Digital Security
Progress. Protected.

Rapport sur les menaces

Premier semestre 2024

Décembre 2023 – Mai 2024

(eset):research

Sommaire

Résumé

Android iOS Menaces financières

GoldDigger poursuit sa route de l'Asie vers de nouveaux territoires

Un nouveau cheval de Troie Android et iOS vole les données de reconnaissance faciale de victimes en Asie afin de créer de fausses vidéos à des fins d'authentification de transactions financières. Une autre version plus ancienne sous Android a également fait son apparition en Amérique latine et en Afrique du Sud.

Linux Botnets Voleurs d'informations

Ebury prospère et pille les serveurs Linux

Alors que des centaines de milliers de serveurs sont compromis, les opérateurs d'Ebury déploient des outils pour maximiser leurs profits.

IA Menaces web d'informations Voleurs

Les logiciels malveillants déguisés en assistants d'IA générative

Un rapide coup d'œil derrière les faux assistants d'IA générative utilisés comme pièges par les voleurs d'informations.

Menaces web

Nouvelles vulnérabilités des plugins WordPress, nouveaux scripts malveillants

Au cours du premier semestre 2024, plus de 20 000 sites web ont été compromis par des injections de code JavaScript malveillant.

Voleurs d'informations Menaces Jeux vidéo

Rencontres programmées : les cybercriminels s'attaquent aux joueurs

Des voleurs d'informations menacent les données personnelles des amateurs de jeux vidéo.

Downloaders

Les downloaders changent de méthode de livraison et font leur grand retour

Après les bouleversements survenus en 2022, les menaces liées aux downloaders refont peu à peu surface.

Rançongiciel

Bilan de LockBit : quel est leur avenir à la suite de l'opération Cronos ?

Au lendemain de son démantèlement, l'avenir du groupe du rançongiciel LockBit montre des signes de lutte, tandis que d'autres acteurs de la menace utilisant la fuite du builder de LockBit se profilent à l'horizon.

Avant-propos

Bienvenue dans le numéro du premier semestre 2024 du rapport sur les menaces d'ESET !

Ces six derniers mois, nous avons découvert un paysage dynamique de menaces financières liées à Android : des logiciels malveillants qui s'attaquent aux fonds bancaires mobiles des victimes, que ce soit sous la forme de logiciels malveillants bancaires « traditionnels » ou, plus récemment, de détourneur de cryptomonnaie.

GoldPickaxe est un nouveau venu intrigant dans ce domaine. Il s'agit d'un nouveau logiciel malveillant pour téléphone portable capable de détourner des données de reconnaissance faciale pour créer de fausses vidéos utilisées à des fins d'authentification de transactions financières frauduleuses par les opérateurs de ce logiciel malveillant. Exploitant les versions Android et iOS, cette menace a ciblé des victimes en Asie du Sud-Est par le biais d'applications malveillantes adaptées à cette région. En se penchant sur cette famille de logiciels malveillants, les chercheurs d'ESET ont découvert qu'une version Android plus ancienne de GoldPickaxe, baptisée GoldDiggerPlus, s'est également frayée un chemin vers l'Amérique latine et l'Afrique du Sud en ciblant activement les victimes de ces régions.

Pour rester dans l'air du temps, les logiciels malveillants voleurs d'informations peuvent désormais également se faire passer pour des outils d'IA générative. Au premier semestre 2024, le voleur d'informations Rilide était connu pour utiliser abusivement les noms d'assistants d'IA générative, tels que Sora d'OpenAI et Gemini de Google, afin d'attirer de potentielles victimes. Dans le cadre d'une autre campagne malveillante, le voleur d'informations Vidar se cachait derrière une prétendue application Windows pour le générateur d'images par IA Midjourney, alors que le modèle d'IA de Midjourney n'est accessible que par le biais de Discord. Depuis 2023, nous constatons que les cybercriminels abusent de plus en plus de la notion d'IA, une tendance qui devrait se poursuivre.

Les amateurs de jeux vidéo qui s'aventurent en dehors des plateformes officielles découvrent malheureusement que les menaces des voleurs d'informations ont également trouvé un moyen de gâcher leur passe-temps favori : certains jeux vidéo piratés et outils de triche utilisés dans les jeux multijoueurs en ligne se sont récemment révélés contenir des logiciels malveillants voleur d'informations tels que Lumma Stealer et RedLine Stealer.

Au premier semestre 2024, nous avons constaté plusieurs pics de détection de RedLine Stealer, dus à des campagnes ponctuelles menées en Espagne, au Japon et en Allemagne. Bien que ce « voleur d'informations à la demande » ait connu un démantèlement en 2023 et ne semble plus être en développement actif, les dernières vagues ont été si importantes que les détections de RedLine Stealer au premier semestre 2024 ont dépassé d'un tiers celles du second semestre 2023.

Balada Injector, un groupe connu pour exploiter les vulnérabilités des plugins WordPress, a continué à sévir au cours du premier semestre 2024, compromettant plus de 20 000 sites web et enregistrant plus de 400 000 occurrences dans la télémétrie d'ESET pour les variantes utilisées dans la récente campagne du groupe.

En ce qui concerne les rançongiciels, l'ancien leader LockBit a été renversé par l'opération Cronos, un démantèlement mondial mené par les forces de l'ordre en février 2024.
Bien que la télémétrie d'ESET ait enregistré deux campagnes LockBit notables au premier semestre 2024, il s'est avéré qu'elles étaient le résultat de groupes non affiliés à LockBit qui utilisaient le builder de LockBit ayant fait l'objet d'une fuite.

Le botnet Ebury, précédemment étudié dans le livre blanc Operation Windigo publié par ESET en 2014, demeure dangereux même dix ans plus tard : une enquête récente menée par les chercheurs d'ESET a révélé que cette menace a compromis près de 400 000 serveurs depuis 2009. Si la boîte à outils d'Ebury était déjà conséquente au moment de la recherche initiale, ces dernières découvertes ont révélé de nouvelles fonctionnalités du botnet, principalement axées sur des méthodes de monétisation telles que le détournement de cryptomonnaies et de cartes de crédit.

Je vous souhaite une lecture enrichissante.

Jiří Kropáč
Directeur de la détection des menaces chez ESET

Tendances en matière de menaces

Android iOS Menaces financières

GoldDigger poursuit sa route de l'Asie vers de nouveaux territoires

Un nouveau cheval de Troie Android et iOS vole les données de reconnaissance faciale de victimes en Asie afin de créer de fausses vidéos à des fins d'authentification de transactions financières. Une autre version plus ancienne sous Android a également fait son apparition en Amérique latine et en Afrique du Sud.

Au cours du premier semestre 2024, la télémétrie ESET a enregistré une forte diminution de la détection de la quasi-totalité des menaces sous Android que nous surveillons. Malgré des fluctuations dans bon nombre de ces catégories, souvent liées à des événements saisonniers tels que Noël et d'autres fêtes similaires (comme indiqué dans le rapport sur les menaces ESET au T3 2022), les menaces financières liées à Android sont restées très répandues.

Cette catégorie a connu une baisse relativement modeste de 3,8 % au premier semestre 2024 par rapport au semestre précédent, ne montrant pas de changements significatifs dans les taux de détection au cours des deux dernières années. Toutefois, les logiciels malveillant de cette catégorie affichent des changements constants dans leur comportement et dans les méthodes qu'ils utilisent pour s'attaquer à leurs cibles.

Tendance de détection des menaces financières liées à Android entre le second semestre 2022 et le premier semestre 2024, moyenne mobile sur sept jours

Dans les rapports sur les menaces ESET, **les menaces financières liées à Android** incluent à la fois les logiciels malveillants bancaires et les détourneurs de cryptomonnaie. Cette fusion tient compte du fait que de nombreux chevaux de Troie bancaires sont maintenant dotés de fonctionnalités permettant de voler les informations d'identification des portefeuilles de cryptomonnaies et de s'approprier ces fonds, ce qui nous a amenés à regrouper ces menaces dans une seule et même catégorie.

Dans ce contexte dynamique, Group-IB a découvert une famille de logiciels malveillants qui volent les données de reconnaissance faciale, lesquelles sont ensuite utilisées pour créer de fausses vidéos. Leur création est facilitée par des services d'intelligence artificielle d'échange de visages et ces vidéos sont ensuite utilisées à des fins d'authentification de transactions financières. Le logiciel malveillant, baptisé GoldPickaxe, se décline en versions Android et iOS et vise les propriétaires de portefeuilles de cryptomonnaies et les clients de services financiers fournis en Asie du Sud-Est. ESET a découvert qu'une version Android plus ancienne de GoldPickaxe, baptisée GoldDiggerPlus, s'est également frayée un chemin vers l'Amérique latine et l'Afrique du Sud en ciblant activement les victimes de ces régions.

Les données de reconnaissance faciale sont devenues un élément important du processus d'authentification numérique et revêtent donc un intérêt pour les cybercriminels. Certaines applications financières, en particulier celles utilisées dans certaines régions, exigent que les utilisateurs enregistrent une brève vidéo de leur visage sous différents angles à l'aide de la caméra frontale de leur appareil mobile. Ils doivent également télécharger des images recto verso de leurs pièces d'identité personnelles. Ces vidéos sont utilisées à des fins de vérification d'identité. Ce processus, souvent appelé authentification biométrique ou reconnaissance faciale, permet aux applications financières de confirmer que la personne qui crée le compte ou effectue la transaction est bien celle qui possède les pièces d'identité fournies. Paradoxalement, il était destiné à ajouter une couche supplémentaire de sécurité pour prévenir le vol d'identité et les activités frauduleuses.

GoldPickaxe s'empare d'Android et d'iOS

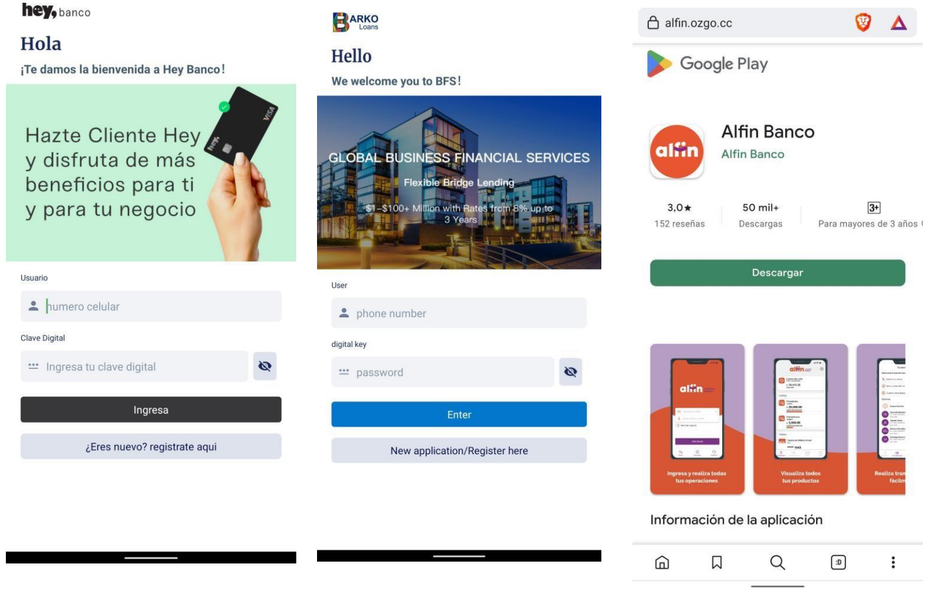
La version Android de GoldPickaxe, détectée par les solutions de sécurité ESET sous le nom de Android/Spy.Banker.CNA, est distribuée via des sites web se faisant passer pour le magasin officiel Google Play. La version iOS, détectée par les solutions de sécurité ESET sous le nom de iOS/Riskware.Frp.A, a été initialement distribuée via TestFlight, la plateforme de test d'applications mobiles d'Apple ; cependant, après son retrait de cette plateforme, les acteurs de la menace ont adopté une approche plus sophistiquée. Ils utilisent désormais un schéma d'ingénierie sociale en plusieurs étapes pour persuader les victimes d'installer un profil de gestion des appareils mobiles, ce qui permet aux acteurs de la menace de prendre le contrôle total de l'appareil iOS de la victime.

Group-IB estime que l'acteur de la menace derrière GoldPickaxe est un groupe qu'il appelle GoldFactory,un groupe de cybercriminels sinophones bien organisé, qui est également derrière les autres versions de GoldPickaxe : GoldDigger et GoldDiggerPlus. GoldPickaxe est en effet basé sur GoldDigger. Bien que nous ne soyons pas en mesure de confirmer certaines des conclusions concernant GoldFactory, nous avons pu détecter des évolutions dans la distribution de certaines variantes de GoldDiggerPlus, qui sont détectées par les produits de sécurité ESET sous les noms Android/Spy.Banker.CAY et Android/Spy.Banker.CMQ.

GoldDigger ne possède que des versions pour Android et abuse des services d'accessibilité d'Android pour extraire des informations personnelles, voler des identifiants d'applications bancaires, intercepter des messages SMS et effectuer toute une série d'autres actions. La dernière version en date, GoldDiggerPlus, est dotée d'une fonction unique qui permet aux auteurs de menaces de passer des appels en temps réel à leurs victimes. Lorsqu'une victime clique sur le bouton du service clientèle dans l'application malveillante, le logiciel malveillant tente de se connecter à un membre disponible du groupe à l'origine de cette menace, créant ainsi l'illusion que les cybercriminels gèrent un véritable centre de service clientèle.

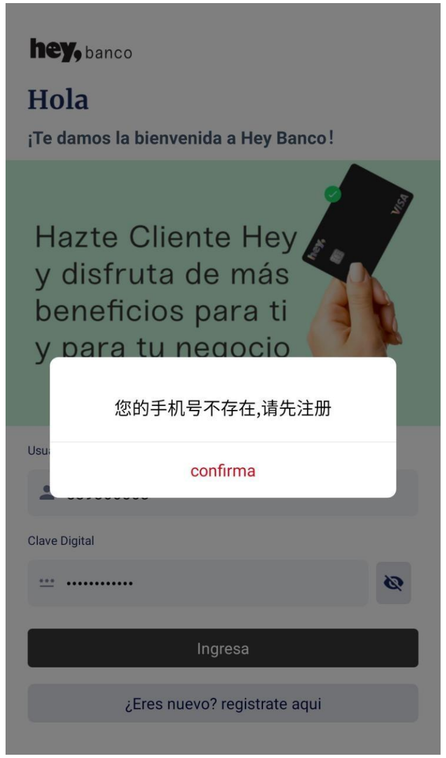
Recherche active de nouvelles victimes en Amérique latine et en Afrique du Sud

Bien que GoldDiggerPlus ait principalement ciblé des victimes en Asie du Sud-Est, les données télémétriques d'ESET montrent que ce cheval de Troie a également été détecté en Amérique latine et en Afrique du Sud. Nous pouvons par ailleurs confirmer que les acteurs de la menace derrière GoldDiggerPlus ciblent activement ces régions et que ces détections ne concernent pas uniquement les propriétaires d'appareils d'Asie du Sud- Est se trouvant dans ces autres pays.

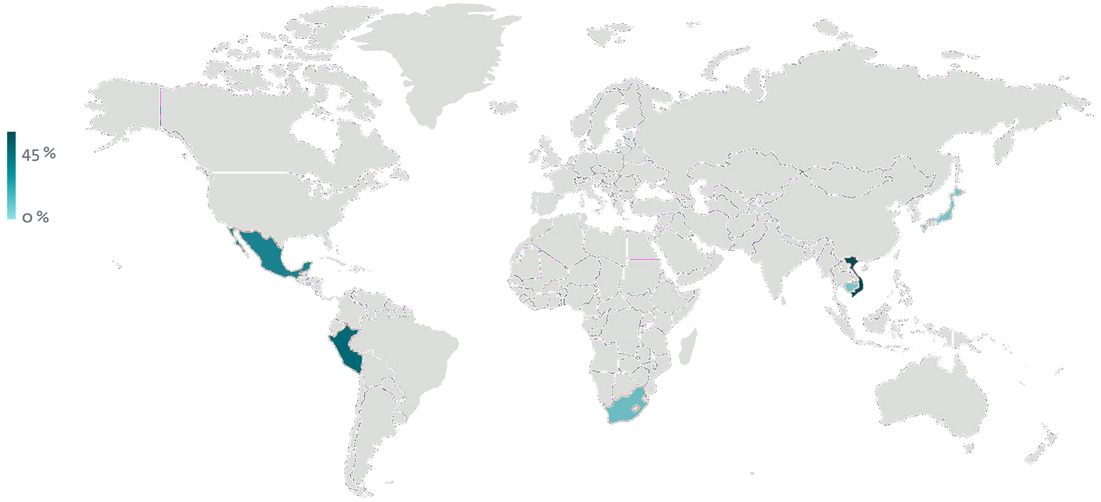


Versions malveillantes de l'application mexicaine Hey Banco, de l'application sud-africaine Barko Financial Services et de l'application péruvienne Alfin Banco,

Le logiciel malveillant GoldDiggerPlus que nous avons analysé se déguise en applications officielles d'Alfin Banco au Pérou, de Hey Banco au Mexique et de Barko Financial Services en Afrique du Sud. La méthode de distribution est identique à celle utilisée en Asie du Sud-Est, les applications malveillantes étant distribuées



Version malveillante de l'application mexicaine Hey Banco qui invite l'utilisateur à s'enregistrer, mais qui est rédigée en chinois



Répartition géographique des détections de GoldDiggerPlus au premier semestre 2024

par l'intermédiaire de sites web qui usurpent l'identité du magasin officiel Google Play. Toutes ces applications malveillantes sont fournies dans la langue locale de la région ciblée. Il est intéressant de noter que des traces de chinois peuvent parfois être détectées dans les applications. Par exemple, lorsque les utilisateurs saisissent des données fausses ou erronées dans la version malveillante de l'application Hey Banco, ils reçoivent un message en chinois qui se traduit par « Votre numéro de téléphone portable n'existe pas, veuillez d'abord vous enregistrer ». Fait amusant, le bouton « confirmer » est correctement traduit.

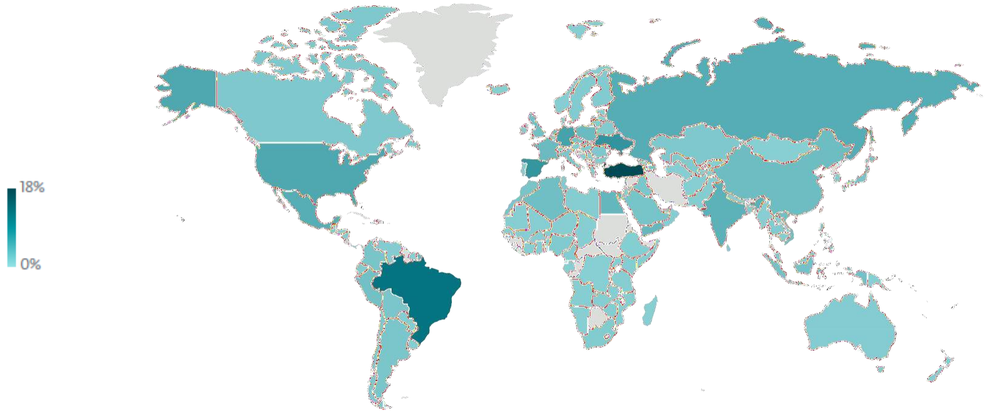
Changements de stratégie pour les menaces financières

Ces dernières années, les menaces financières liées à Android ont considérablement évolué en réponse aux mesures de sécurité renforcées et à l'évolution du paysage numérique. Les stratégies employées par la famille GoldDigger décrites ci-dessus ne représentent qu'une fraction des adaptations effectuées par les acteurs de la menace. De tels changements découlent de la volonté des attaquants de mettre au point des méthodes d'intrusion plus sophistiquées et moins détectables.

Par exemple, l'utilisation abusive des services d'accessibilité d'Android permet aux attaquants de déclencher et d'enregistrer n'importe quel événement sur un appareil, obtenant ainsi un contrôle total, tandis que la technologie Virtual Network Computing (informatique virtuelle en réseau) facilite la diffusion en continu de l'écran de la victime en temps réel. Les attaquants ont également mis au point des systèmes de transfert automatique, qui permettent de transférer ou de déposer sans autorisation des fonds du compte de la victime, rendant ainsi la transaction moins suspecte ; ils ont trouvé des moyens de contourner les systèmes d'authentification à deux facteurs basés sur des logiciels tels que Google Authenticator ; ils peuvent aussi contourner les « paramètres restreints », mesure de sécurité introduite sous Android 13.

Lorsqu'une nouvelle menace financière mobile émerge, elle présente souvent des liens avec l'Amérique latine ou l'Asie du Sud-Est. Ces régions sont progressivement devenues des épicentres d'activités cybercriminelles, notamment en matière de menaces financières mobiles. Cependant, au cours des deux dernières années, la Turquie a été le pays le plus touché par les menaces financières liées à Android, selon les données télémétriques d'ESET.

La raison de cette première position de la Turquie et de la prévalence de ces menaces en Amérique latine, en Asie du Sud-Est et dans certains pays d'Afrique est simple : une transformation numérique fulgurante. Une grande partie de la population de ces régions délaisse les PC ou les ordinateurs portables et accède à la toile au moyen



Répartition géographique des menaces financières liées à Android au premier semestre 2024

de smartphones. Un grand nombre de personnes qui n'avaient jusqu'à présent pas accès aux services bancaires en ligne traditionnels utilisent désormais leur smartphone pour effectuer des transactions financières. Ce basculement rapide vers les services bancaires numériques a malheureusement entraîné une augmentation de la cybercriminalité. Les cybercriminels ciblent souvent ces régions, profitant de leurs vulnérabilités pour commettre des fraudes.

La stabilité de la tendance en matière de détection des menaces financières liées à Android s'inscrit dans un contexte de baisse, dans presque toutes les catégories que nous surveillons : Applications cachées (-67 %), logiciels espions (-43 %), chevaux de Troie SMS (-25 %), logiciels publicitaires (-23 %), logiciels traqueurs (-22 %), rançongiciels (-18 %) et clickers (-15 %). Ainsi, le nombre de détections de l'ensemble des menaces Android a chuté de 41 %. À contrario de cette tendance à la baisse, la catégorie des applications frauduleuses a connu une hausse de 18 %.Cependant, il est de plus en plus difficile de repérer certaines des menaces Android en déclin, car elles sont introduites sur les appareils par l'intermédiaire de droppers. Ces programmes sont souvent déguisés en applications légitimes et, une fois installés sur un appareil, sont en mesure de déployer toute une série de logiciels malveillants, généralement à l'insu de l'utilisateur. L'objectif principal d'un dropper est de garantir la persistance du logiciel malveillant sur l'appareil, même si l'application malveillante qu'il installe en premier lieu est détectée et supprimée. Au premier semestre, nous avons observé plusieurs droppers courants installant des applications cachées, mais la télémétrie d'ESET ne peut pas les surveiller, car ces droppers peuvent installer différents types de menaces, ou même installer de nouvelles applications complètement différentes à l'avenir. Néanmoins, les droppers ont également connu une baisse au cours du premier semestre de cette année.

DE NOUVEAUX VECTEURS DE COMPROMISSION POUR LES APPAREILS IOS ?

La prévalence des menaces sur la plateforme iOS est notablement plus faible par rapport aux autres systèmes d'exploitation, mais elle n'est pas inexistante, comme l'illustre la version iOS de GoldPickaxe. Cette réduction du risque s'explique principalement par le processus rigoureux d'approbation des applications d'Apple et par l'environnement fermé de l'écosystème iOS. Il fonctionne selon le principe du bac à sable qui isole chaque application, les empêchant d'interférer entre elles et même d'accéder facilement à leurs données respectives, réduisant ainsi les activités malveillantes potentielles. Ce principe signifie également qu'une application de sécurité sur un appareil iOS ne peut pas analyser l'ensemble de l'appareil ou d'autres applications, mais seulement elle-même, rendant ainsi la détection des menaces plus complexe. En principe, les menaces potentielles liées à iOS devraient être identifiées et atténuées par les protocoles de sécurité intégrés d'Apple. Jusqu'à présent, contrairement à Android, iOS n'autorisait pas le téléchargement d'applications à partir de sources tierces, ce qui réduisait davantage le risque d'être confronté à des menaces. Cette politique est toutefois sur le point de connaître un changement important, du moins pour les utilisateurs d'appareils iOS dans l'Union européenne (UE).

En vertu du règlement sur les marchés numériques de la Commission européenne, les utilisateurs d'iOS résidant dans l'UE pourront bientôt télécharger des applications à partir de sites web et de marchés d'applications alternatifs, en plus de l'App Store traditionnel. Ce changement, influencé par plusieurs actions en justice et par l'examen de la réglementation, vise à ouvrir l'écosystème habituellement fermé d'Apple à des concurrents plus modestes, offrant ainsi un choix plus large aux consommateurs.

Toutefois, ce changement s'accompagne d'une multitude de contraintes. Pour protéger les utilisateurs, Apple a mis en place un processus de notarisation pour toutes les applications, quel que soit le canal de distribution, afin de s'assurer qu'elles respectent les normes de base en matière d'intégrité de la plateforme.

Le nouveau programme de téléchargement sur le web contraint les développeurs à répondre à des critères spécifiques, comme le fait de disposer d'une application ayant été téléchargée plus d'un million de fois dans l'UE. En outre, les entreprises peuvent proposer un magasin d'applications pour les iPhone dans l'UE, à condition qu'il ne donne accès qu'aux applications d'une seule entreprise.

Malgré cela, des attaquants potentiels pourraient encore trouver des moyens d'exploiter ce système en déguisant des logiciels malveillants en applications légitimes, ou en compromettant des marchés d'applications alternatifs moins sécurisés. Reste à savoir dans combien de temps ils seront en mesure de le faire.

Linux Botnets Voleurs d'informations

Ebury prospère et pille les serveurs Linux

Alors que des centaines de milliers de serveurs sont compromis, les opérateurs d'Ebury déploient des outils pour maximiser leurs profits.

Dix ans plus tôt, ESET Research publiait un livre blanc décrivant une campagne à grande échelle baptisée Operation Windigo, dans laquelle des acteurs malveillants utilisaient un réseau de botnets pour compromettre des milliers de serveurs Linux et Unix à l'aide de la famille de logiciels malveillants Ebury.
Malgré l'arrestation et l'extradition d'un des auteurs en 2015, les activités du botnet se poursuivent à ce jour : les chiffres d'Ebury connaissent une augmentation plus ou moins continue depuis 2009, avec des mises à jour régulières sur des dizaines de milliers de serveurs chaque année, soit près de 400 000 serveurs affectés au total.

En mai 2024, après une enquête approfondie et de longue haleine sur le botnet en collaboration avec les forces de l'ordre, ESET Research a publié un nouveau livre blanc détaillant nos nouvelles découvertes.

Si la boîte à outils d'Ebury était déjà conséquente au moment de la recherche initiale, les *honeypots* (leurre) de miel conçus par ESET avec l'aide des forces de l'ordre ont révélé de nouvelles fonctionnalités du botnet. Ces derniers visent principalement à tirer profit des serveurs compromis par divers moyens, notamment par le détournement de cryptomonnaies et le vol de cartes de crédit.

Ebury est une porte dérobée OpenSSH et un voleur d'informations d'identification formant le cœur d'un groupe de menaces orientées serveur, initialement utilisées à des fins de redirection web, de diffusion de logiciels malveillants sous Windows et de spamming.
Aujourd'hui, le botnet Ebury intercepte également les requêtes HTTP POST adressées aux serveurs afin de voler des informations financières provenant de sites web transactionnels.

Déploiements d'Ebury par mois depuis 2009, axe Y logarithmique

Lorsqu'il s'attaque aux fonds de cryptomonnaies, Ebury tire parti de sa présence dans les centres de données du monde entier pour mener des attaques de type « adversary-in-the-middle ». Une fois que les opérateurs ont identifié un serveur de valeur, ils sont en mesure de rediriger le trafic réseau vers un système sous leur contrôle afin de capturer ses identifiants SSH et d'exécuter ensuite des scripts pour exfiltrer les données des portefeuilles de cryptomonnaies du système.

En ce qui concerne le vol de cartes de crédit, le botnet a recours à l'écoute clandestine du trafic réseau, attendant le moment où les victimes soumettent leurs informations de carte de crédit à un magasin en ligne compromis. Une fois les données transmises, Ebury peut déployer divers outils pour intercepter les informations.

En plus de voler des données de cartes de crédit et des fonds en cryptomonnaies, les acteurs de la menace derrière Ebury ont développé d'autres moyens pour soutenir leurs efforts de monétisation. Citons notamment les modules Apache qui exfiltrent les requêtes HTTP ou transfèrent le trafic, les modules du noyau Linux qui effectuent des redirections et les outils Netfilter modifiés qui injectent des règles de pare-feu.

La découverte des activités des auteurs a également permis de comprendre comment Ebury se propage en volant des informations d'identification et en compromettant l'infrastructure des fournisseurs d'hébergement, en déployant des logiciels malveillants sur l'ensemble des serveurs loués par les clients, aboutissant parfois à la compromission de milliers de serveurs, hébergeant des millions de domaines.

Les opérations à grande échelle menées par Ebury depuis des décennies et sa capacité à compromettre les utilisateurs de Linux les plus avertis, tels que les responsables de linux.org, mettent en évidence de nombreuses lacunes dans l'état de la sécurité de Linux.

Le livre blanc contient beaucoup plus de détails techniques, ainsi que des conseils pour ceux qui veulent s'assurer que leurs systèmes sont sécurisés. Ce dernier point est délicat en raison des techniques de rootkit employées par le logiciel malveillant Ebury, mais nous proposons également des méthodes de détection de la présence de rootkits userland grâce à diverses techniques. Notez que pour garantir qu'un système compromis par Ebury est totalement exempt de toute compromission permanente, une réinstallation complète est nécessaire et aucune des clés ou des informations d'identification du serveur affecté ne doit être réutilisée.

IA Menaces web Voleurs d'informations

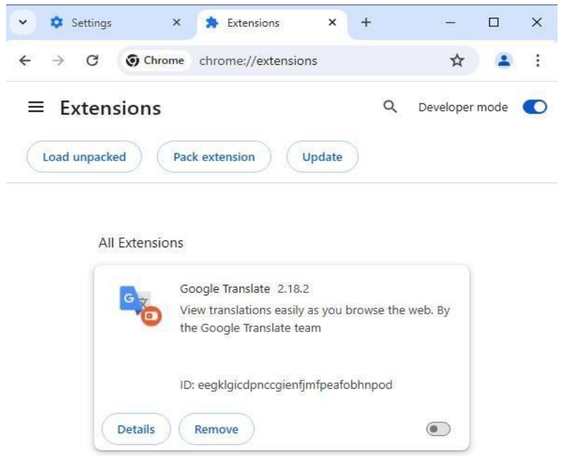
Les logiciels malveillants déguisés en assistants d'IA générative

Un rapide coup d'œil derrière les faux assistants d'IA générative utilisés comme pièges par les voleurs d'informations.

La télémétrie d'ESET a enregistré plusieurs tentatives d'utilisation des noms d'assistants d'IA générative pour diffuser des logiciels malveillants. Les cas les plus intéressants observés au premier semestre 2024 sont peut-être une extension de navigateur Chrome malveillante, connue sous le nom de Rilide Stealer, et un programme d'installation malveillant prétendant fournir une application de bureau pour un logiciel d'IA, mais diffusant à la place le voleur d'informations Vidar.

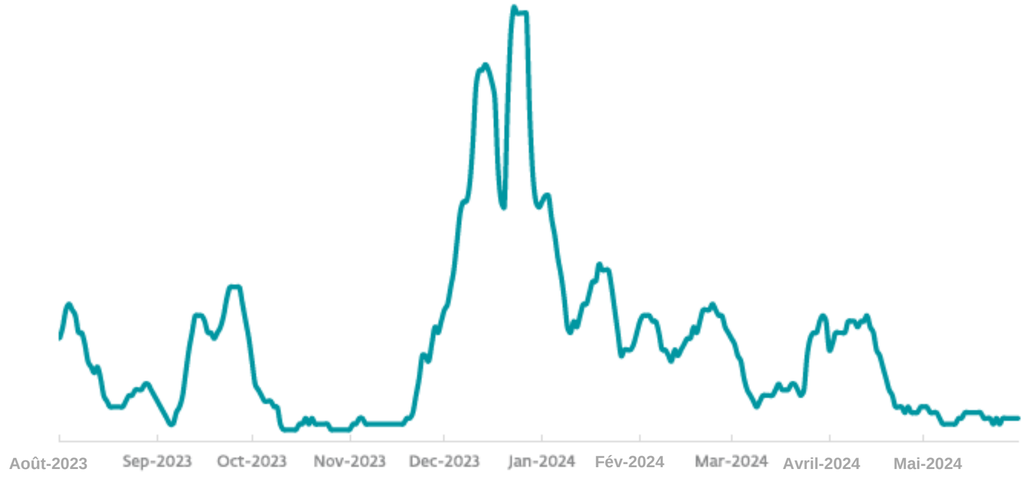
Rilide Stealer

Cette extension de navigateur malveillante est fournie aux victimes qui ont été dupées en cliquant sur des publicités malveillantes, le plus souvent diffusées sur Facebook, qui promettent les services d'un modèle d'IA générative. Bien que l'extension elle-même se fasse passer pour Google Traduction, elle utilise comme leurre la page web officielle de l'un des services d'IA, notamment Sora d'OpenAI et Gemini de Google. Détectée comme JS/Extenbro.Agent.EK et JS/Extenbro.Agent.EP par les produits de sécurité ESET, cette extension est en réalité un voleur d'informations, connu sous le nom de Rilide Stealer V4, destiné à s'emparer des informations d'identification Facebook.



L'extension de navigateur Chrome Rilide Stealer V4, se faisant passer pour Google Traduction

Depuis août 2023, la télémétrie d'ESET a enregistré plus de 4 000 tentatives d'installation de l'extension malveillante.



Tendance de détection de l'extension de navigateur Rilide Stealer V4, moyenne mobile sur sept jours

Voleur d'informations Vidar

Diffusé par le biais de publicités Facebook, de groupes Telegram et de forums du dark web, le programme d'installation malveillant prétend offrir Midjourney, un générateur d'images par IA, mais transmet en réalité le voleur d'informations Vidar. Lors de l'exécution, si le programme d'installation détecte qu'un environnement d'exécution Java (JRE) n'est pas installé sur le système, un message d'erreur concernant l'environnement d'exécution manquant s'affiche et la page officielle de téléchargement de Java s'ouvre ; Java est nécessaire au fonctionnement du programme d'installation. Si le JRE est déjà installé, un écran de démarrage présentant Midjourney s'affiche.

Le programme d'installation, détecté comme Java/TrojanDownloader. Agent.NWR, installe plusieurs logiciels malveillants et la version 3 d'AutoIt, qui diffuse à son tour Vidar. Ce voleur d'informations peut enregistrer les frappes de clavier et dérober les informations d'identification stockées par les navigateurs et les données des portefeuilles de cryptomonnaie.

Cependant, Midjourney ne propose pas d'application de bureau ; son modèle d'IA est accessible en tant que bot Discord sur le serveur Discord officiel de Midjourney, en envoyant directement un message au bot dans Discord, ou en l'ajoutant à un serveur Discord tiers. Étant donné que le logiciel malveillant utilise le nom `Midjourneyv6`, il tente de se faire passer pour la dernière version du modèle Midjourney actuellement disponible.

Écran de démarrage affiché par le programme d'installation du voleur d'informations Vidar, se faisant passer pour Midjourney

COMMENTAIRE D'EXPERT

Bien que le développement continu de modèles d'IA générative ait été accompagné de mesures de protection visant à empêcher leur utilisation abusive, cela n'a pas empêché les cybercriminels de mettre l'IA générative au service de la cybercriminalité. Depuis 2023, les voleurs d'informations sont les plus nombreux à abuser de cette notion et nous nous attendons à ce que cette tendance se poursuive. Au lieu de cliquer sur des liens douteux promettant l'accès à des modèles d'IA générative, orientez-vous toujours vers les sites web officiels des fournisseurs. Pour rester protégé contre les voleurs d'informations, veillez à utiliser des solutions de sécurité fiables sur vos appareils.

Jiří Kropáč, directeur de la détection des menaces chez ESET

Menaces web

Nouvelles vulnérabilités des plugins WordPress, nouveaux scripts malveillants

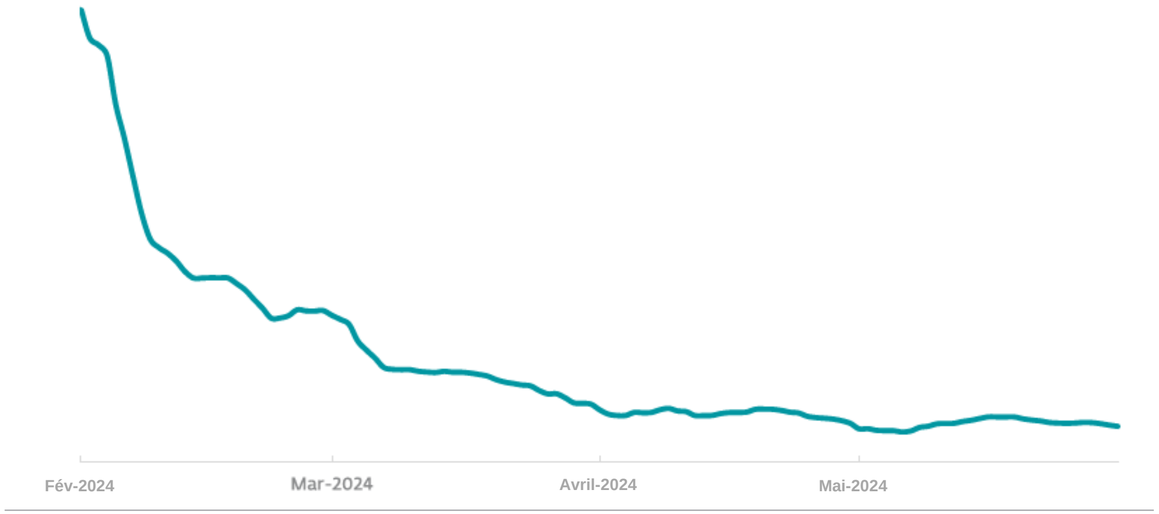
Au cours du premier semestre 2024, plus de 20 000 sites web ont été compromis par des injections de code JavaScript malveillant.

Comme indiqué dans notre rapport sur les menaces du second semestre 2023, l'exploitation des vulnérabilités des plugins WordPress est une technique d'accès initial privilégiée par le groupe Balada Injector. En janvier 2024, le groupe a de nouveau frappé, provoquant une nouvelle vague de JavaScripts malveillants de type JS/Agent dans les données télémétriques d'ESET.

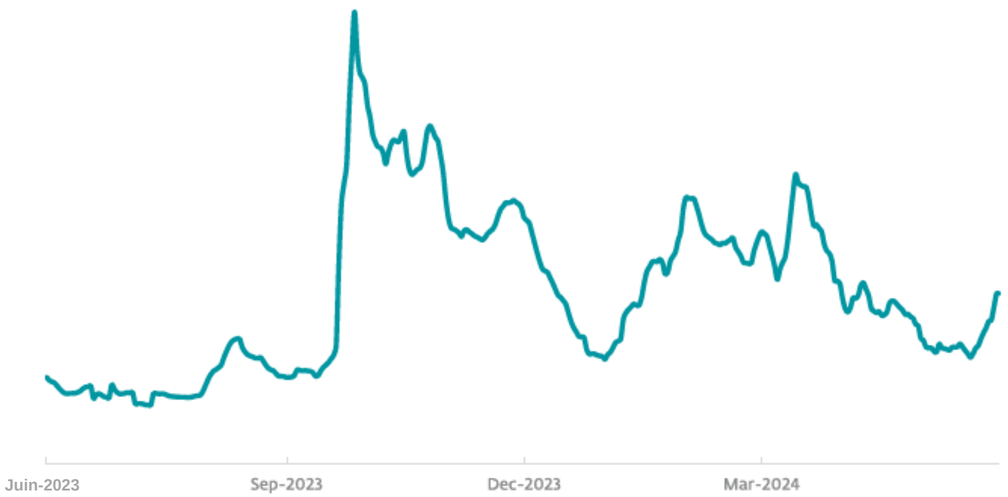
Les variantes détectées sont identiques ou similaires à celles décrites dans un article de blog de Sucuri, publié le même mois, concernant des attaques en cours contre des sites web utilisant des versions vulnérables du plugin WordPress Popup Builder. L'ensemble des scripts malveillants sont des morceaux de JavaScript légèrement obfusqués dont la principale fonction est de rediriger vers un serveur malveillant et de diffuser d'autres logiciels malveillants, ce qui conduit finalement à la compromission des comptes d'administrateurs et des serveurs web, à la diffusion de portes dérobées ou au ciblage des visiteurs du site web compromis.

La plupart des détections sont dues à JS/Agent.RJR, une nouvelle variante apparue pour la première fois en 2024. La Pologne (9 %), la France (7 %) et les États- Unis (6 %) représentent les plus grandes parts individuelles de ces détections ; cependant, .RJR est très répandu, notamment en Espagne, en Italie et en Allemagne (5 % chacun), ainsi qu'en Tchéquie (3 %). Fait intéressant, d'autres variantes, telles que .RKY et .RJZ, contiennent une autre variante : .RKA.

La télémétrie d'ESET a enregistré plus de 400 000 détections pour les variantes de Balada Injector utilisées dans le cadre de cette campagne, et le nombre de sites web affectés a dépassé les 20 000. Au premier semestre 2024, la variante .RJR a décroché la quatrième place parmi toutes les variantes JS/Agent, contribuant de manière significative aux hausses continues observées sur la tendance de cette famille depuis septembre 2023.



Tendance de détection de Balada Injector au premier semestre 2024, moyenne mobile sur sept jours



Tendance de détection de JS/Agent de juin 2023 à mai 2024, moyenne mobile sur sept jours

COMMENTAIRE D'EXPERT

Les scripts Balada Injector pouvant conduire au contrôle total de votre serveur web, veillez à les supprimer de votre site web et à mettre à jour tous les plugins vulnérables afin de prévenir d'éventuels exploits futurs. Les acteurs de la menace de Balada Injector ayant le don d'installer de multiples mécanismes de persistance, n'oubliez pas de les supprimer également en vérifiant la présence de comptes d'administrateurs indésirables et de fichiers malveillants sur votre serveur web, et en modifiant les informations d'identification.

Ján Adámek, ingénieur de détection principal chez ESET

Voleurs d'informations | Menaces web | Jeux vidéo

Rencontres programmées : les cybercriminels s'attaquent aux joueurs

Des voleurs d'informations menacent les données personnelles des amateurs de jeux vidéo.

Les jeux vidéo sont devenus une industrie de plusieurs milliards de dollars et ce succès attire naturellement la cybercriminalité. Certaines entreprises de jeux vidéo ont déjà été ciblées par des groupes de rançongiciels : l'attaque de rançongiciel la plus récente a eu lieu vers le début du premier semestre 2024, lorsque la société Insomniac Games, développeurs principalement connus pour leurs deux jeux à gros budget Spider-Man, a été victime d'une fuite de données à grande échelle après avoir refusé de payer une rançon au célèbre groupe de rançongiciels Rhysida. Des données sensibles, allant des informations personnelles des développeurs à la feuille de route des futurs jeux d'Insomniac Games, ont été publiées sur internet.

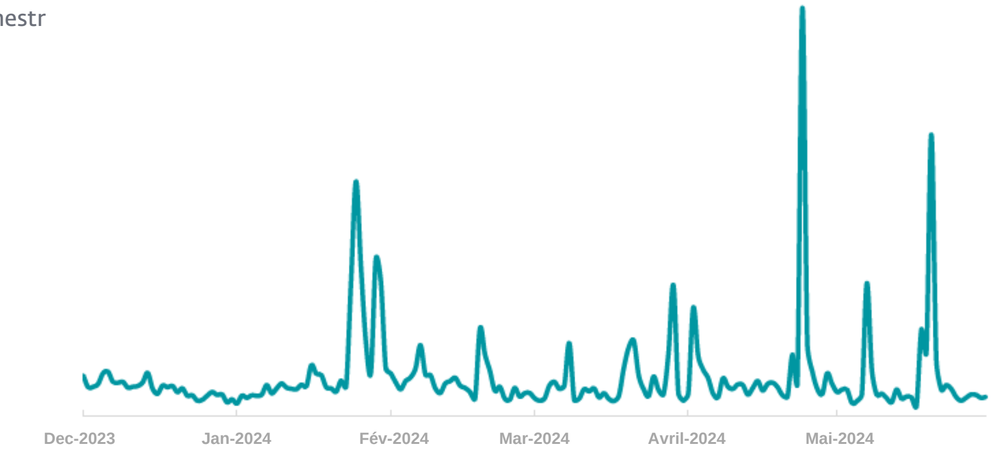
Néanmoins, les grandes entreprises ne sont pas les seules à être menacées ; les informations personnelles des joueurs de jeux vidéo constituent également une cible attrayante pour les cyberescrocs, comme en témoignent les acteurs de la menace qui dissimulent des charges utiles de logiciels malveillants dans toutes sortes de fichiers issus de jeux vidéo.

Les amateurs de jeux vidéo sont souvent confrontés à des logiciels malveillants en s'aventurant hors de l'écosystème officiel (boutiques, référentiels officiels de contenu de jeux vidéo) vers les eaux inconnues des sites de torrents et des serveurs Discord douteux proposant des jeux piratés et des outils de triche. C'est précisément dans ces zones grises que les criminels prospèrent : la possibilité d'obtenir un jeu gratuitement ou de réaliser des tirs en pleine tête à travers les murs à la perfection dans les jeux de tir multijoueurs constitue un appât parfait pour les joueurs peu méfiants. Une fois les victimes touchées, elles se retrouvent souvent face à des voleurs d'informations en quête de leurs mots de passe, de leurs informations de carte de crédit ou de leurs cryptomonnaies.

Voleurs d'informations à la demande

Ces attaques sont souvent menées à l'aide de voleurs d'informations distribués à la demande ; RedLine Stealer et Lumma Stealer, présentés dans les précédents rapports sur les menaces ESET, se sont avérés être les charges utiles de fichiers se faisant passer pour des logiciels de triche ou pour des cracks de jeux vidéo. Selon nos données de télémétrie, nous pouvons confirmer que ces deux menaces étaient encore très actives au premier semestr

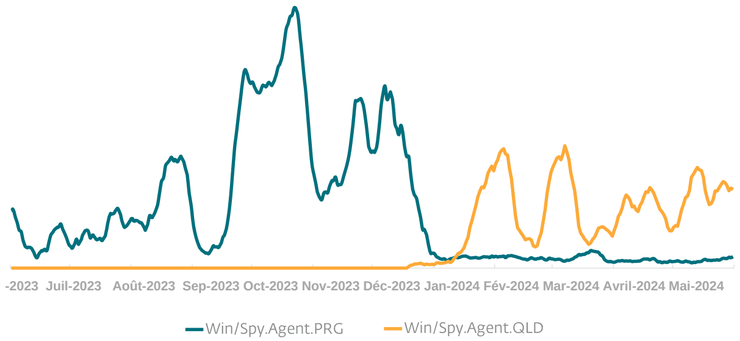
En ce qui concerne RedLine Stealer, il semble que ce voleur d'informations à gages refuse de disparaître, même après le démantèlement mené en 2023. Si RedLine Stealer n'est plus mis à jour,



Tendance de détection journalière de RedLine Stealer au premier semestre 2024

nos données indiquent qu'il est toujours en service, bien qu'il soit principalement relégué à des campagnes ponctuelles isolées dans un ou deux pays. En 2024, les trois plus gros pics de données le concernant ont été enregistrés le 25 janvier (50 % des détections enregistrées en Allemagne), le 24 avril (87 % en Espagne), et le 20 mai (91 % au Japon). Toutefois, ces pics ont été si importants que les détections de RedLine Stealer au premier semestre 2024 ont en effet dépassé celles du second semestre 2023, affichant une augmentation à hauteur de 31 %.

Après l'ascension fulgurante de Lumma Stealer au second semestre 2023, les détections de cette menace, qui cible principalement les cryptomonnaies, ont connu une baisse au premier semestre 2024. Cependant, il est intéressant de noter qu'il semble y avoir eu un changement dans les variantes de menaces spécifiques utilisées par cette famille de logiciels malveillants. Au second semestre 2023, ESET a enregistré des détections de Lumma Stealer principalement sous le nom de Win/Spy.Agent.PRG ; ces détections ont presque entièrement disparu en 2024. En revanche, à la fin de l'année 2023, le logiciel malveillant a été remplacé par une nouvelle variante dénommée Win/Spy.Agent.QLD. Contrairement à la variante .PRG, .QLD a affiché une croissance au premier semestre 2024.



Tendances de détection de Win/Spy.Agent.PRG et Win/Spy.Agent.QLD au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours

Des mods compromis

Les joueurs qui ne sont pas enclins à pirater des jeux ou à utiliser des outils de triche peuvent néanmoins tomber sur des fichiers nuisibles lorsqu'ils téléchargent d'autres éléments liés aux jeux vidéo. À titre d'exemple, les mods, qui sont des modifications apportées à un jeu vidéo par ses fans, peuvent également être compromis par des cybercriminels. Bien qu'il soit préférable de s'en tenir aux répertoires de mods réputés ou de passer par les plateformes officielles telles que Steam, il est arrivé que même ces dernières ne soient pas sans danger.

En juin 2023, des pirates informatiques ont réussi à compromettre plusieurs comptes sur des plateformes de modding Minecraft et ont injecté du code de vol d'informations dans des projets existants. Plus récemment, en décembre 2023, un mod populaire pour le jeu Slay the Spire a été piraté pour diffuser Epsilon Stealer (qu'ESET détecte comme étant le cheval de Troie JS/PSW.Agent, avec ses variantes .CH et .CI) par le biais du système de mise à jour de Steam. Dans ce cas, la meilleure ligne de défense consiste à utiliser un logiciel de sécurité à jour pour détecter les fichiers potentiellement malveillants.

MODS DE JEUX VIDÉO

Modifications de jeux vidéo existants, généralement développées par les fans et proposées gratuitement. Ces modifications peuvent ajouter de nouvelles fonctionnalités, changer l'apparence des modèles du jeu ou même ajouter de nouveaux éléments de jeu et de contenu scénaristique. Certains jeux vidéo populaires ont été créés à partir de mods très complets ; l'un des exemples les plus célèbres est le jeu de tir à la première personne Counter-Strike, qui a vu le jour en tant que mod pour Half-Life. Bien que de nombreux développeurs acceptent les mods créés par leur communauté, le modding de jeux occupe une zone d'ombre juridique en raison des lois sur les droits d'auteur.

CRACKS DE JEUX VIDÉO

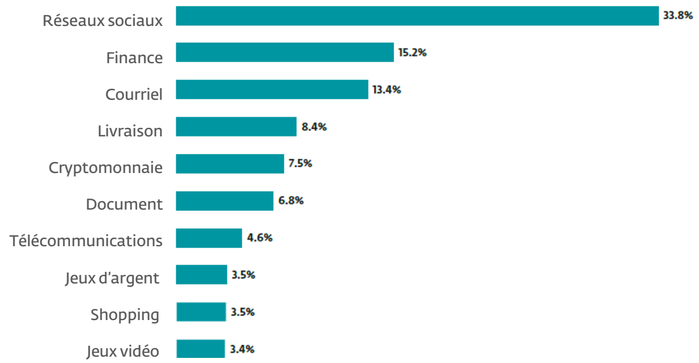
Versions de jeux dont la protection anticopie a été supprimée. Cette pratique est généralement utilisée pour contourner les mesures antipiratage.

OUTILS DE TRICHE

Principalement utilisés dans les jeux multijoueurs en ligne, les outils de triche sont des logiciels tiers permettant aux joueurs d'obtenir des avantages déloyaux sur les autres joueurs. À titre d'exemple, citons l'assistance à la visée dans les jeux de tir à la première personne (également connus sous le nom d'aimbots) et la possibilité pour les tricheurs de voir à travers les objets (wallhack).

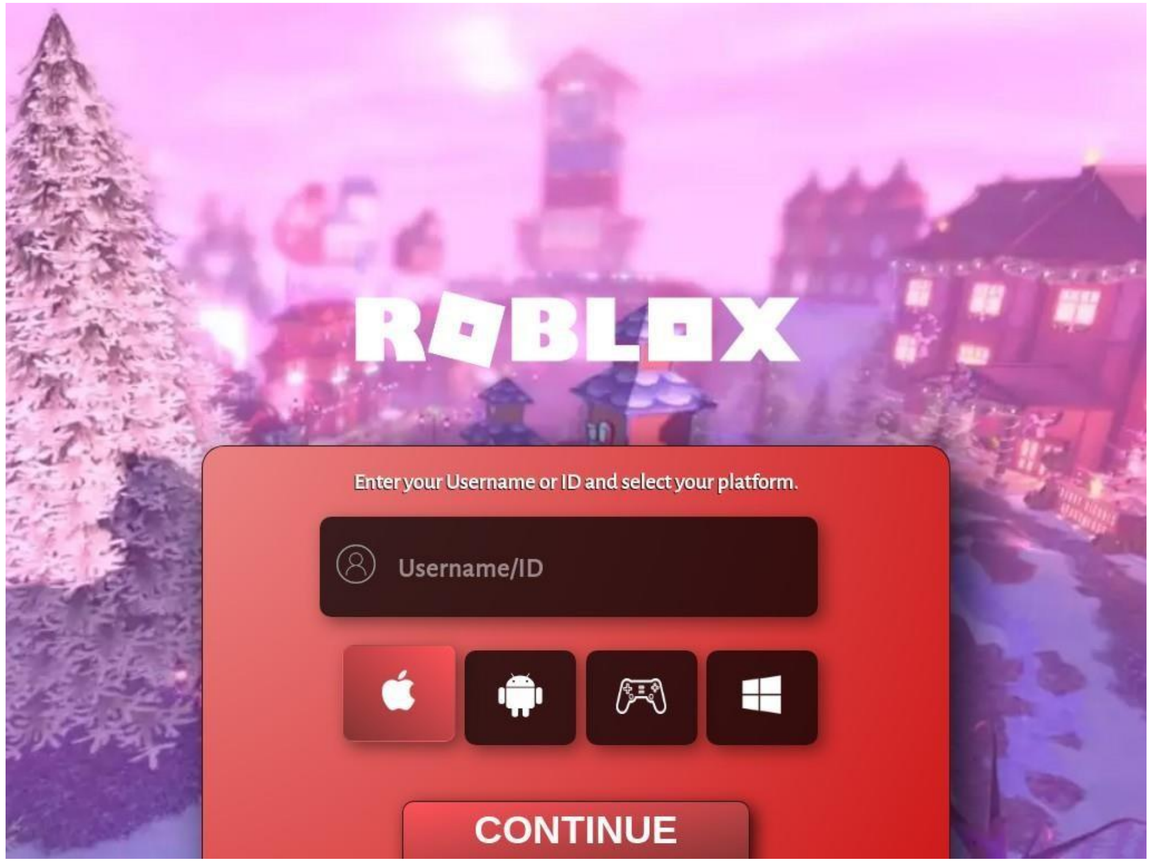
Escroqueries par hameçonnage

Non seulement les joueurs peuvent être amenés à télécharger des charges utiles malveillantes, mais ils peuvent également être victimes d'escroqueries par hameçonnage. Selon les données d'ESET sur l'hameçonnage, les jeux vidéo occupent la dixième place dans le classement des principales catégories de sites d'hameçonnage pour le premier semestre 2024.



Top 10 des catégories de sites d'hameçonnage au premier semestre 2024

L'hameçonnage peut s'avérer particulièrement dangereux lorsqu'il cible des jeux dont le public principal est constitué d'enfants. L'année dernière, Cisco Talos a publié un rapport sur les nombreuses façons dont Roblox, une plateforme de jeu de type bac à sable très populaire auprès des enfants, est exploitée par les cybercriminels. Les escroqueries par hameçonnage figurent en tête de la liste établie par Cisco Talos. Étant donné que Roblox contient une monnaie virtuelle appelée Robux qui peut être achetée avec de l'argent réel, il constitue une cible hautement privilégiée pour les cybercriminels. Nos données sur l'hameçonnage ont révélé plusieurs cas de faux écrans de connexion à Roblox ou de sites web prétendant distribuer des Robux aux personnes qui s'y connectent.



Site d'hameçonnage se faisant passer pour Roblox à l'adresse robuq[.]com

Downloaders

Les downloaders changent de méthode de diffusion et font leur grand retour

Après les bouleversements survenus en 2022, les menaces liées aux downloaders refont peu à peu surface.

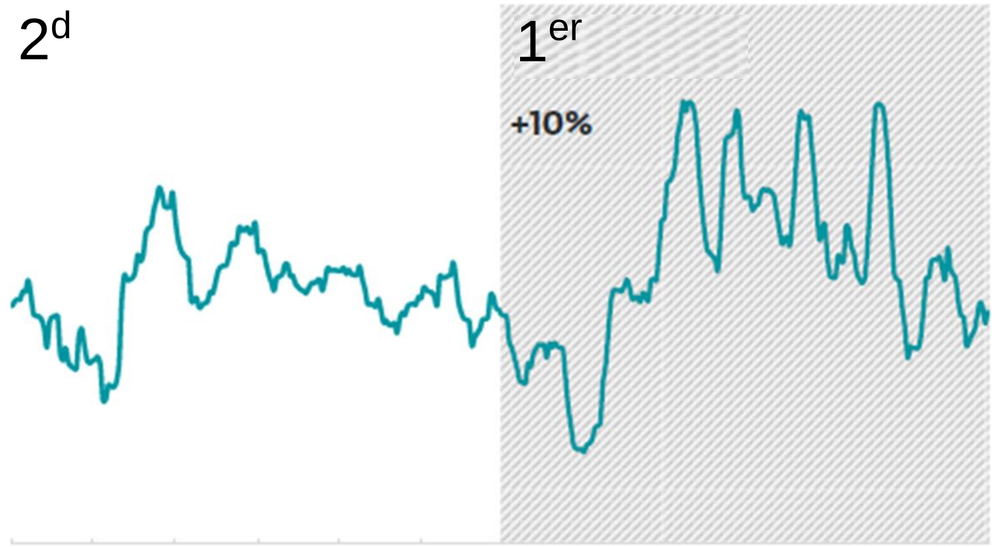
Avec la désactivation par Microsoft des macros Internet en 2022, les downloaders (téléchargeurs) malveillants ont été fortement perturbés, en particulier ceux qui utilisent des macros. La disparition ultérieure d'Emotet, qui s'appuyait largement sur ce vecteur d'attaque, n'a fait que confirmer que l'âge d'or des downloaders était révolu. Ce phénomène a été clairement identifié grâce à la télémétrie d'ESET : entre 2022 et 2023, les données montrent une baisse de 65 % du nombre de downloaders. Cependant, à partir du second semestre 2023, ces menaces ont lentement repris du terrain. Au second semestre 2023, ils affichaient déjà une hausse de 10 % par rapport au premier semestre de la même année, et cette tendance à la hausse s'est poursuivie au premier semestre 2024, avec une nouvelle augmentation de 10 %.

L'augmentation du premier semestre 2024 concerne effectivement la majorité des downloaders que nous surveillons. Parmi les 10 premiers downloaders détectés au cours de cette période, seuls deux d'entre eux n'ont pas connu de croissance significative.

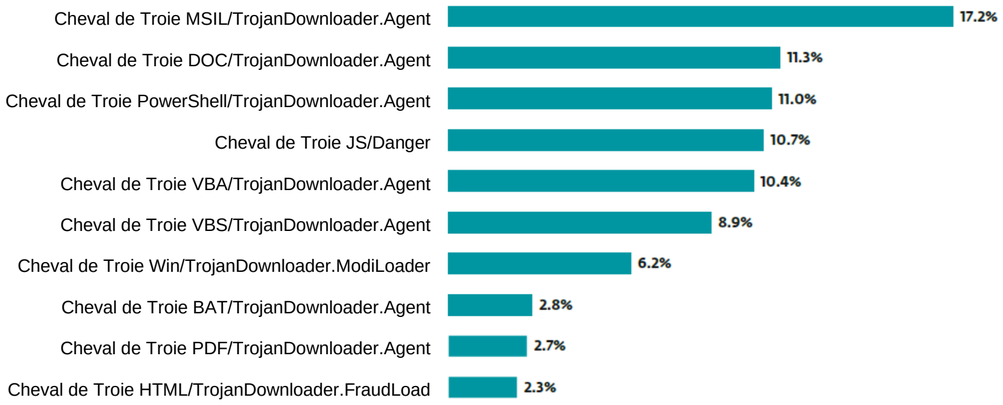
D'après les données télémétriques d'ESET, ce phénomène a commencé à la fin du mois de janvier et se poursuit depuis, ce qui laisse supposer une activité accrue des acteurs de la menace dans ce domaine.

Pour rester dans la course une fois les macros automatiques désactivées, de nombreux cybercriminels ont décidé de modifier leurs méthodes de diffusion. C'est pourquoi, de nos jours, les downloaders les plus répandus se présentent sous la forme de courriels de spam dont les pièces jointes contiennent des scripts malveillants ne reposant pas sur des macros. Ceux-ci sont exécutés après que la victime a cliqué dessus.

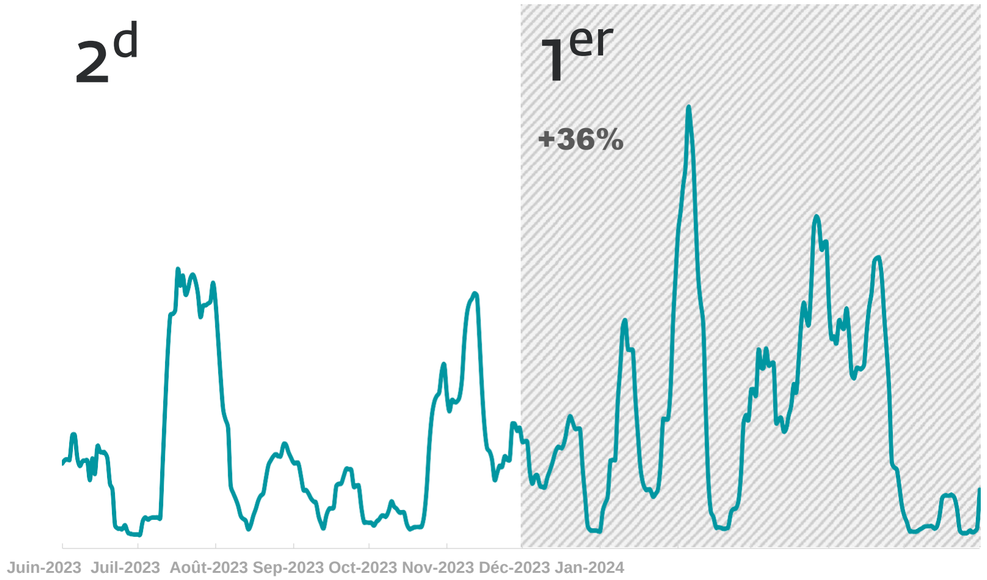
Cette évolution se manifeste notamment par l'augmentation du nombre de courriels contenant des pièces jointes JavaScript malveillantes, répertoriées dans nos données télémétriques sous le nom de cheval de Troie JS/Danger. Après une forte baisse des détections au début de l'année 2021, cette famille de logiciels malveillants semble connaître une renaissance, avec une augmentation de 36 % au



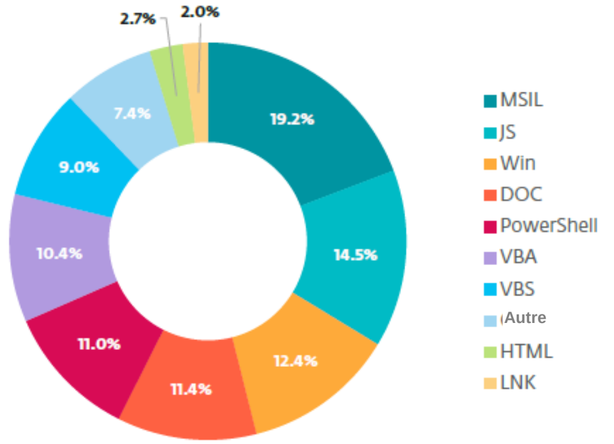
Tendance de détection des downloaders au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours



Top 10 des détections de downloaders au premier semestre 2024 (% des détections de downloaders)



Tendance de détection du cheval de Troie JS/Danger au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours



Détections de downloaders par type de détection au premier semestre 2024

premier semestre 2024. Au cours de la même période, les downloaders JS sont également devenus la deuxième catégorie de downloaders la plus répandue dans la télémétrie d'ESET.

L'augmentation globale du nombre de downloaders va de pair avec l'augmentation du nombre de détections de familles de logiciels malveillants qu'ils diffusent. Ainsi, les deux plus grands pics de détection de VBS/TrojanDownloader.Agent aux États-Unis (9 février et 8 mars) ont été provoqués par des variantes téléchargeant l'Agent Tesla, un voleur d'informations notoire qui a connu une augmentation de 40 % au premier semestre 2024.

Fait intéressant, même les menaces qui s'appuient sur des macros ont connu une croissance au premier semestre 2024 : la famille de chevaux de Troie VBA/TrojanDownloader.Agent a enregistré une hausse de 24 %. Nous avons également enregistré un pic de détection provoqué par VBA/TrojanDownloader.Agent.EGF, le 22 février. Cette variante se présente sous la forme d'une macro de document Word qui exécute un court script PowerShell de téléchargement utilisé pour télécharger d'autres logiciels malveillants.

COMMENTAIRE D'EXPERT

L'augmentation du nombre de downloaders dépendants des macros pourrait n'être qu'une simple coïncidence. Les acteurs de la menace continuent de faire circuler ces menaces dans l'espoir qu'au moins une fraction de la population activera manuellement les macros dans ses documents Microsoft. En ce sens, l'approche des criminels est similaire à celle des tristement célèbres systèmes de courriels d'avance de frais qui garantissent des gains trop beaux pour être vrais. Le petit nombre de personnes qui tombent dans le panneau est suffisant pour que l'escroquerie soit rentable pour les criminels.

Dušan Lacika, ingénieur de détection principal chez ESET

Rançongiciel

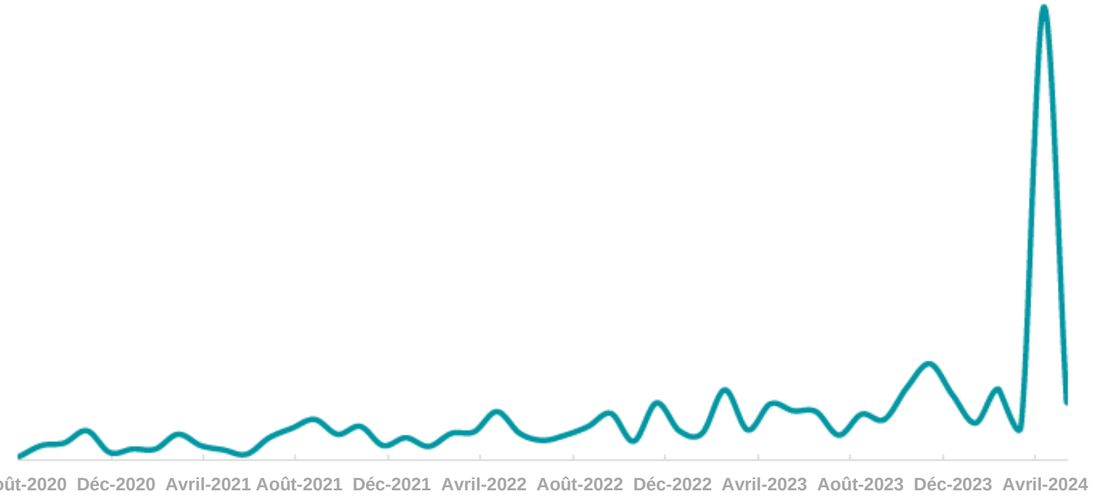
Bilan de LockBit : quel est leur avenir à la suite de l'opération Cronos ?

Au lendemain de ce démantèlement, l'avenir du groupe du rançongiciel LockBit montre des signes de lutte, tandis que d'autres acteurs de la menace utilisant la fuite du builder de LockBit se profilent à l'horizon.

Issu en 2019 d'une famille de rançongiciels connue sous le nom d'ABCD, LockBit est devenu un acteur puissant du paysage des rançongiciels, occupant, semble-t-il, la première place du classement du nombre d'attaques de rançongiciels dans le monde entre septembre 2023 et avril 2024. LockBit a ensuite perdu ce titre à la suite du bannissement de LockBitSupp, le célèbre représentant public de LockBit, des forums de piratage tels que XSS et Exploit et, plus important encore, de l'opération Cronos, un démantèlement mondial coordonné par l'Agence nationale britannique de lutte contre la criminalité, Europol et Eurojust en février 2024.

Ce démantèlement a conduit à l'arrestation de deux affiliés de LockBit en Pologne et en Ukraine, tandis que les autorités judiciaires françaises et américaines ont émis des actes d'accusation et des mandats d'arrêt internationaux à l'encontre de plusieurs co-conspirateurs de LockBit. En outre, les forces de l'ordre ont réussi à confisquer plus de 200 portefeuilles de cryptomonnaies, à trouver une liste de près de 200 noms d'affiliés, démasqué la véritable identité de LockBitSupp, et ont développé et publié un outil de décryptage.

La télémétrie d'ESET confirme que le groupe LockBit a du mal à s'en sortir. Nous avons observé deux campagnes LockBit notables depuis le démantèlement, bien qu'il s'agisse dans les deux cas d'échantillons construits à l'aide du constructeur de LockBit qui a fait l'objet d'une fuite en septembre 2022. Un signe révélateur de l'utilisation de cet outil par des groupes n'appartenant pas à LockBit réside dans les notes de



Tendance de détection quotidienne du rançongiciel LockBit depuis août 2020

Les rançongiciels constituent généralement la charge utile finale d'une chaîne de menaces qui peut être précédée d'un hameçonnage, d'une exploitation, d'une attaque par force brute, d'une compromission d'informations d'identification,de downloaders ou de logiciels malveillants sur mesure. De nombreuses attaques par rançongiciels potentielles ne sont donc probablement jamais réalisées, car elles sont détectées à un stade précoce du cycle de vie de l'attaque. Si les attaquants parviennent à exploiter des vulnérabilités ou d'autres failles dans la défense d'une organisation et sont en mesure de déployer un rançongiciel, les produits de sécurité réputés seront en mesure de détecter ce dernier maillon de la chaîne.

rançon : contrairement à celles du groupe LockBit, qui renvoient la victime vers un site de fuite de LockBit, celles de ces échantillons n'indiquent généralement qu'un courriel ou un contact Tox.

L'une des campagnes mentionnées ci-dessus s'est déroulée juste après le démantèlement de février. De nombreux acteurs de la menace ont tenté de diffuser LockBit en exploitant les vulnérabilités CVE-2024-1708 et CVE- 2024-1709 de ScreenConnect, qui venaient alors d'être rendues publiques. Les victimes appartenaient à divers secteurs d'activité, principalement basés en Europe et aux États-Unis.

L'autre était une campagne de courriels malveillants lancée à la mi-avril 2024, qui diffusait le rançongiciel LockBit par le biais de pièces jointes à des courriels. Le format et le nom de la pièce jointe, ainsi que le corps de texte du courriel, suggèrent un ciblage généralisé, sans ciblage de secteur d'activité particulier. Selon un rapport, le botnet Phorpiex est responsable de l'envoi de ces courriels malveillants.

LockBit est généralement une menace très ciblée ; cependant, en raison de la portée considérable de cette campagne, elle a considérablement marqué la télémétrie d'ESET concernant LockBit, provoquant un pic important le 17 avril 2024.

COMMENTAIRE D'EXPERT

Contrairement à ce que l'on pouvait penser au départ, les effets de l'opération Cronos se manifestent déjà : LockBit a été détrôné de sa première place et tente désespérément de défendre sa position en affichant d'anciennes victimes sur ses sites de fuites.

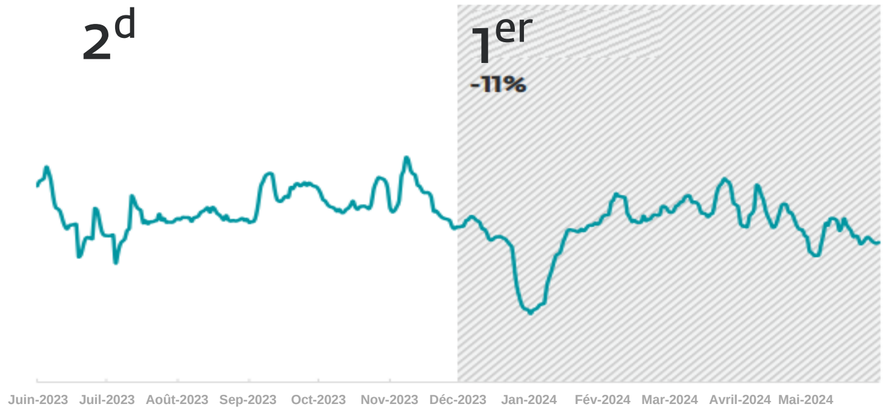
Le paysage des rançongiciels a encore été bouleversé par l'**escroquerie de sortie** organisée par BlackCat au lendemain de l'incident impliquant Change Healthcare. RansomHub, un groupe apparu pour la première fois à la mi-février, et Play, un groupe plus ancien actif depuis la mi-2022, ont tous deux profité de cette occasion pour attirer de nouveaux affiliés et tenter de grimper dans la hiérarchie des rançongiciels à la demande.

Les données publiées sur les sites de fuite indiquent que le nombre d'attaques de rançongiciels au premier trimestre 2024 a augmenté de plus de 20 % par rapport au trimestre précédent. Toutefois, nous estimons que ce nombre sera inférieur au deuxième trimestre 2024, notamment en raison de la fragilisation de certains des groupes cités précédemment et du chaos qui s'installe dans le paysage. Cela ne signifie pas que les rançongiciels à la demande vont disparaître ; le second semestre 2024 offrira certainement une image plus claire des groupes vers lesquels les affiliés insatisfaits se tournent, et les classements des rançongiciels refléteront ces changements d'alliance.

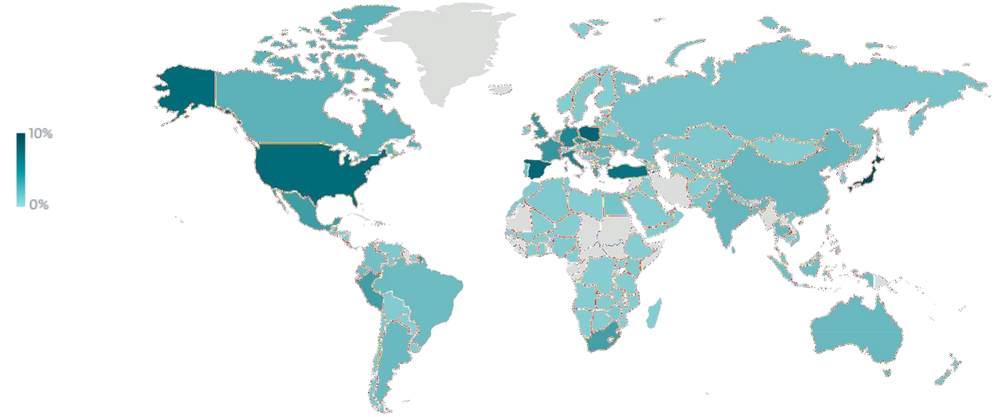
Jakub Souček, chercheur en logiciels malveillants principal chez ESET

Télémétrie des menaces

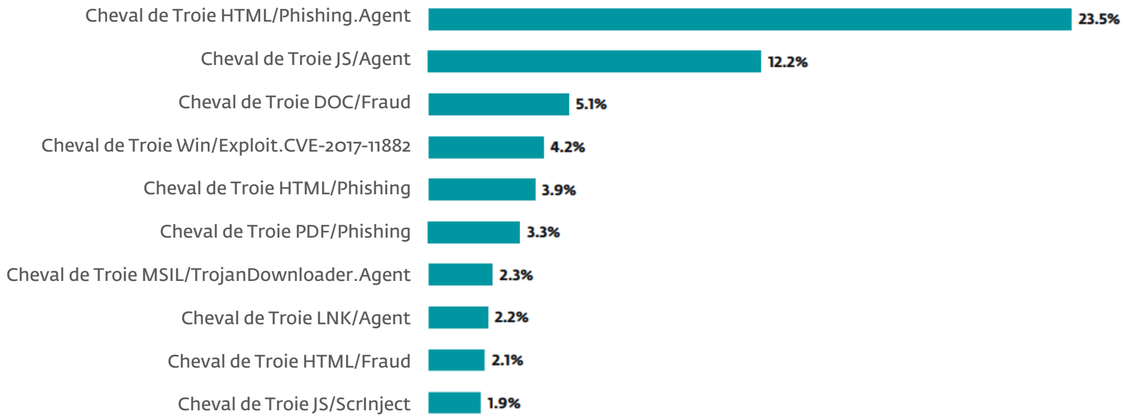
Ensemble des menaces



Tendance de détection des menaces au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours

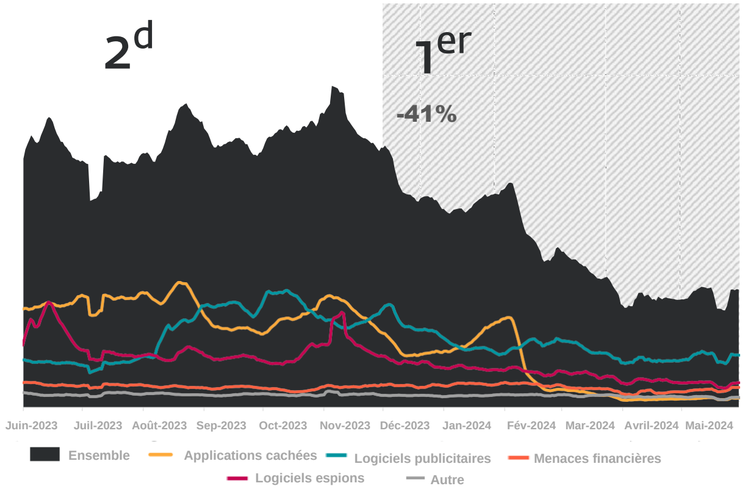


Répartition géographique des détections de logiciels malveillants au premier semestre 2024

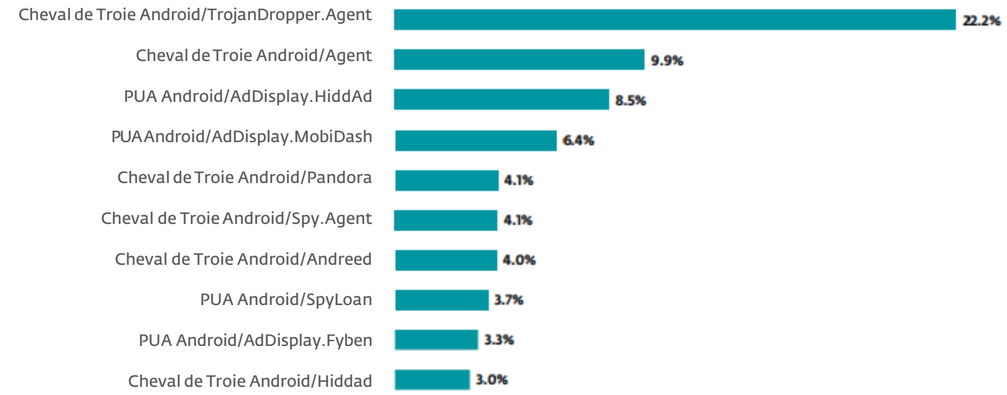


Top 10 des détections de logiciels malveillants au premier semestre 2024 (% de détection de logiciels malveillants)

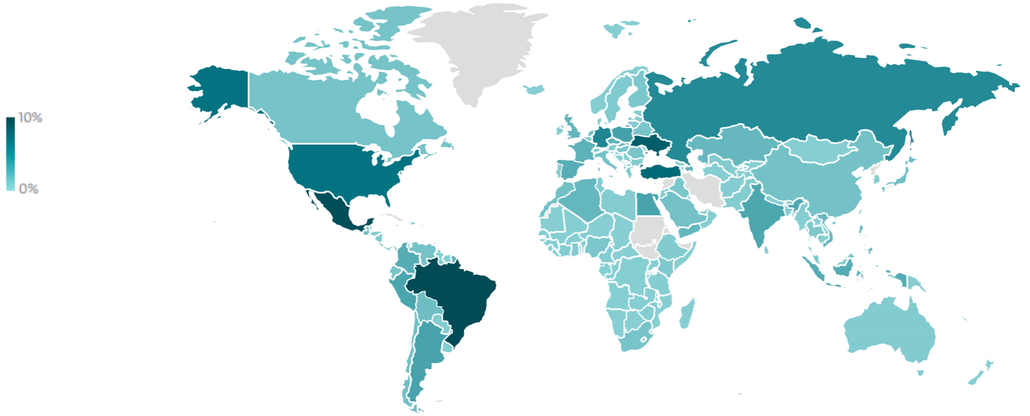
Android



Tendances de détection de certaines catégories de détection sous Android au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours (la ligne Autres regroupe les tendances des clickers, mineurs de cryptomonnaie, rançongiciels, applications frauduleuses, chevaux de Troie SMS et logiciels traqueurs)

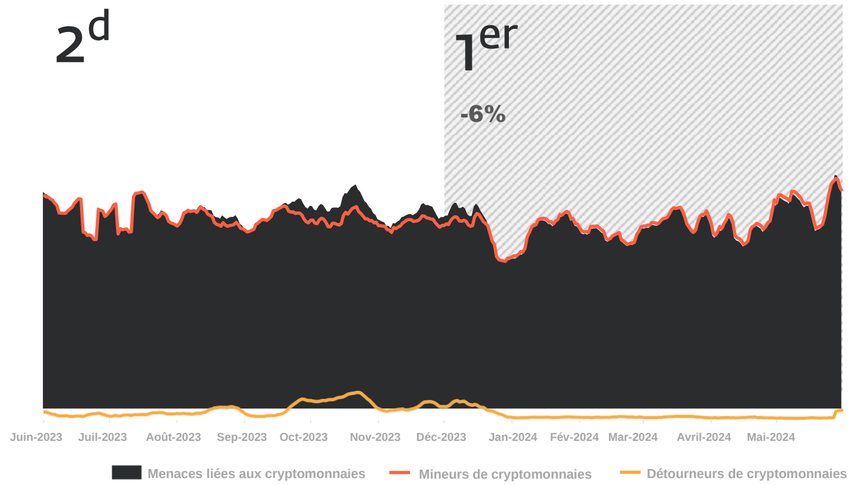


Top 10 des détections sous Android au premier semestre 2024 (% de détection sous Android)

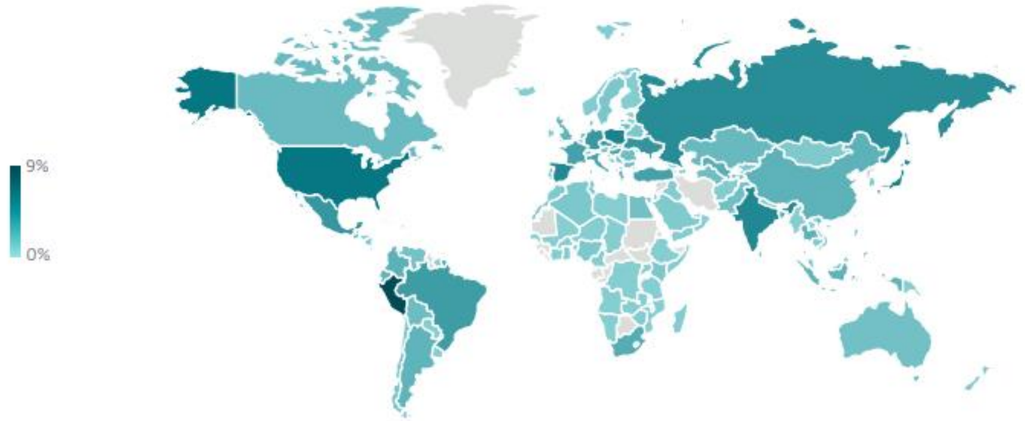


Répartition géographique des détections sous Android au premier semestre 2024

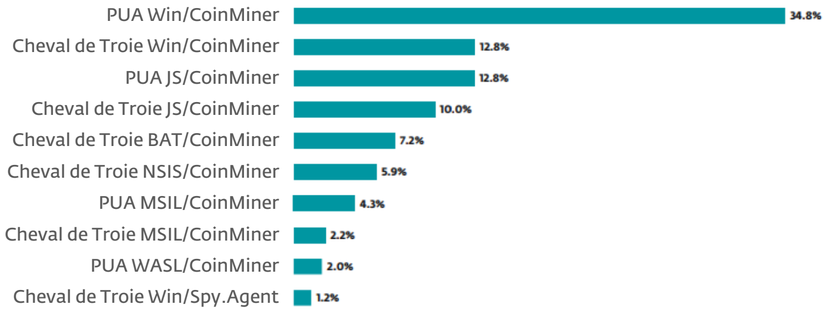
Menaces liées aux cryptomonnaies



Tendance de détection des menaces liées aux cryptomonnaies au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours

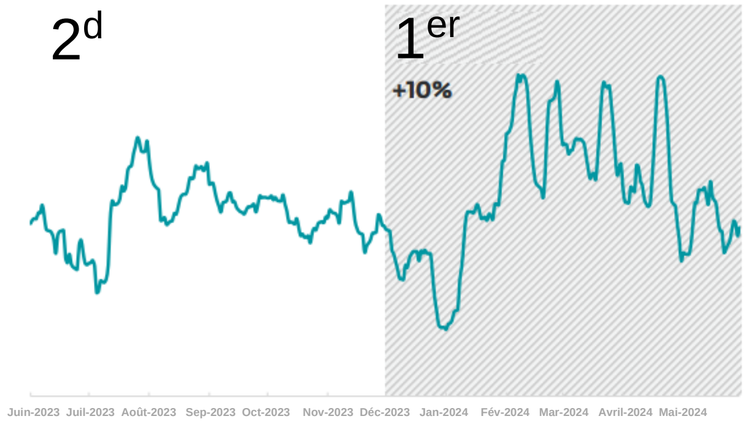


Répartition géographique des détections de menaces liées aux cryptomonnaies au premier semestre 2024

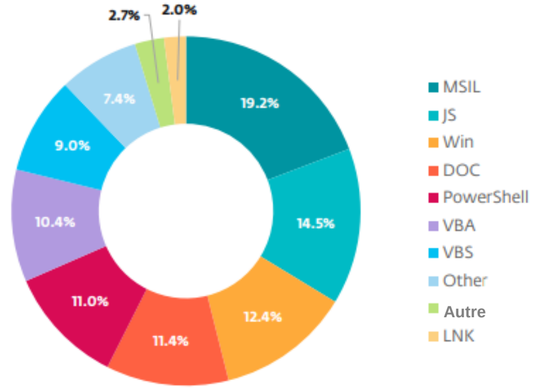


Top 10 des détections de menaces liées aux cryptomonnaies au premier semestre 2024 (% de détection de menaces liées aux cryptomonnaies)

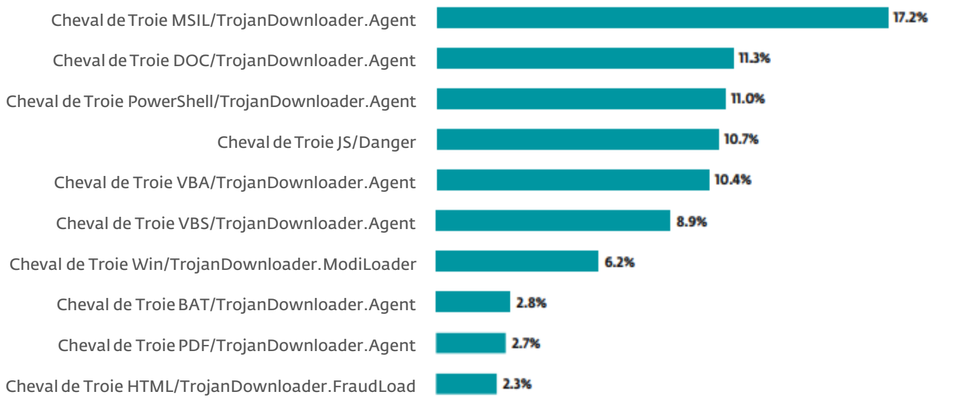
Downloaders



Tendance de détection des downloaders au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours



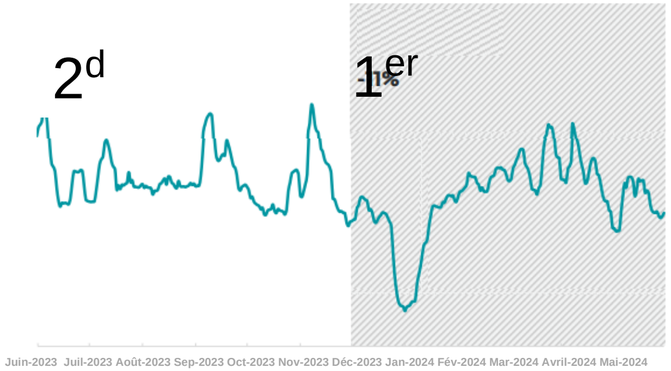
Détections de downloaders par type de détection au premier semestre 2024



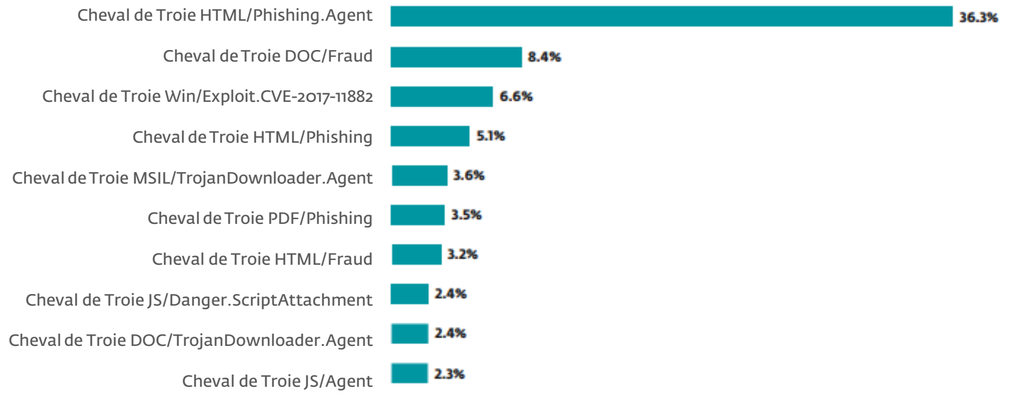
Top 10 des détections de downloaders au premier semestre 2024 (% de détections de downloaders)

Répartition géographique des détections de downloaders au premier semestre 2024

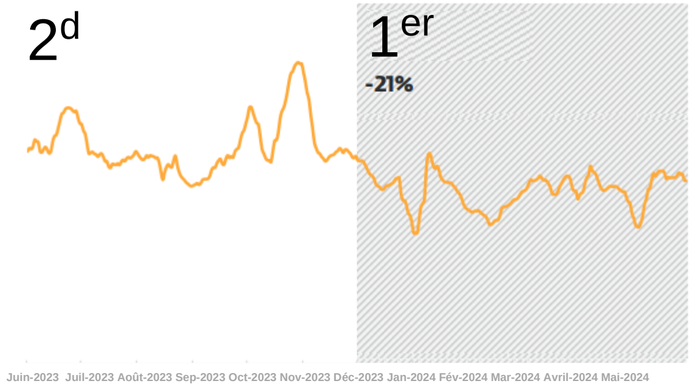
Menaces liées aux courriels



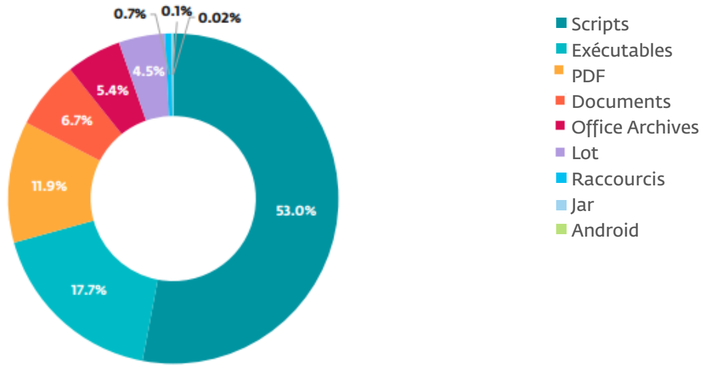
Tendance de détection des courriels malveillants au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours



10 menaces détectées dans les courriels au premier semestre 2024

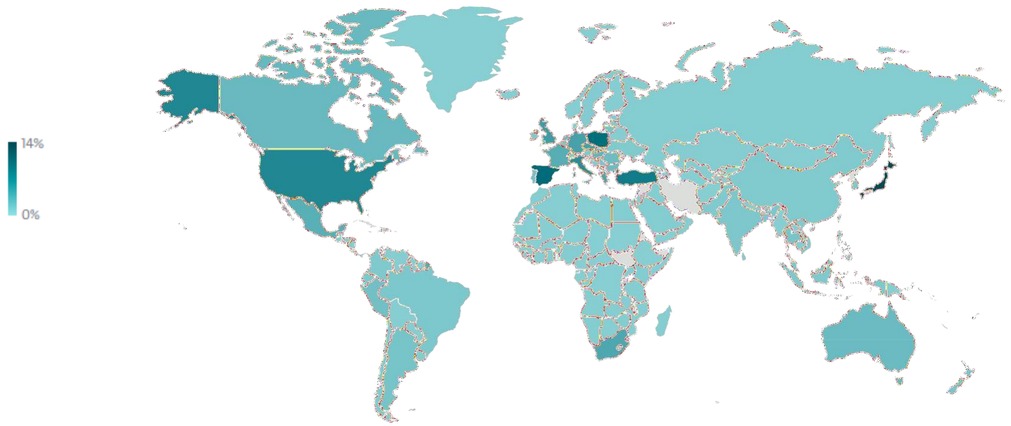


Tendance de détection des spams au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours



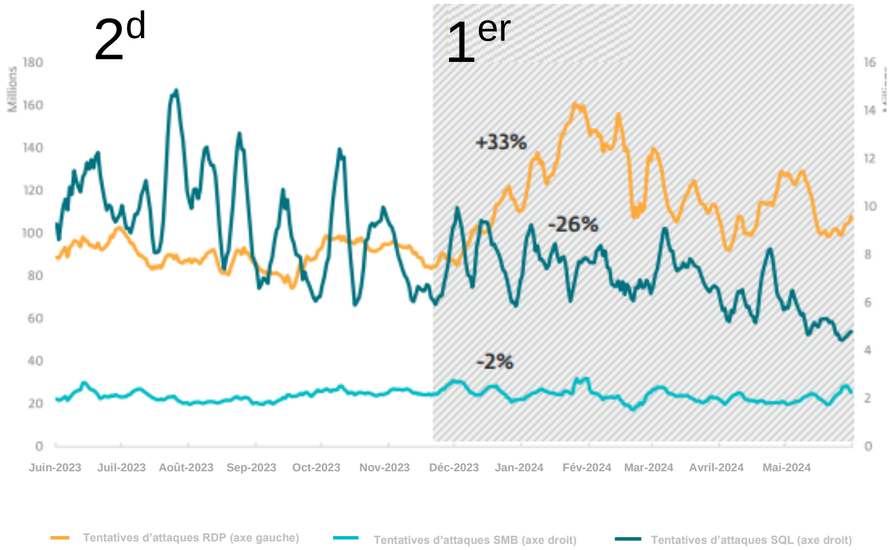
Principaux types de pièces jointes au premier semestre 2024

Menaces liées aux courriels

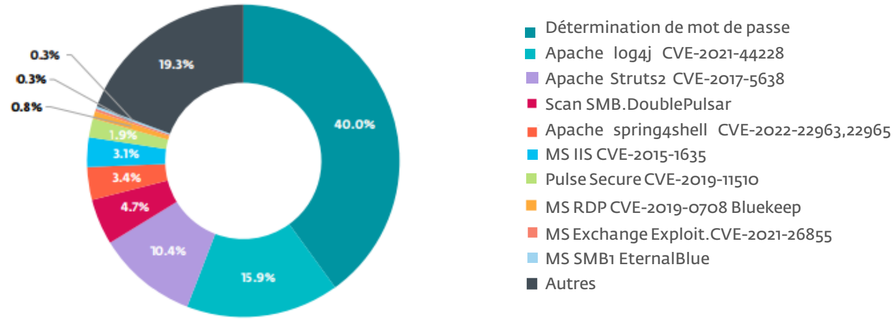


Répartition géographique des détections de menaces liées aux courriels au premier semestre 2024

Exploits

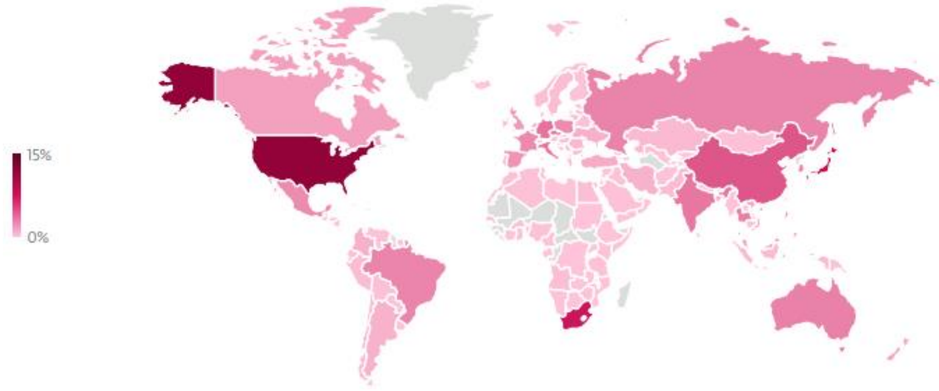


Tendances des tentatives d'attaques RDP, SMB et SQL au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours



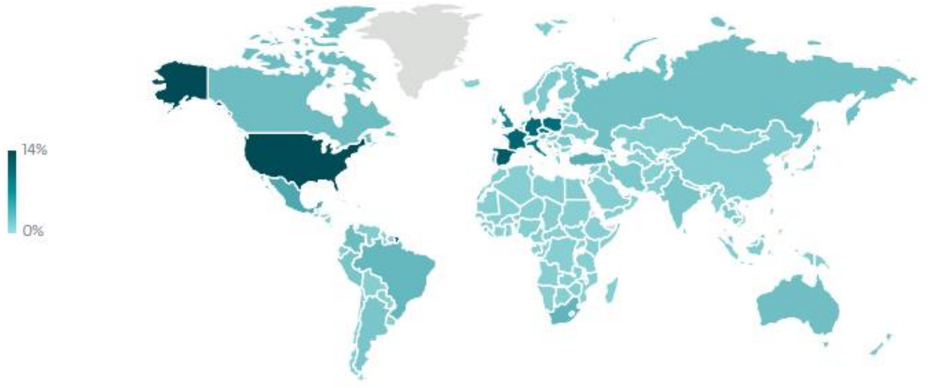
Vecteurs d'intrusion dans les réseaux externes signalés par des clients uniques au premier semestre 2024

Exploits

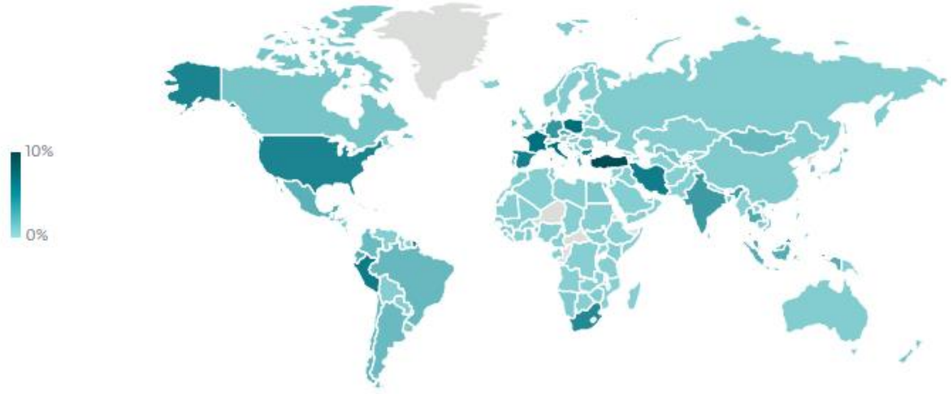


Répartition géographique des sources de tentatives d'attaques RDP par détermination de mot de passe au premier semestre 2024

Répartition géographique des cibles de tentatives d'attaques SMB par détermination de mot de passe au premier semestre 2024

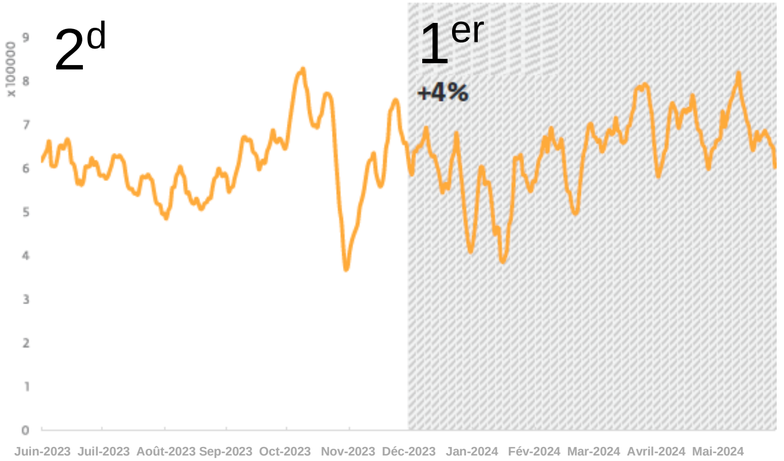


Répartition géographique des cibles de tentatives d'attaques RDP par détermination de mot de passe au premier semestre 2024

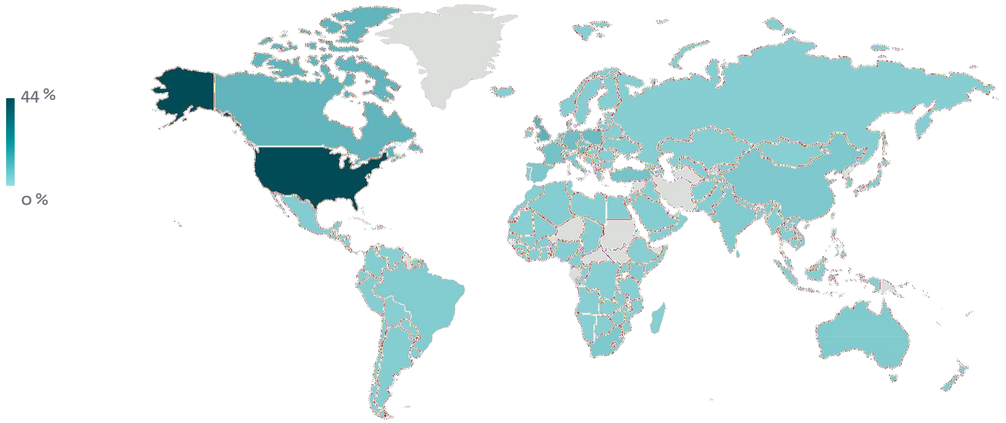


Répartition géographique des cibles de tentatives d'attaques SQL par détermination de mot de passe au premier semestre 2024

Exploits

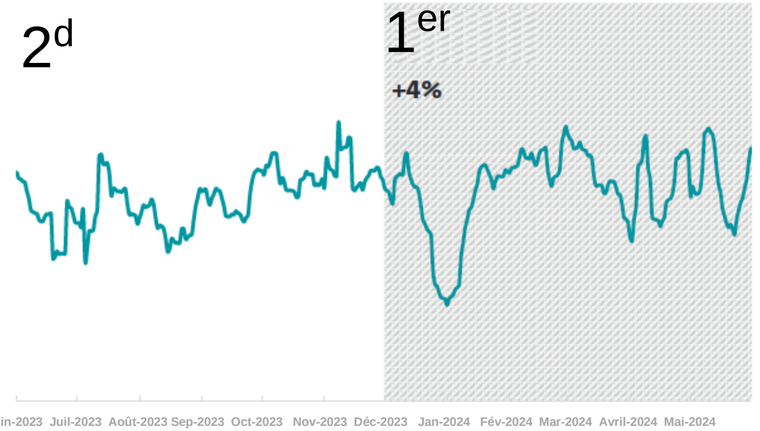


Tendance de détection des tentatives d'exploitation de Log4Shell au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours

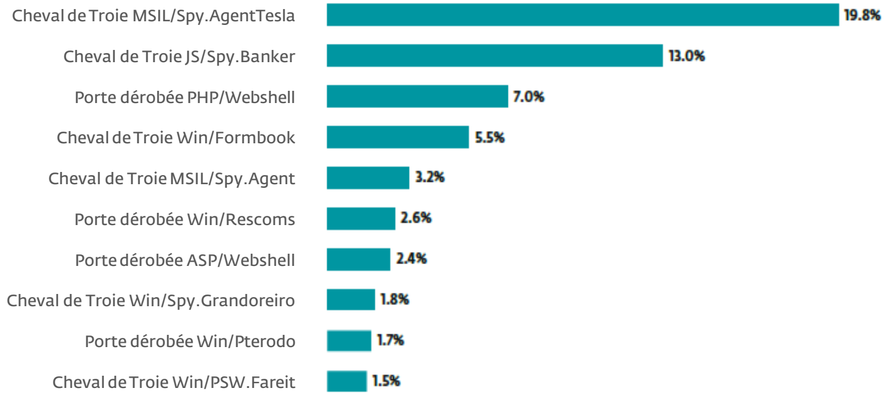


Répartition géographique des tentatives d'exploitation de Log4Shell au premier semestre 2024

Voleurs d'informations

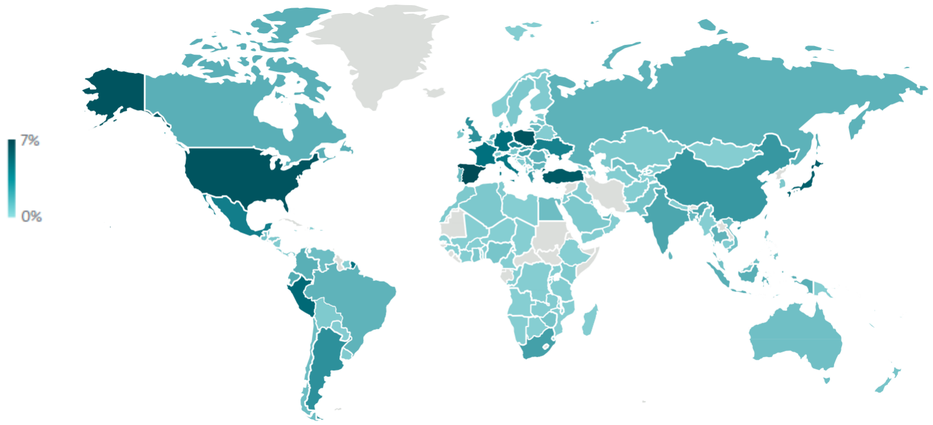


Tendance de détection des voleurs d'informations au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours



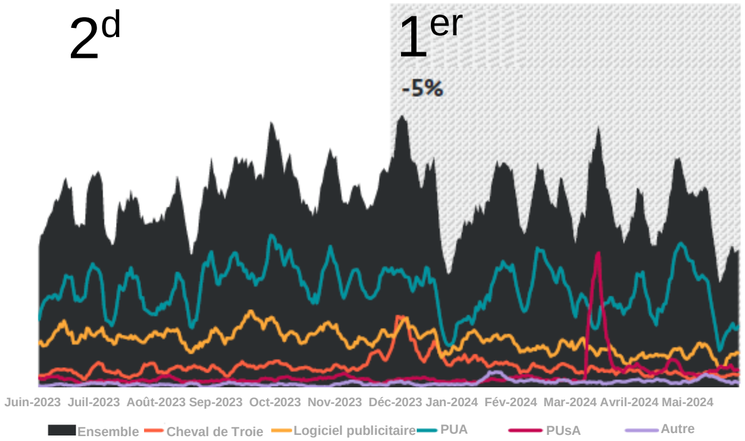
Top 10 des familles de voleurs d'informations au premier semestre 2024 (% de détection de voleurs d'informations)

Voleurs d'informations

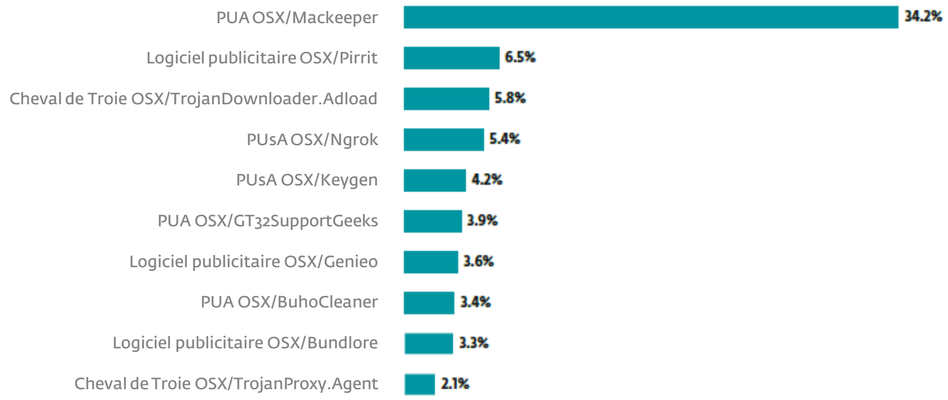


Répartition géographique des détections de voleurs d'informations au premier semestre 2023

macOS

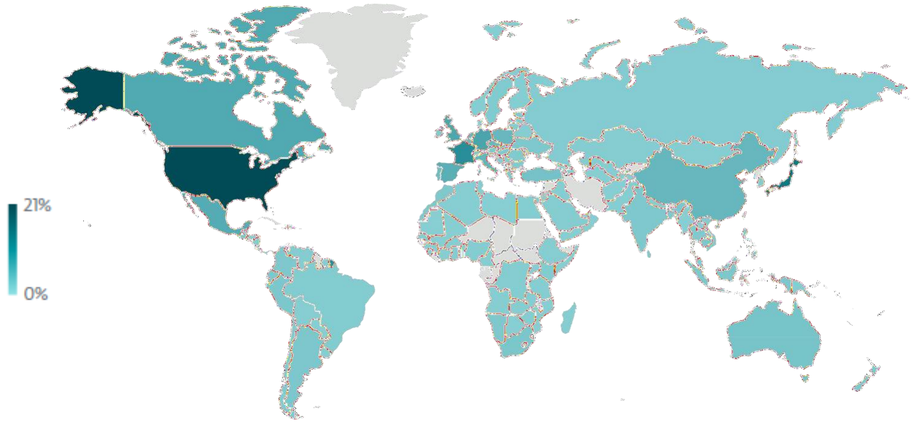


Tendance de détection sous macOS au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours



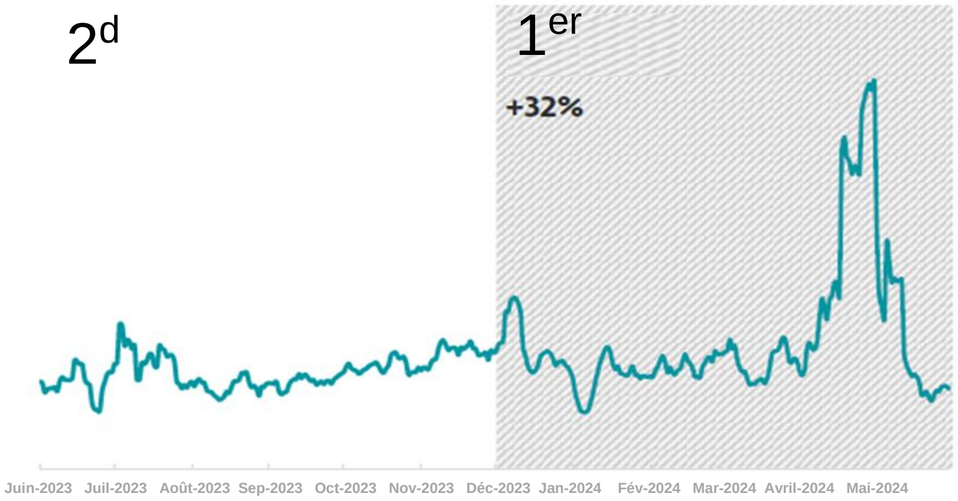
Top 10 des détections sous macOS au premier semestre 2024 (% de détection sous macOS)

macOS

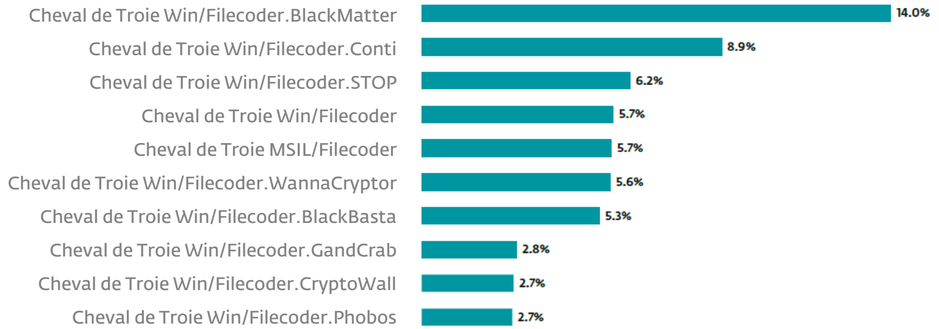


Répartition géographique des détections sous macOS au premier semestre 2024

Rançongiciels

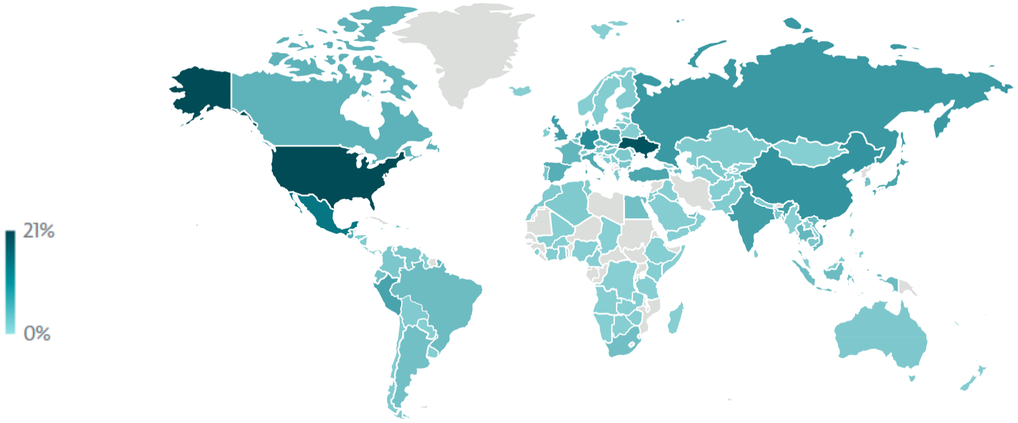


Tendance de détection de rançongiciels au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours



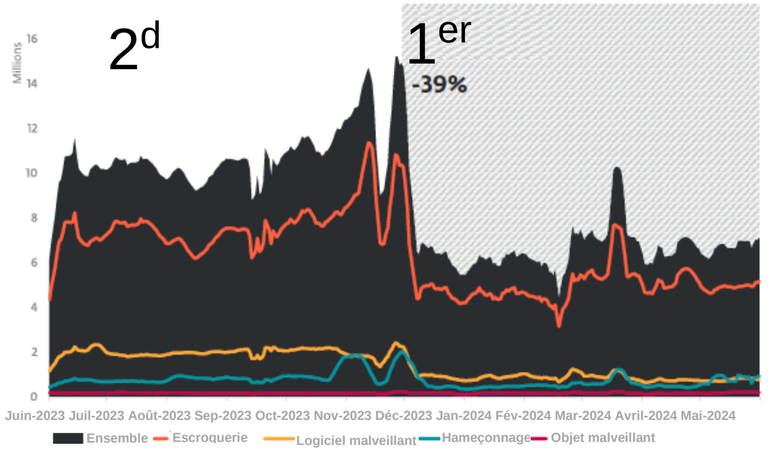
Top 10 des détections de rançongiciels au premier semestre 2024 (% de détection de rançongiciels)

Rançongiciel

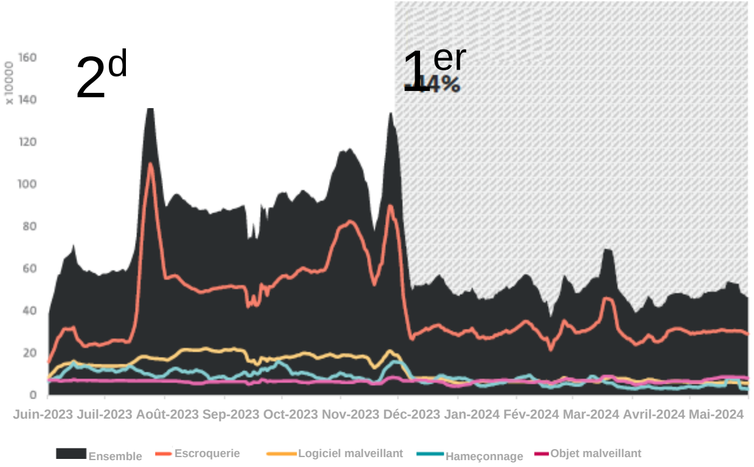


Répartition géographique des détections de rançongiciels au premier semestre 2024

Menaces web



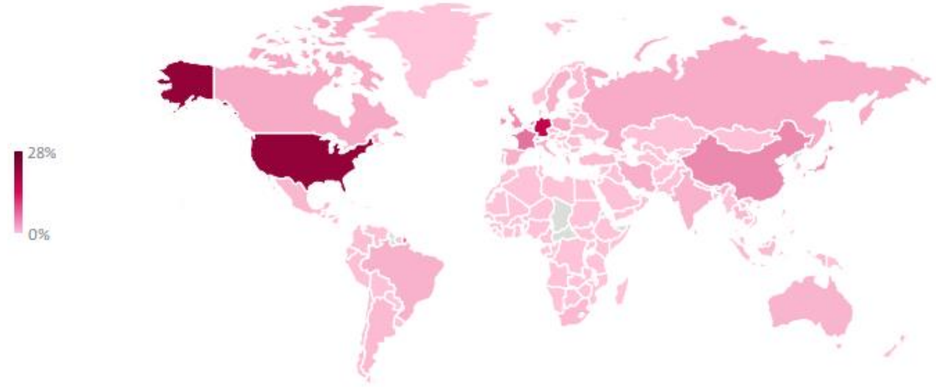
Tendance du blocage des menaces web au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours



Tendance de blocage des URL uniques au second semestre 2023 et au premier semestre 2024, moyenne mobile sur sept jours

Menaces web

Répartition mondiale des blocages de menaces web au premier semestre 2024



Répartition mondiale des hébergements de domaines bloqués au premier semestre 2024

Publications de recherche

Gare aux fausses technologies financières : les usuriers utilisent des applications Android pour atteindre de nouveaux sommets

Les chercheurs d'ESET font état de la montée en puissance des applications de prêt trompeuses pour Android et des techniques qu'elles utilisent pour contourner Google Play

Un pot-pourri pernicieux de paquets Python au sein de PyPI

Au cours de l'année écoulée, plus de 10 000 paquets malveillants hébergés sur le dépôt officiel de paquets Python ont été téléchargés

Attaques incessantes d'OilRig à l'aide de downloaders alimentés par des services en nuage

Les chercheurs d'ESET font état d'une série de nouveaux downloaders d'OilRig, qui s'appuient tous sur des fournisseurs de services en nuage légitimes pour les communications C&C

Podcast ESET Research : Neanderthals, Mammoths et Telekopye

Les chercheurs d'ESET discutent de la dynamique au sein et entre les différents groupes d'escrocs utilisant un robot Telegram baptisé Telekopye pour escroquer les gens sur les marchés en ligne

NSPX30 : un implant de pointe adapté à l'AitM en évolution depuis 2005

Les chercheurs d'ESET ont découvert NSPX30, un implant de pointe utilisé par un nouveau groupe APT affilié à la Chine, que nous avons baptisé Blackwood

ESET au cœur d'une opération mondiale pour démanteler le cheval de Troie bancaire Grandoreiro

ESET a fourni une analyse technique, des informations statistiques et des serveurs C&C identifiés tout en ayant un aperçu de la victimologie

Podcast ESET Research : ChatGPT, le piratage de MOVEit et Pandora

Un agent de dialogue basé sur l'IA déclenche par inadvertance une vague de cybercriminalité, des criminels spécialisés dans les rançongiciels pillent les entreprises sans déployer de rançongiciel, et un nouveau botnet prend en otage les téléviseurs Android

VajraSpy : un Patchwork d'applications d'espionnage

Les chercheurs d'ESET ont découvert plusieurs applications Android contenant VajraSpy, un cheval de Troie d'accès à distance utilisé par le groupe APT Patchwork

Operation Texonto : une campagne de désinformation ciblant les porte-parole ukrainiens dans un contexte de guerre

Mélange d'opération de désinformation, d'espionnage et de fausses pharmacies canadiennes !

Evasive Panda détourne le festival Monlam pour cibler des Tibétains

Les chercheurs d'ESET découvrent une opération stratégique de compromission du web et des attaques de la chaîne d'approvisionnement ciblant les Tibétains

Rescoms surfe sur les vagues de spam d'AceCryptor

Aperçu des statistiques de télémétrie d'ESET sur AceCryptor au second semestre 2023 et plus particulièrement sur les campagnes de Rescoms menées dans les pays européens

Campagne eXotic Visit : sur la trace des envahisseurs virtuels

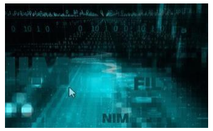
Les chercheurs d'ESET ont découvert la campagne d'espionnage eXotic Visit qui cible principalement les utilisateurs indiens et pakistanais au moyen d'applications en apparence inoffensives

Ebury est actif, mais reste invisible : 400 000 serveurs Linux compromis pour des vols de cryptomonnaies et l'appât du gain

L'une des campagnes de logiciels malveillants orientés serveur les plus avancées est encore en pleine expansion, avec des centaines de milliers de serveurs compromis, et se diversifiant par des vols de cartes de crédit et de cryptomonnaies

Écoute aux portes (dérobées) : Lunar s'infiltre dans les missions diplomatiques

Les chercheurs d'ESET fournissent une analyse technique de la boîte à outils Lunar qui a probablement été utilisée par le groupe APT Turla et qui a permis d'infiltrer un ministère européen des affaires étrangères



Découvrez Nimfilt : un outil de rétro-ingénierie pour les binaires compilés en Nim

Disponible sous forme de plugin IDA et de script Python, Nimfilt facilite la rétro-ingénierie des binaires compilés avec le compilateur du langage de programmation Nim en décomposant les noms de paquets et de fonctions, et en appliquant des structures aux chaînes de caractères

Rapport d'activité ESET sur les groupes APT, une analyse du quatrième trimestre 2023 au premier trimestre 2024

Un aperçu des activités d'une sélection de groupes APT, étudiés et analysés par ESET Research au quatrième trimestre 2023 et au premier trimestre 2024

Crédits

Équipe

Peter Stančík, chef d'équipe

Hana Matušková, rédactrice en chef

Aryeh Goretsky

Branislav Ondrášik

Bruce P. Burrell

Klára Kobáková

Nick FitzGerald

Ondrej Kubovič

Rene Holt

Zuzana Pardubská

Contributeurs

Alexandre Côté-Cyr

Dušan Lacika

Igor Kabina

Jakub Souček

Jan Holman

Ján Adámek

Ján Šugarek

Jiří Kropáč

Ladislav Janko

Lukáš Štefanko

Marc-Étienne Léveillé

Martin Červeň

Mathieu Tartare

Vladimír Šimčák

Yevhenii Fomiachenko

À propos des données de ce rapport

Les statistiques et les tendances relatives aux menaces présentées dans ce rapport sont basées sur les données télémétriques mondiales d'ESET. Sauf mention contraire explicite, les données incluent les détections quelle que soit la plateforme ciblée.

De plus, les données excluent les détections d'applications potentiellement indésirables, d'applications potentiellement dangereuses et de logiciels publicitaires, sauf indication contraire dans les sections plus détaillées et propres à chaque plateforme, ainsi que dans la section Menaces liées aux cryptomonnaies.

Ces données ont été traitées avec l'intention sincère d'atténuer l'ensemble des biais connus, dans le but de valoriser au maximum les informations fournies.

La plupart des graphiques de ce rapport montrent des tendances en matière de détection plutôt que des chiffres absolus. En effet, les données peuvent être sujettes à diverses interprétations erronées, en particulier lorsqu'elles sont directement comparées à d'autres données télémétriques. Toutefois, des valeurs absolues ou des ordres de grandeur sont fournis lorsqu'ils sont jugés utiles.

À propos d'ESET

ESET® fournit une sécurité numérique de pointe pour prévenir les attaques avant qu'elles ne se produisent. En combinant la puissance de l'IA et l'expertise humaine, ESET garde une longueur d'avance sur les cybermenaces connues et émergentes : elle sécurise ainsi les entreprises, les infrastructures critiques et les individus. Que ce soit pour la protection des terminaux, du nuage ou des mobiles, nos solutions et services basés sur l'IA et axés sur le nuage restent très performantes et faciles à utiliser. La technologie ESET inclut une détection et une réponse efficaces, un chiffrement ultra-sécurisé et une authentification multifacteurs. Grâce à une défense en temps réel 24 heures sur 24, 7 jours sur 7, et à une assistance locale fiable, nous assurons la sécurité des utilisateurs et le bon fonctionnement des entreprises sans interruption. Un paysage numérique en constante évolution exige une approche évolutive de la sécurité : ESET s'engage à mener des recherches de niveau international et à fournir des informations fiables sur les menaces, en s'appuyant sur des centres de R&D et un solide réseau mondial de partenaires. Pour plus d'informations, consultez **www.eset.com** ou suivez-nous sur **LinkedIn**, **Facebook** et **X**.

WeLiveSecurity.com

@ESETresearch GitHub

ESET

Rapports sur les menaces et rapports d'activité sur les groupes APT d'ESET

Digital Security
Progress. Protected.

(eset):research