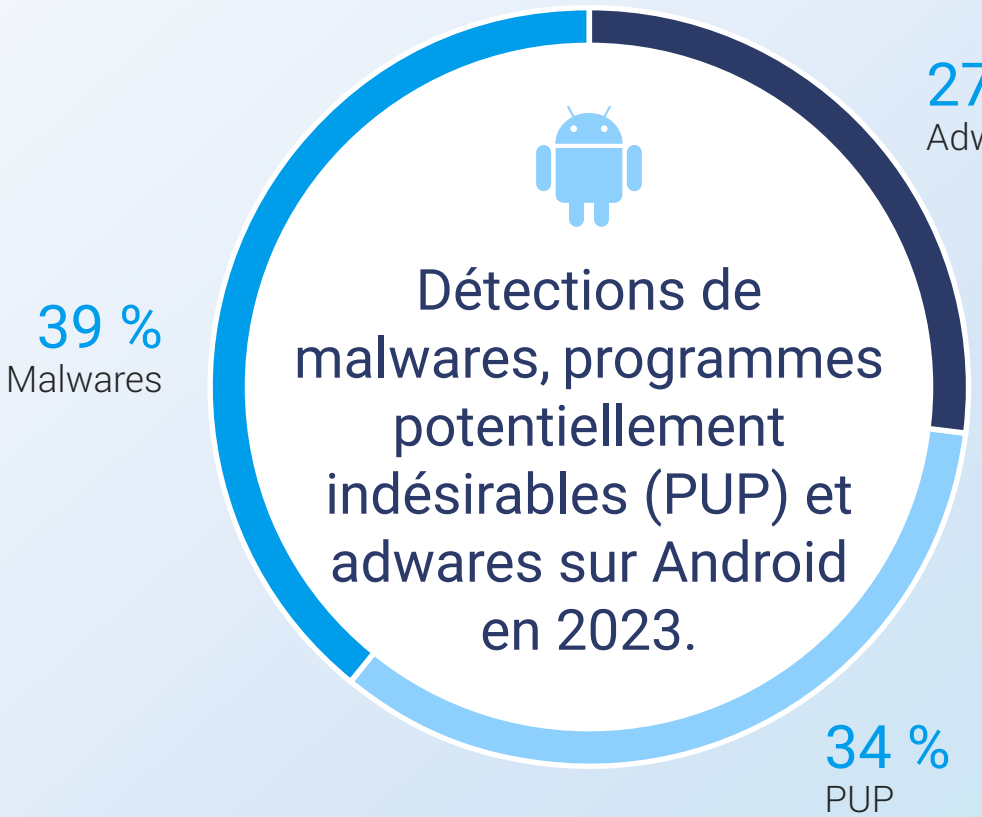
L'application malveillante est discrètement installée sur l'appareil cible ; elle avance typiquement à couvert grâce à une icône vide et en affichant une entrée vide lorsqu'un utilisateur essaie de lire les informations à son sujet.

Une fois installée, cette application malveillante demande à l'utilisateur de lui accorder des services d'accessibilité sous prétexte d'amélioration des fonctionnalités. Cela lui permet de surveiller les autres applications et de leur superposer des couches d'interface frauduleuses. Les surcouches capturent des informations d'identification personnelle, comme des mots de passe.

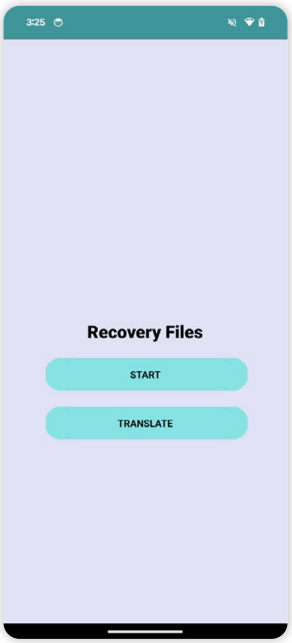
L'application implémente également un mécanisme d'interception discret pour capturer des jetons d'authentification multifacteur dans les SMS, sans alerter l'utilisateur.

Une fois doté des autorisations d'accès, le malware initialise son système de transfert automatisé (ATS), un ensemble complexe de scripts et de commandes conçus pour réaliser des transactions bancaires automatisées sans intervention de l'utilisateur.

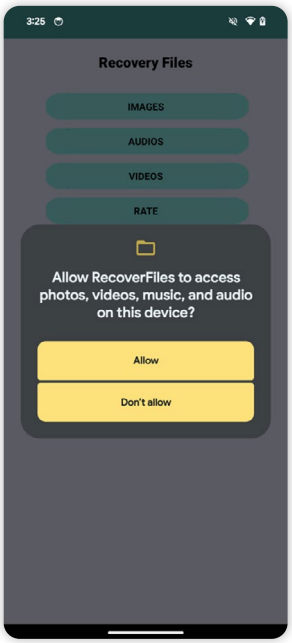
Le cadre ATS utilise les identifiants recueillis pour opérer des transferts de fonds non autorisés vers des comptes détenus par le cybercriminel. L'opération imite le comportement des utilisateurs réels pour tromper les systèmes de détection des fraudes.



Détections de malwares, programmes potentiellement indésirables (PUP) et adwares sur Android en 2023.

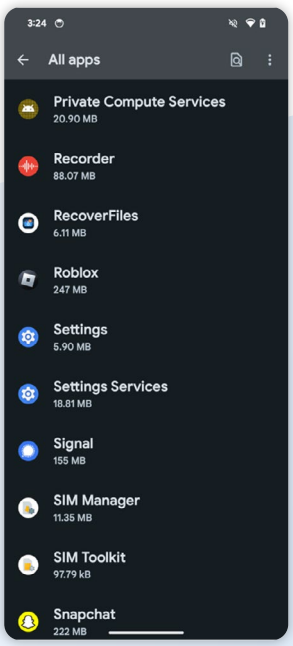


L'écran de démarrage d'un cheval de Troie bancaire dissimulé dans une application de récupération de fichiers.

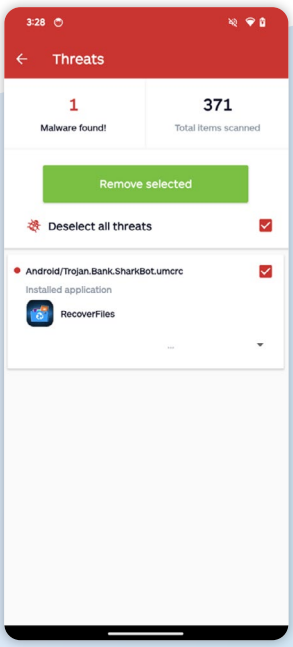


L'application demande l'autorisation d'accéder aux fichiers, de se connecter à d'autres applications et d'échanger avec elles, et d'envoyer des paiements via Google Play.

Aucune icône ne s'affiche après l'installation.



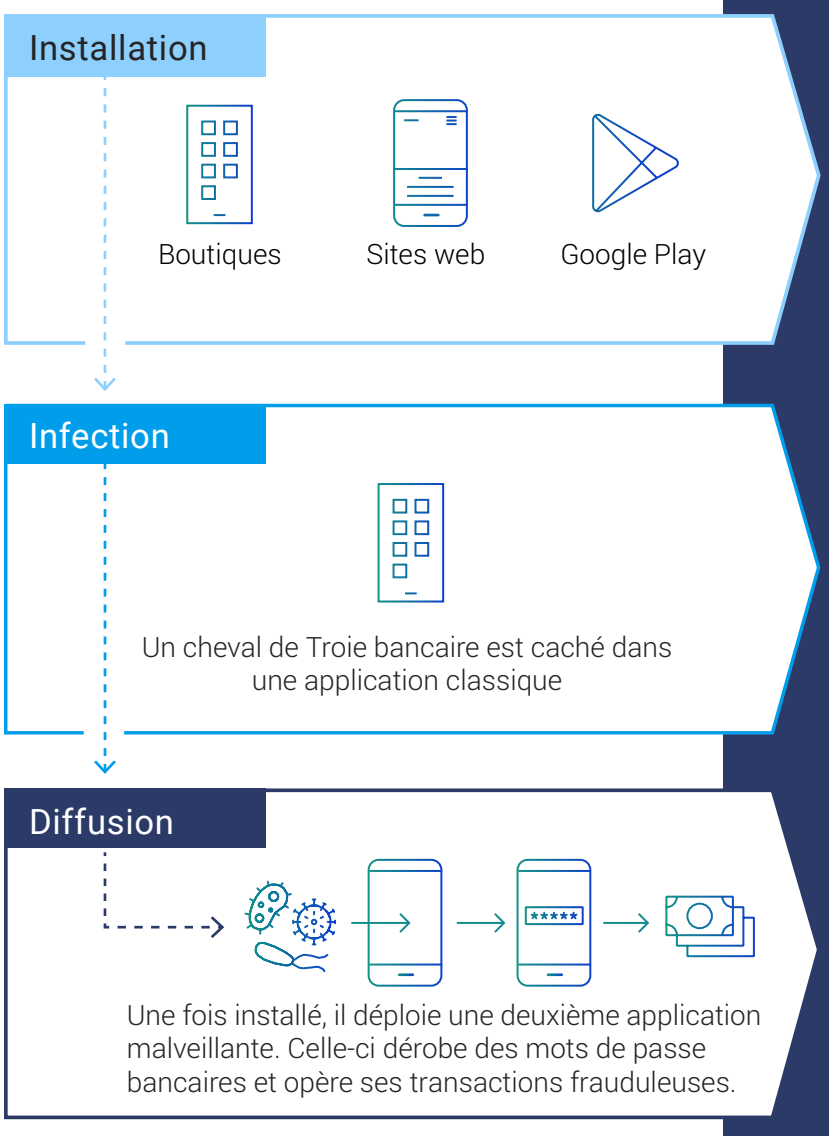
Cependant, l'application apparaît dans la liste.



Malwarebytes détecte l'application comme étant le cheval de Troie bancaire SharkBot.

Les chevaux de Troie bancaires représentent des menaces complexes et discrètes qui prennent la forme d'applications classiques au fonctionnement optimal. Ils copient les mots de passe bancaires et les utilisent pour voler en toute discrétion de l'argent directement sur les comptes bancaires. Se défendre contre les chevaux de Troie bancaires requiert la meilleure protection mobile qui soit, capable de détecter et de supprimer les malwares sur les appareils Android.

Phases d'attaque des chevaux de Troie bancaires



Protection avec ThreatDown

Mobile Security détecte et supprime les chevaux de Troie bancaires et d'autres malwares Android.

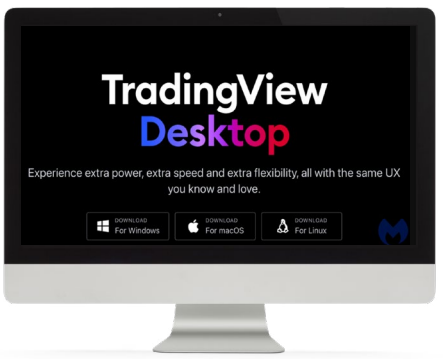
8. Les nouvelles tactiques de malware sur Mac

Contrairement à certaines croyances désormais obsolètes, les malwares ont toujours existé sur Mac. En fait, c'est simplement que le type de détections qui affectent généralement les Mac est différent. Plutôt que de se concentrer sur les ransomwares, les cybercriminels se tournent davantage vers des adwares agressifs et indésirables pour gagner de l'argent. En 2023, les malwares sur Mac ont adopté un certain nombre de tactiques qui nous rappellent qu'aucune prétendue « magie Apple » n'empêche les techniques et outils malveillants qui fonctionnent sur les machines Windows de très bien se porter également sur les Mac.

Le cybercrime va là où se trouve l'argent, et les ordinateurs personnels Windows, ainsi que les réseaux de machines d'entreprise Windows, ont traditionnellement représenté une cible bien plus importante, plus connectée et plus lucrative pour la cybercriminalité. Cependant, tout porte à croire que cette situation est en train de changer. La demande pour les Mac grandit parallèlement à la baisse des ventes de PC, et le système macOS d'Apple, sous ses nombreuses formes, représente maintenant 31 % du total des systèmes d'exploitation pour bureau aux États-Unis, tandis qu'un quart des entreprises utilisent des Mac au moins en partie sur leurs réseaux.

11 %

Les malwares représentaient 11 % des détections sur Mac en 2023.



Un site de malvertising distribue des téléchargements de malware pour Windows, Mac

Certains signes révèlent que les cybercriminels sont au fait de ces tendances, et qu'ils s'adaptent à la popularité croissante de la plateforme en intégrant des options Mac dans leurs chaînes d'attaque et en faisant en sorte que les attaques ciblent les utilisateurs Windows et Mac en même temps.

En septembre, Malwarebytes a mis au jour une campagne cybercriminelle qui diffusait le malware Atomic Stealer (AMOS) auprès des utilisateurs de Mac via des publicités malveillantes prétendant vendre l'application de suivi de marchés financiers TradingView.

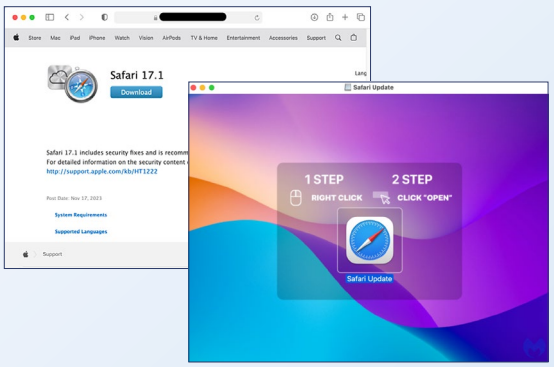
La publicité en question redirigeait les victimes vers un faux site d'aspect authentique, aux couleurs de TradingView, présentant des boutons de téléchargement distincts pour Windows, Mac et Linux. Les utilisateurs de Windows et Linux tombaient sur le cheval de Troie d'accès à distance NetSupport, tandis que les utilisateurs de Mac recevaient Atomic Stealer.

AMOS est un infostealer pour Mac capable de récolter des mots de passe, des données de navigateur, des cookies, des fichiers et des cryptomonnaies. Les campagnes de cybercrime qui se servent d'AMOS parviennent à contrôler l'infostealer via une console d'administration web vendue « en tant que service » (à l'instar des applications cloud légitimes) pour 1 000 $ (921 €) par mois.

En novembre, on a également découvert que la fausse chaîne de mise à jour de navigateur ClearFake distribuait AMOS. ClearFake a recours à des sites web compromis pour inciter les utilisateurs à télécharger des malwares qui ressemblent à des mises à jour de sécurité pour navigateurs.

L'infrastructure de la campagne détermine quel navigateur utilise la victime pour que la prétendue mise à jour soit conforme au navigateur utilisé. Les fausses mises à jour de navigateur ciblent généralement les utilisateurs Windows, c'est pourquoi l'apparition de pages aux couleurs de Safari diffusant des malwares dirigés contre macOS constitue une nouveauté.

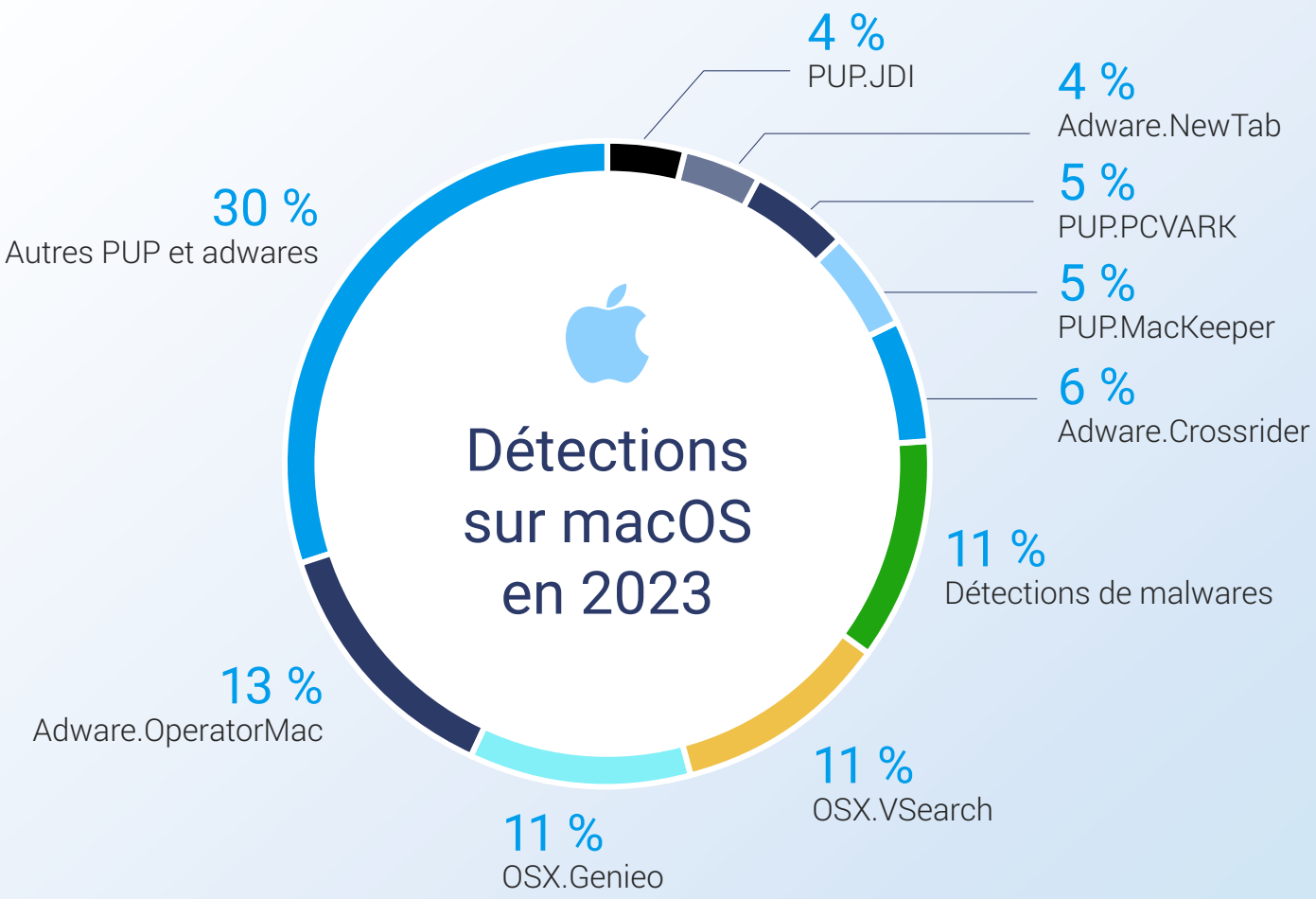
Le coût d'ajout d'une option macOS à une chaîne de distribution de malwares Windows existante est faible. Si les Mac continuent de prendre le chemin inverse des ventes de PC en 2024, alors cibler cette plateforme deviendra un choix de plus en plus évident pour les entreprises du cybercrime.



Une fausse mise à jour Safari imite le site web Apple officiel, et est même disponible en plusieurs langues.

LOCKBIT 3.0

En avril, les chercheurs sont tombés sur une version Mac de LockBit, le ransomware le plus dangereux au monde. Bien que l'outil en question soit encore au stade expérimental, le groupe LockBit a affirmé être en train de « développer activement » son ransomware pour Mac.

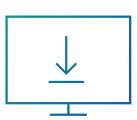

Détections sur macOS en 2023
4 %
PUP.JDI
4 %
Adware.NewTab
5 %
PUP.PCVARK
5 %
PUP.MacKeeper
6 %
Adware.Crossrider
11 %
Détections de malwares
11 %
OSX.VSearch
11 %
OSX.Genieo
13 %
Adware.OperatorMac
30 %
Autres PUP et adwares

À mesure que les Mac gagnent en popularité, les cybercriminels ajoutent des options Mac comme Atomic Stealer à leurs campagnes de malvertising et de fausses mises à jour de navigateur. Pour lutter contre les malwares Mac, un antivirus de nouvelle génération capable de détecter ce genre de menaces est nécessaire.

Phases d'attaque d'Atomic Stealer

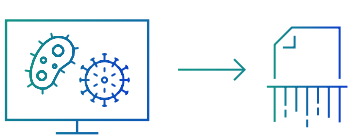
Accès

Installation



Les techniques d'ingénierie sociale permettent de contourner la fonctionnalité Gatekeeper

Attaque



Protection avec ThreatDown

Le filtrage des contenus de sites web peut bloquer les sites utilisés pour le malvertising et les fausses mises à jour.

Un antivirus de nouvelle génération peut stopper les malwares sur Mac.

9. Comment se préparer

Mark Twain disait : « l'histoire ne se répète pas, elle rime ». Le rythme persistant de la cybersécurité, répété sur des dizaines d'années, montre que les menaces commencent souvent par exploiter les failles des logiciels avant de s'attaquer à celles des humains.

Cela étant, pendant toutes ces années, la cybersécurité s'est largement concentrée sur les premières, en négligeant les failles humaines. Après tout, la technologie et les processus qui permettent leur mise à disposition peuvent toujours être améliorés, d'une manière inapplicable aux êtres humains. Avec une bonne dose de dévouement et de persévérance, les systèmes peuvent lentement être rendus plus sûrs ; les capacités de détection améliorées, les surfaces d'attaque réduites, les tests multipliés et les mises à jour appliquées plus fréquemment, afin de minimiser l'exploitation des failles techniques.

Pourtant, ce sont ces évolutions qui ont ouvert la voie à l'innovation dans le monde de la cybercriminalité.

Les améliorations apportées à la sécurité des navigateurs web ont mené à la disparition de l'exploitation routinière des navigateurs et des plug-ins au profit des attaques d'ingénierie sociale comme les fausses mises à jour et le malvertising.

Les ransomwares ont généré des milliards de dollars en délaissant les campagnes d'e-mails automatisées en faveur d'attaques manuelles contre de grands comptes, où les criminels affrontent plus directement les équipes informatiques et de sécurité.

L'amélioration des sauvegardes et de la détection a conduit un nombre toujours plus élevé de groupes de ransomwares à compléter leurs actions de chiffrement malveillant par des menaces de fuite des données volées, une situation délicate humainement, impossible à résoudre par logiciel. Elle a aussi mené à l'adoption des techniques LOTL (« ***Living Off The Land*** »), qui sont difficiles à repérer pour les logiciels sans intervention humaine.

Ces évolutions ont inévitablement rendu la composante humaine essentielle dans le processus de détection des menaces. Quelle que soit la taille de votre organisation, en 2024, votre capacité à associer logiciels de sécurité de pointe et personnel de sécurité compétent sera un facteur décisif dans votre lutte contre les cyberattaques, même les plus graves.

10. Présentation des offres ThreatDown

ThreatDown relève les défis en constante évolution de la cybersécurité moderne avec les technologies et services primés de Malwarebytes, qui offrent une protection sur tout le cycle d'attaque : de la diminution de la surface d'attaque à la prévention, la détection et la réponse jusqu'à la remédiation complète.

ThreatDown Core

Core offre une prévention complète contre les malwares, les menaces zero day et plus encore. **Core** inclut des technologies primées qui simplifient agréablement la gestion de la protection des terminaux.

ThreatDown Advanced

Advanced offre une protection supérieure sous la forme d'une solution unique, facile à gérer et à un prix raisonnable. Pensé pour les entreprises avec de petites équipes de sécurité aux ressources limitées, **Advanced** intègre des technologies primées qui simplifient considérablement la gestion de la protection des terminaux.

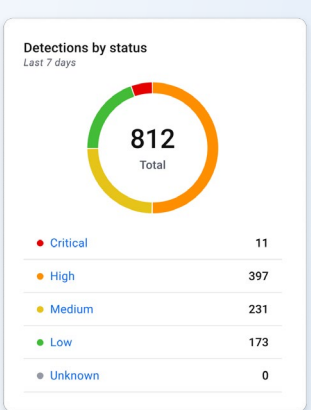
ThreatDown Elite

Elite offre une protection complète sous la forme d'une solution unique qui propose une facilité d'utilisation inégalée à un prix raisonnable. Conçue pour les entreprises avec des équipes de sécurité réduites (voire pas d'équipe de sécurité) qui manquent des ressources nécessaires pour s'occuper de toutes les alertes de sécurité, **Elite** intègre des technologies primées et la surveillance et la réponse gérées par des experts 24 h/24, 7 j/7 et 365 jours par an.

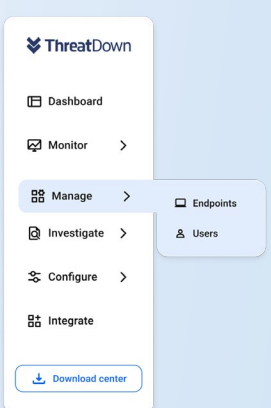
ThreatDown Ultimate

Ultimate offre la protection la plus complète contre tout le cycle d'attaque, de la réduction de la surface d'attaque ultraperformante à la prévention, la détection, la réponse et la remédiation complète, entièrement gérées, 24 h/24, 7 j/7, 365 jours par an.

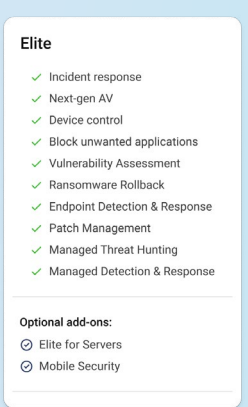
Démantelez les menaces.



Réduisez la complexité.



Limitez les coûts.



Nous le savons bien, le monde de la sécurité est complexe. Les produits de sécurité, eux, ne devraient pas l'être.

Découvrez les possibilités contenues dans chaque offre ThreatDown pour lutter contre ces six grandes cybermenaces.

Fonctionnalité	Core	Advanced	Elite	Ultimate
Incident Response	✓	✓	✓	✓
AV de prochaine génération	✓	✓	✓	✓
Contrôle des dispositifs	✓	✓	✓	✓
Blocage des applications injustifées	✓	✓	✓	✓
Vulnerability Assessment	✓	✓	✓	✓
Ransomware Rollback		✓	✓	✓
Endpoint Detection & Response		✓	✓	✓
Patch Management		✓	✓	✓
Managed Threat Hunting		✓		
Managed Detection & Response (includes threat hunting)			✓	✓
Filtrage des contenus de site web				✓
Modules complémentaires	✓	✓	✓	✓

Essayez les offres ThreatDown dès aujourd'hui !

Faites-nous confiance pour la sécurité de vos terminaux. Déployez la solution qui offre une défense optimale, une gestion d'une simplicité sans nom et le meilleur retour sur investissement pour votre sécurité.

Commencer

ThreatDown™ Powered by Malwarebytes

ThreatDown
Powered by Malwarebytes

One Albert Quay, 2nd Floor
Cork, Irlande
+1-800-520-2796