Digital Security
Progress. Protected.

Rapport sur les menaces

S1 2025

Décembre 2024 – Mai 2025

(eset):research

Table des matières

Synthèse

Vecteurs d'attaques | Ingénierie sociale

ClickFix : fausses erreurs, vraies menaces

Une nouvelle technique d'ingénierie sociale appelée ClickFix s'impose dans le paysage des menaces comme second vecteur d'attaques le plus répandu après l'hameçonnage.

Infostealers | Malwares As a Service

Double peine pour de célèbres infostealers

ESET a participé à des opérations de déstabilisation de deux infostealers notables : Lumma Stealer et Danabot.

Infostealers | Malwares As a Service

SnakeStealer se glisse vers le sommet

Après l'abandon du malware Agent Tesla par ses créateurs, SnakeStealer redevient l'infostealer le plus détecté dans les données télémétriques d'ESET.

Android | Adwares

Kaléidoscope et son jumeau inondent Android de publicités

Les détections d'adwares sur Android ont augmenté de 160 %, en raison de l'apparition d'une nouvelle escroquerie et de l'essor d'applications potentiellement indésirables.

Android | NFC | Escroqueries

L'évolution de la fraude à la technologie NFC : NGate, GhostTap et escroqueries par relais

La fraude à la technologie NFC a été multipliée par plus de trente-cinq, alimentée par des campagnes d'hameçonnage et des techniques de relais inventives.

Ransomwares

Guerre des gangs : quand les ransomwares s'entre-déchirent

Tandis que le nombre de gangs et d'attaques de ransomwares augmente, les groupes de ransomwares s'affrontent de plus en plus, ce qui touche plusieurs acteurs, y compris RansomHub, le principal Ransomware As a Service.

Avant-propos

Bienvenue dans l'édition du S1 2025 du Rapport général sur les menaces !

Le paysage des menaces au cours du premier semestre 2025 était loin d'être ennuyeux : nouvelles techniques d'ingénierie sociale, menaces mobiles sophistiquées, perturbations causées par des infostealers, et plus encore.

L'un des développements les plus frappants de cette période a été l'émergence de ClickFix, un nouveau vecteur d'attaques trompeur qui a explosé de plus de 500 % dans la télémétrie ESET par rapport à S2 2024. Devenu le second vecteur d'attaques le plus courant après l'hameçonnage, ClickFix manipule les internautes pour qu'ils exécutent des commandes malveillantes sous prétexte de corriger une fausse erreur. Les malwares installés à la fin des attaques ClickFix varient considérablement, pouvant comprendre des infostealers, des ransomwares et même des malwares développés par des États, ce qui en fait une menace polyvalente et redoutable sur Windows, Linux et macOS.

Le paysage des infostealers a également connu d'importants changements. Agent Tesla étant maintenant obsolète, SnakeStealer (également connu sous le nom de Snake Keylogger) a pris sa place pour devenir l'infostealer le plus détecté dans notre télémétrie. ESET a également contribué à d'importantes opérations de perturbation de Lumma Stealer et Danabot, deux malwares prolifiques disponibles en tant que services.

En ce qui concerne Android, les détections d'adwares ont augmenté de 160 %, en grande partie à cause d'une nouvelle menace sophistiquée baptisée Kaleidoscope. Ce malware utilise une stratégie trompeuse dite de « jumeau maléfique » pour diffuser des applications malveillantes qui bombardent les utilisateurs de publicités intrusives et dégradent les performances de leur appareil. En parallèle, la fraude à la technologie NFC a été multipliée par plus de trente-cinq, alimentée par des campagnes d'hameçonnage et des techniques de relais inventives. Même si les chiffres globaux restent encore modestes, ce bond met en évidence l'évolution rapide des méthodes des criminels et l'attention constante qu'ils portent à l'exploitation de la technologie NFC. Chaque nouvelle itération des menaces par NFC, qu'il s'agisse de NGate ou de GhostTap, et plus récemment de SuperCard, démontre que les attaquants s'adaptent aux nouvelles mesures de sécurité.

La scène des ransomwares est devenue (encore plus) chaotique, avec des luttes entre bandes rivales de ransomwares qui ont touché plusieurs acteurs, y compris RansomHub, le principal Ransomware As a Service. Les données annuelles montrent que si les attaques de ransomwares et le nombre de gangs actifs ont augmenté, les paiements de rançons ont connu une baisse significative.

Cette contradiction peut être le résultat des démantèlements et des escroqueries de sortie qui ont remanié la scène des ransomwares en 2024, et elle est également due en partie à une diminution de la confiance dans la capacité des gangs à respecter leur part du marché.

Je vous souhaite une bonne lecture.

Jiří Kropáč
Director of Threat Prevention Labs chez ESET

Tendances du paysage des menaces

Vecteurs d'attaques | Ingénierie sociale

ClickFix : fausses erreurs, vraies menaces

Une nouvelle technique d'ingénierie sociale appelée ClickFix s'impose dans le paysage des menaces comme second vecteur d'attaques le plus répandu après l'hameçonnage.

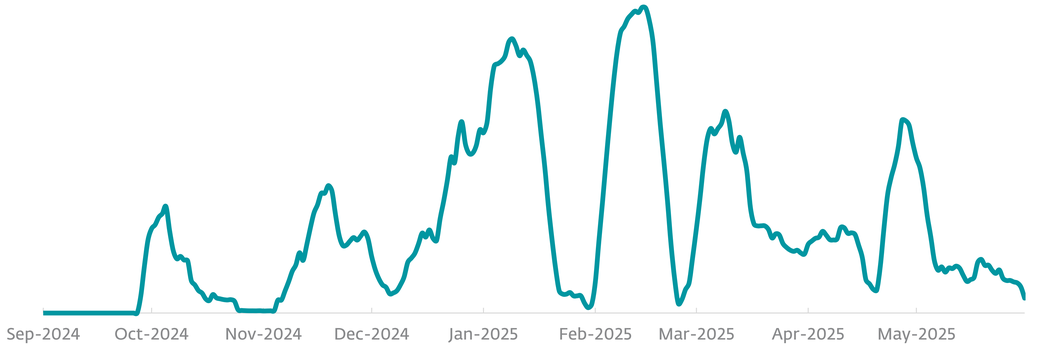
Prouver que l'on est un être humain en ligne peut revêtir de nombreuses formes. Il est parfois nécessaire de retranscrire un texte flou dans un champ vide, tandis qu'à d'autres occasions, il vous est demandé de sélectionner toutes les images de bus, de feux de circulation ou d'escaliers. Dans d'autres cas, un site web peut vous demander de faire glisser une pièce de puzzle à son emplacement correct dans une image. À mesure que la variété des contrôles reCAPTCHA s'est accrue, les utilisateurs se sont habitués au processus, et peu d'entre eux remettraient en question un nouveau type de défi, tel que copier-coller un élément sur leur appareil. C'est précisément ce qu'ont imaginé les cybercriminels en transformant l'une des fonctions les plus frustrantes du web en un nouveau vecteur d'intrusion.

ClickFix est un nouveau type d'ingénierie sociale qui utilise un faux message d'erreur ou de vérification pour manipuler les victimes afin qu'elles copient et collent un script malveillant puis l'exécutent. La liste des menaces auxquelles renvoie ClickFix s'allonge de jour en jour et comprend actuellement des infostealers, des ransomwares, des chevaux de Troie d'accès à distance, des extracteurs de cryptomonnaie, des outils de post-exploitation et même des malwares personnalisés développés par des groupes APT sponsorisés par des États.

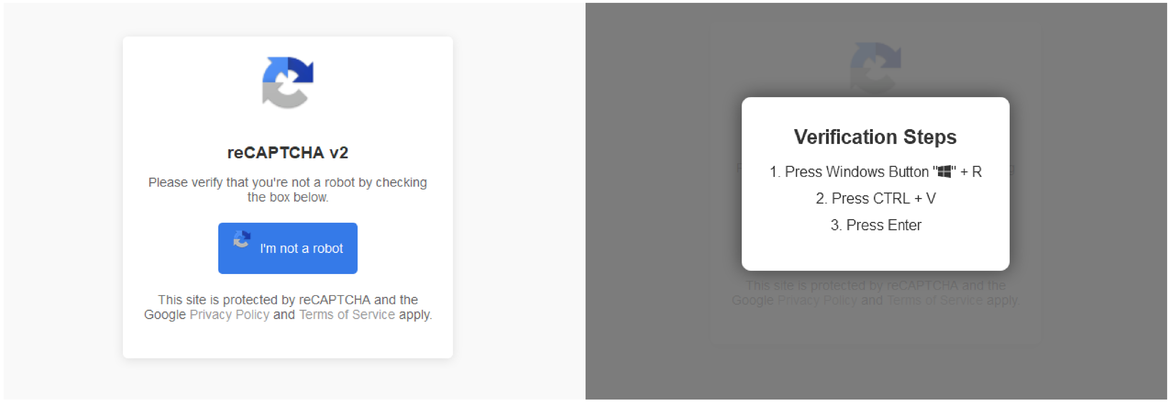
Alors que la détection par ESET de HTML/FakeCaptcha pour ClickFix était pratiquement inexistante il y a un an, elle a augmenté de 517 % entre S2 2024 et S1 2025. Cela en fait l'une des menaces qui se développent le plus rapidement. Elle représente près de 8 % de toutes les attaques bloquées, se hissant au deuxième rang **de notre Top 10**.

Il est important de noter que les multiples étapes de l'attaque, y compris les commandes ou les scripts PowerShell copiés, les exécutables, les « enveloppes » malveillantes et les malwares embarqués, sont couvertes par des dizaines d'autres noms de détection. Par conséquent, la prévalence réelle de cette menace est probablement encore plus élevée que les chiffres relatifs à HTML/FakeCaptcha. Les pays qui signalent le plus grand nombre de détections dans la télémétrie ESET sont le Japon (23 %), le Pérou (6 %), la Pologne, l'Espagne et la Slovaquie (plus de 5 % chacun).

ClickFix est apparu en mars 2024, dans le cadre d'une campagne des groupes ClearFake et TA571 **documentée** par Proofpoint. Cette campagne utilisait des emails d'hameçonnage contenant des pièces jointes HTML malveillantes qui affichaient une page imitant Microsoft Word ou OneDrive. Une fenêtre contextuelle affichée sur ces pages prétend faussement qu'une erreur doit être



Tendance de la détection de HTML/FakeCaptcha pour S2 2024 et S1 2025, moyenne mobile sur sept jours



Faux contrôle reCAPTCHA demandant à la victime de copier-coller et d'exécuter une commande malveillante sur son appareil

résolue avant de pouvoir accéder au contenu. La victime est ensuite invitée à cliquer sur un bouton « corriger », copier une commande PowerShell dans son presse-papiers, ouvrir un terminal PowerShell et y coller la commande pour l'exécuter. Au lieu de résoudre l'erreur inventée, cela déclenche une chaîne de téléchargement et d'exécution d'autres scripts malveillants qui aboutissent finalement à une compromission par le malware DarkGate ou Matanbuchus proposé en tant que service sur le dark web.

À la fin de l'année 2024, des attaques utilisant la même technique d'ingénierie sociale ont inondé le web. Des acteurs de menaces ont créé de faux sites web imitant des services populaires tels que Booking.com ou Google Meet, ont compromis des sites web légitimes avec de fausses demandes de mise à jour du navigateur, de fausses vérifications Cloudflare ou reCAPTCHA, ou ont distribué des liens menant à des pages ClickFix via des campagnes d'emailing. Comme l'indique un récent **Rapport sur les activités des APT**, le groupe DeceptiveDevelopment sponsorisé par la Corée du Nord a également utilisé cette tactique d'ingénierie sociale, en créant de faux problèmes dans des dépôts GitHub populaires, puis en proposant un « correctif » qui livrait le malware WeaselStore du groupe.

Encouragés par l'efficacité de l'approche de ClickFix, des acteurs de menaces **auraient** maintenant commencé à vendre des outils fournissant des pages d'atterrissage équipées de ClickFix à d'autres attaquants.

Le nombre de variantes de ClickFix a augmenté, tout comme le nombre de menaces diffusées à l'aide de cette technique. La liste comprend actuellement des infostealers populaires tels que **Lumma Stealer**, VidarStealer, StealC et **Danabot**, des chevaux de Troie d'accès à distance tels que VenomRAT, AsyncRAT et NetSupport RAT, des outils de gestion et de surveillance à distance tels que MeshAgent, des frameworks de post-exploitation tels que Havoc et Cobalt Strike, des extracteurs de cryptomonnaies, des chargeurs, des détourneurs de presse-papiers et bien d'autres encore. Au début de l'année 2025, des attaques tentaient de déployer le ransomware Interlock (anciennement Rhysida).

Des acteurs de menaces sponsorisés par des États ont également rapidement pris le train en marche, incorporant cette technique d'ingénierie sociale dans leurs boîtes à outils d'obtention d'un accès initial. Kimsuky, Lazarus et DeceptiveDevelopment, alignés sur la Corée du Nord, ont été les premiers à cibler les utilisateurs de Windows, Linux et macOS. D'autres groupes ont rapidement suivi, notamment Callisto et Sednit, alignés sur la Russie, MuddyWater, aligné sur l'Iran, et APT36, aligné sur le Pakistan.

Si les utilisateurs de Windows sont les plus touchés, les utilisateurs de macOS et de Linux sont également dans le collimateur. Sur macOS, des signalements publics révèlent que les campagnes de ClickFix diffusaient le voleur AMOS. Pour Linux, APT36 redirigeait les victimes vers une page CAPTCHA contrefaite qui leur demandait d'exécuter du code malveillant via Alt+F2. Sur la plupart des distributions Linux, ce raccourci clavier ouvre une boîte de dialogue d'exécution de commande. Toutefois, dans ce cas précis, la compromission récupérait un fichier JPEG caché sur le serveur de l'attaquant puis l'ouvrait en arrière-plan sans causer de dommages ou entreprendre d'autres actions malveillantes.

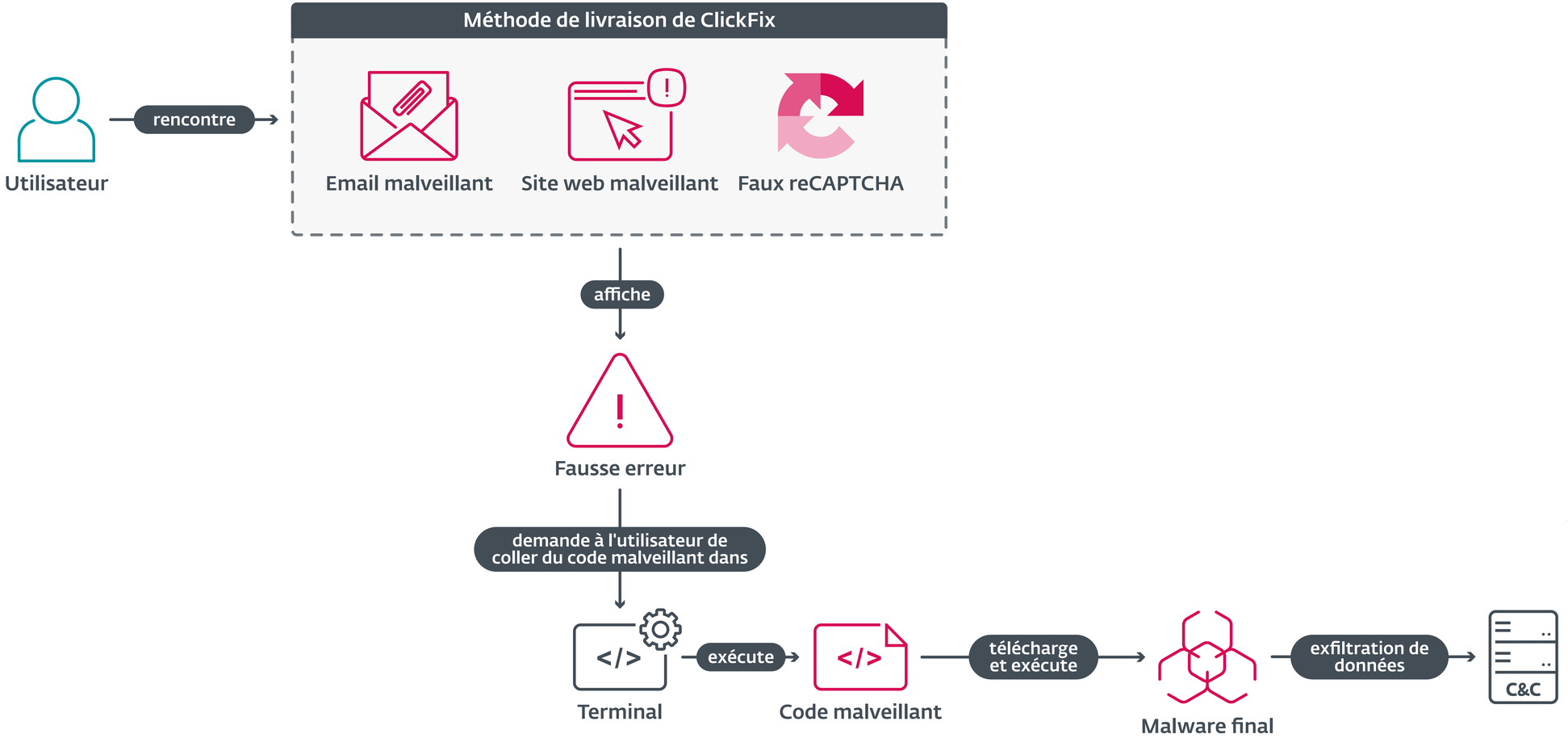
Comme indiqué précédemment, les attaques ClickFix peuvent être interceptées par des solutions de sécurité à plusieurs stades. Il s'agit notamment des URL des sites web malveillants et compromis, des pièces jointes des emails en HTML, des fichiers HTA, des fichiers JavaScript, des scripts PowerShell et des programmes de ligne de commande utilisés pour installer des malwares. Des solutions de sécurité fiables devraient également bloquer les « enveloppes » utilisées par les attaquants pour obscurcir ou masquer les malwares embarqués (détectées par ESET comme Win/Kryptik ou Win/GenKryptik), reconnaître les activités malveillantes dans la mémoire et identifier les comportements suspects sur le réseau, telles que l'exfiltration de données.

Les utilisateurs devraient également rester vigilants lorsqu'on leur propose des solutions « en un clic » ou « par copier-coller » à des problèmes inconnus. Dans les environnements d'entreprise, les outils de détection et de réponse sur endpoints (EDR) peuvent signaler une utilisation anormale de PowerShell, en particulier sur des machines qui en ont rarement besoin, et ainsi améliorer la visibilité et la protection contre de telles attaques.

ÉCLAIRAGE DE NOTRE EXPERT

Les données télémétriques d'ESET montrent que ClickFix est rapidement devenu l'un des principaux vecteurs d'intrusions des cybercriminels. Cette nouvelle technique d'ingénierie sociale est efficace parce qu'elle est suffisamment simple pour que la victime suive les instructions, suffisamment crédible pour donner l'impression qu'elle pourrait résoudre un problème inventé, et qu'elle joue sur le fait que les victimes ne prêtent pas beaucoup attention aux commandes exactes qu'on leur a demandé de coller et d'exécuter sur leur appareil. C'est également un bon exemple qui illustre l'adoption rapide par les acteurs de menaces de nouvelles techniques, une fois qu'elles ont fait leurs preuves. Compte tenu de sa popularité croissante, il est possible que Microsoft et Apple, mais également la communauté open source, ajoutent une sorte d'avertissement de sécurité, comme pour les macros dans Word ou Excel, ou pour les fichiers téléchargés depuis Internet, notifiant les utilisateurs qu'ils sont sur le point d'exécuter un script potentiellement dangereux.

Dušan Lacika, Senior Detection Engineer chez ESET



Flux d'attaque simplifié de ClickFix

Infostealers Malwares As a Service

Double peine pour de célèbres infostealers

ESET a participé à des opérations de déstabilisation de deux infostealers notables : Lumma Stealer et Danabot.

Le monde est rempli de nouvelles sombres et inquiétantes ces derniers temps. Que diriez-vous de quelque chose de positif pour changer ? Des mois de travail acharné de la part des forces de police et d'entreprises de cybersécurité comme ESET, ont porté leurs fruits et ont permis aux autorités de sérieusement freiner les activités de non pas un, mais de deux importants infostealers. Lumma Stealer, un malware disponible en location (MaaS), et Danabot, un autre MaaS considérablement malveillant, ont vu leurs infrastructures en grande partie démantelées en mai 2025.

Nous vous présentons ici une vue d'ensemble de ces deux opérations, ainsi que les données récentes issues de la télémétrie d'ESET concernant ces deux infostealers. Nos recherches approfondies et nos rapports sur ces événements récents sont disponibles dans les articles **Lumma Stealer** et **Danabot** sur WeLiveSecurity.

Lumma Stealer ne vole plus ?

Tout juste six mois après la publication de l'article couvrant la croissance sans précédent de Lumma Stealer dans le **Rapport sur les menaces** du S2 2024, le moment est venu de faire le bilan de ce Malware As a Sservice. En mai 2025, ESET, aux côtés de Microsoft, BitSight, Lumen, Cloudflare, CleanDNS et GMO Registry, a pris part à un effort mondial coordonné visant à déstabiliser Lumma Stealer. L'opération a ciblé tous les serveurs de C&C (commande et contrôle) connus de Lumma Stealer au cours de l'année écoulée pour éliminer une grande partie du réseau d'exfiltration du malware. Dans le cadre de l'opération, ESET a fourni des analyses techniques et des informations statistiques. Grâce à nos systèmes automatisés, nous avons également extrait des données essentielles des dizaines de milliers d'échantillons de malwares, notamment les serveurs de C&C et les identifiants d'affiliés.

Tendance de détection de Lumma Stealer au S1 2025, moyenne mobile sur sept jours

ÉCLAIRAGE DE NOTRE EXPERT

Nous pouvons sans aucun doute qualifier de succès le démantèlement de Lumma Stealer. Le malware a subi un revers technique considérable qui l'a mis hors service pendant un certain temps après l'opération. Même si nous constatons aujourd'hui que ses auteurs ont commencé à reconstruire son infrastructure en utilisant des serveurs DNS situés en Russie, la réputation de cette entreprise cybercriminelle a incontestablement été endommagée. Le succès continu de Lumma Stealer repose en grande partie sur la confiance de ses affiliés. Cela signifie que même si Lumma Stealer réussit à se reconstruire, sa base d'utilisateurs risque de l'abandonner au profit d'un autre infostealer, auquel cas la solution la plus probable pour ses opérateurs serait de remanier complètement l'image de leur service.

Jakub Tomanek, Malware Analyst chez ESET

Si l'on examine nos données télémétriques, avant l'opération, l'activité de Lumma Stealer au S1 2025 était encore plus élevée qu'au S2 2024. Nous avons enregistré une augmentation de 21 % des détections du malware. Au cours de cette période, un pic considérable a été enregistré le 11 avril à la suite d'une campagne d'emails non sollicités ciblant principalement le Mexique, où plus de 40 % des tentatives d'attaque de Lumma Stealer ont eu lieu ce jour-là. Bien que l'opération ait eu lieu très peu de temps avant la fin de la période du reporting, nous avions déjà pu constater une baisse des détections de Lumma Stealer.

Nos recherches approfondies ont révélé l'ampleur de l'activité des auteurs de la menace en coulisses : entre le 17 juin 2024 et le 1er mai 2025, nous avons observé 3 353 nouveaux domaines de C&C uniques, soit environ 74 nouveaux domaines par semaine. Nous avons également constaté que des mises à jour régulières du code ont été effectuées au cours de cette période. Cela montre que Lumma Stealer est une menace extrêmement prolifique, et qu'il est d'autant plus important de le mettre hors d'état de nuire.

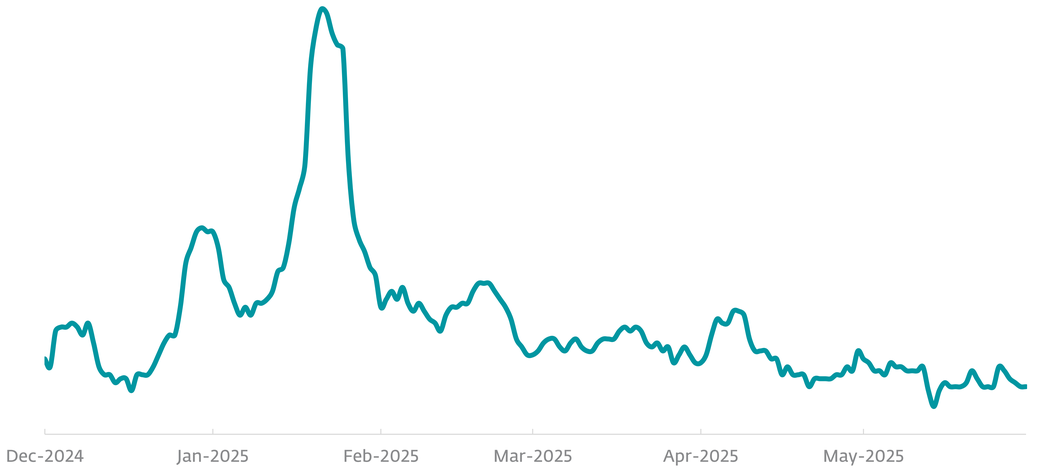
La télémétrie d'ESET indique également que Lumma Stealer est le principal malware embarqué du cheval de Troie HTML/FakeCaptcha, utilisé dans les attaques d'ingénierie sociale de ClickFix décrites dans **la section précédente de ce rapport**. Même si cette méthode a été principalement utilisée pour diffuser Lumma Stealer dans le passé, son utilisation s'est déjà étendue à d'autres menaces. Par conséquent, cette opération de démantèlement n'aura probablement qu'un effet temporaire sur FakeCaptcha et d'autres variétés d'attaques ClickFix.

Danabot à genoux

Quelques jours seulement après le démantèlement de Lumma Stealer, le célèbre infostealer Danabot a lui aussi eu sa part du gâteau, **ciblé** par le FBI et le Defense Criminal Investigative Service (DCIS) du ministère de la défense des États-Unis, dans le cadre d'**Operation Endgame** coordonnée par **Europol et Eurojust**.

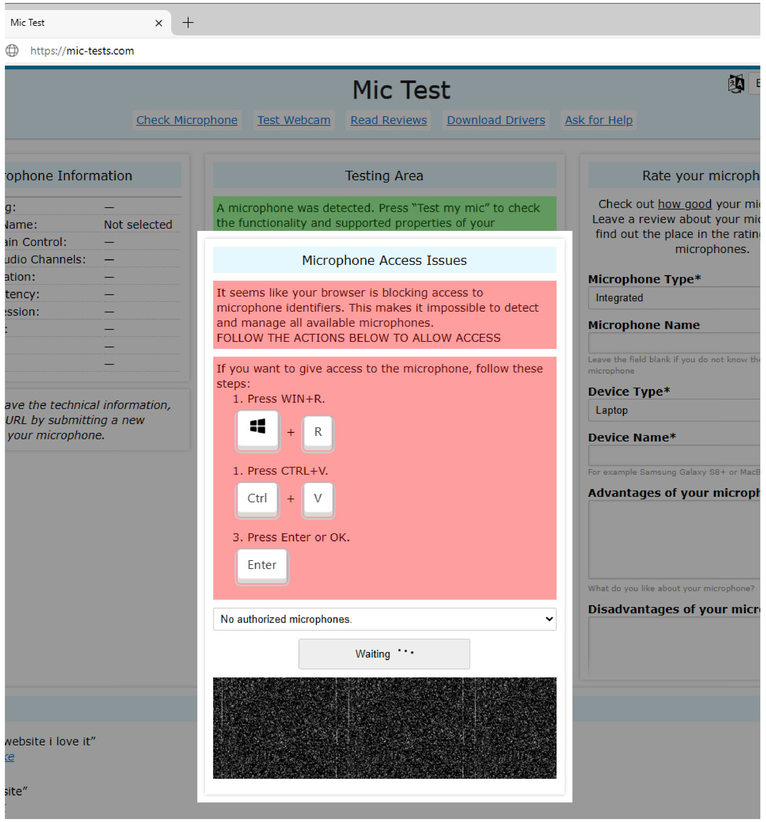
ESET a participé à cette opération aux côtés d'Amazon, CrowdStrike, Flashpoint, Google, Intel471, PayPal, Proofpoint, Team Cymru, Zscaler et de plusieurs agences de forces de police dans le monde entier. Elle est l'aboutissement d'un effort de plusieurs années de la part des parties concernées. La participation d'ESET a commencé dès 2018. Notre contribution a consisté à fournir des analyses techniques de l'infostealer et de son infrastructure de back-end, ainsi qu'à identifier ses serveurs de C&C. Cette opération coordonnée a permis de mettre hors service une grande partie de l'infrastructure de Danabot, ce qui a eu un impact considérable sur le malware.

Danabot est un infostealer programmé en Delphi, qui est proposé en tant que service sur des forums clandestins, comme Lumma Stealer. Il est disponible en location, ce qui met toute une série d'outils entre les mains d'affiliés qui peuvent alors créer et gérer leurs propres botnets.



Tendance de détection de Danabot au S1 2025, moyenne mobile sur sept jours

Des cybercriminels ont utilisé Danabot de plusieurs façons : outre ses fonctionnalités typiques d'exfiltration de données telles que l'enregistrement des frappes au clavier, des captures d'écran et le vol de fichiers, il est également utilisé pour installer d'autres malwares sur les systèmes compromis, notamment des ransomwares. Nous avons par exemple découvert qu'il pouvait aussi installer LockBit, Buran et Crisis. Les machines compromises par l'infostealer ont également été utilisées pour lancer des attaques DDoS.



Site web incitant des victimes à exécuter du code malveillant copié dans le presse-papiers

Le malware lui-même est diffusé par différents moyens. En plus de pièces jointes d'emails d'hameçonnage, il est également transmis par d'autres malwares, ainsi que par des liens sponsorisés malveillants dans les résultats de recherche de Google. Dernièrement, ce malware a été distribué par la méthode **ClickFix** : la victime potentielle se voit présenter un faux problème technique, dont la « solution » consiste à exécuter une commande dans une fenêtre de terminal qui contient un code PowerShell malveillant téléchargeant finalement Danabot.

Selon les données télémétriques d'ESET, Danabot n'est pas aussi répandu que Lumma Stealer, mais il reste un MaaS d'une ampleur considérable. Au fil des années de traque de cet infostealer, ESET a analysé un grand nombre d'échantillons distincts et a identifié plus de 1 000 serveurs de C&C uniques. Avant son démantèlement, l'activité du malware avait augmenté de plus de 50 % au S1 2025. Les pays les plus touchés par les tentatives d'attaques de Danabot au cours de cette période étaient les États-Unis (44 %) et la Pologne (29 %). Heureusement, comme le montrent les données de tendance de la page précédente, les détections de Danabot ont commencé à diminuer à la suite de l'opération de démantèlement.

Infostealers Malwares As a Service

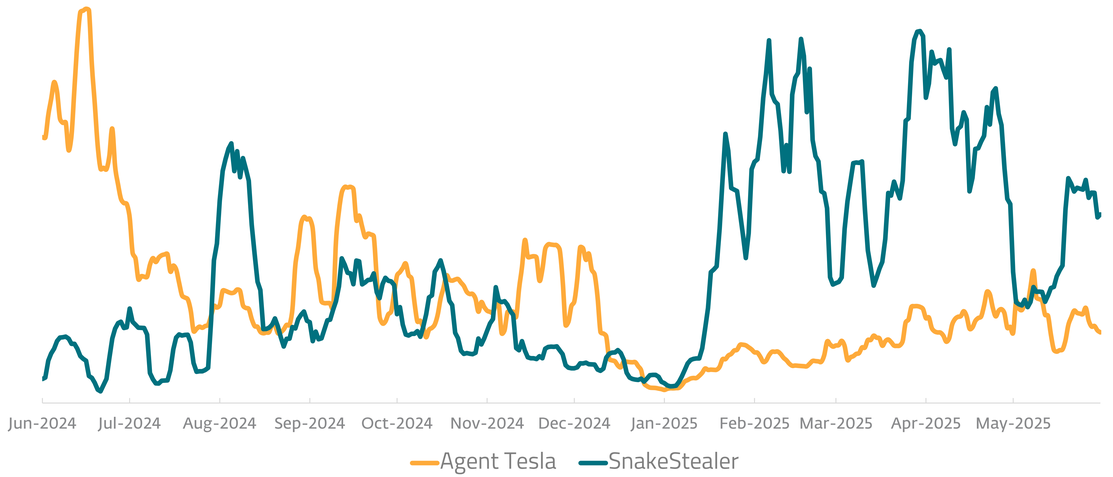
SnakeStealer se glisse vers le sommet

Après l'abandon du malware par les créateurs d'Agent Tesla, SnakeStealer redeviens l'infostealer le plus détecté dans les données télémétriques d'ESET.

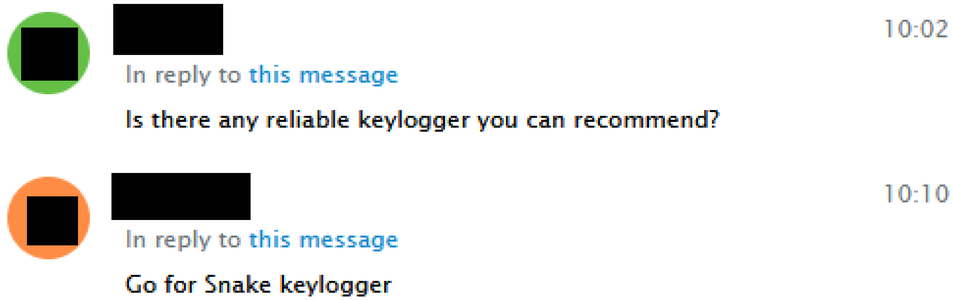
Après plusieurs années de domination dans la catégorie des infostealers dans les statistiques d'ESET, il semble que l'ère d'Agent Tesla soit révolue. Il était déjà tombé en deuxième position au S2 2024, lorsqu'il a été dépassé par Win/Formbook et sa trajectoire descendante s'est poursuivie depuis. Maintenant en quatrième position, les détections d'Agent Tesla au S1 2025 ont diminué de 57 % par rapport à la période précédente. D'après les déclarations des auteurs de ce célèbre Malware As a Service (MaaS), la raison du déclin est assez prosaïque : les opérateurs ont perdu l'accès aux serveurs contenant son code source et ont donc décidé d'arrêter son développement pour une durée indéterminée. C'est pourquoi la baisse du nombre de détections a été progressive plutôt que spectaculaire. Le malware n'a pas complètement disparu, mais de nouvelles versions ne sont tout simplement pas développées.

Pendant qu'il s'éteint lentement, Agent Tesla a déjà été remplacé par une nouvelle étoile montante : un autre MaaS nommé SnakeStealer que nous avons repéré principalement sous le nom MSIL/Spy.Agent.AES. Il est désormais l'infostealer numéro un selon les données télémétriques d'ESET. Le canal Telegram d'Agent Tesla recommande même SnakeStealer comme remplacement adéquat. Il semble que les recommandations aient joué un rôle clé dans le succès du malware, car la première vague de détections de SnakeStealer à partir de la fin du mois de juillet 2024 coïncide à peu près avec le moment où le développement d'Agent Tesla a été interrompu.

SnakeStealer, également connu sous le nom de Snake Keylogger ou 404 Keylogger, est un malware .NET qui est apparu pour la première fois en 2019. Vendu via un groupe Telegram, cet infostealer est capable d'enregistrer les frappes au clavier, voler des identifiants enregistrées, effectuer des captures d'écran et collecter les données du presse-papiers. Ces éléments sont ensuite exfiltrés via FTP, SMTP ou des bots Telegram. Le malware est principalement diffusé sous forme de pièces jointes malveillantes dans des



Tendances de détection de SnakeStealer et d'Agent Tesla au S2 2024 et S1 2025, moyenne mobile sur sept jours



Des membres du canal Telegram d'Agent Tesla recommandaient SnakeStealer

ÉCLAIRAGE DE NOTRE EXPERT

S'il est certainement possible que SnakeStealer remplace Agent Tesla en tant qu'infostealer dominant, nous devons garder à l'esprit que la concurrence est féroce et qu'il existe plusieurs autres infostealers prédominants sur le marché. C'est le cas de Pure Logs qui a également gagné en importance depuis qu'Agent Tesla a cessé d'être mis à jour. D'un autre côté, nous ne pouvons pas ignorer l'utilité du bouche à oreille, puisque nous avons remarqué que de nombreuses personnes sur le dark web recommandaient SnakeStealer comme alternative d'Agent Tesla. Cependant, il n'y a pas grand-chose d'autre en soi qui distingue SnakeStealer de ses concurrents.

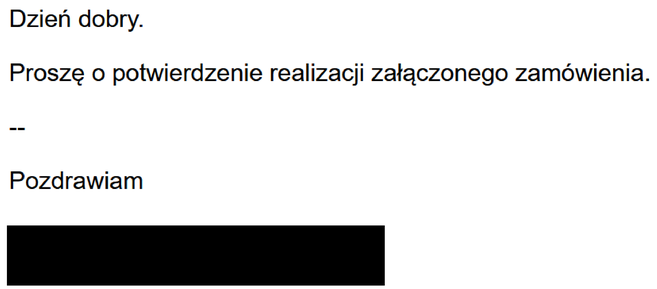
Jakub Kaloč, Malware Analyst chez ESET

emails d'hameçonnage. Les opérateurs de SnakeStealer proposent également une version VIP qui contient des fonctionnalités supplémentaires moyennant un prix plus élevé. Comme ces deux versions sont assez similaires d'un point de vue technique, notre détection de MSIL/Spy.Agent.AES les couvre toutes deux.

En examinant les données télémétriques d'ESET, nous constatons que SnakeStealer représentait près d'un cinquième de toutes les détections d'infostealers que nous avons enregistrées au S1 2025. Après une période d'accalmie pendant les fêtes de fin d'année, les détections de ce malware ont régulièrement augmenté à partir de mi-janvier. Leur nombre a plus que doublé entre S2 2024 et S1 2025. Le taux d'activité le plus élevé de SnakeStealer a été observé au printemps, après le lancement de trois campagnes successives d'envoi d'emails, avec des pics de détection rapprochés le 25 mars, le 3 avril et le 9 avril. À chacune de ces dates, le malware a été détecté plus de 6 000 fois par jour. Les pays qui ont connu le plus grand nombre de tentatives d'attaques par SnakeStealer sont la Turquie (15 %), le Japon (13 %) et l'Espagne (11 %).

Nos recherches ont également permis de repérer plusieurs campagnes de SnakeStealer visant l'Europe centrale et l'Europe de l'Est. Parmi les pays surveillés, la Pologne et la Lettonie ont enregistré le plus grand nombre de tentatives d'attaques : en ne tenant compte que des plus intensives, c'est-à-dire les tentatives ciblées ou nécessitant des mesures considérables pour paraître crédibles, nous en avons recensé près de 5 000 en Lettonie et plus de 18 000 en Pologne entre janvier et avril 2025.

Dans ces campagnes, SnakeStealer était généralement fourni avec Cassandra Protector ou Pure Crypter, que nous détectons sous les noms MSIL/Kryptik et MSIL/TrojanDownloader.Agent. Un exemple typique est la réception par la victime d'un email contenant un fichier ISO en pièce jointe, dans lequel se trouve un exécutable Pure Crypter qui télécharge puis déchiffre et lance SnakeStealer.


Dzień dobry.

Proszę o potwierdzenie realizacji załączonego zamówienia.

--

Pozdrawiam

[redacted]

Un des emails d'hameçonnage avec une pièce jointe installant SnakeStealer (traduction machine : Bonne journée. Veuillez confirmer la commande ci-jointe. Meilleures salutations)

Android Adwares

Kaléidoscope et son jumeau inondent Android de publicités

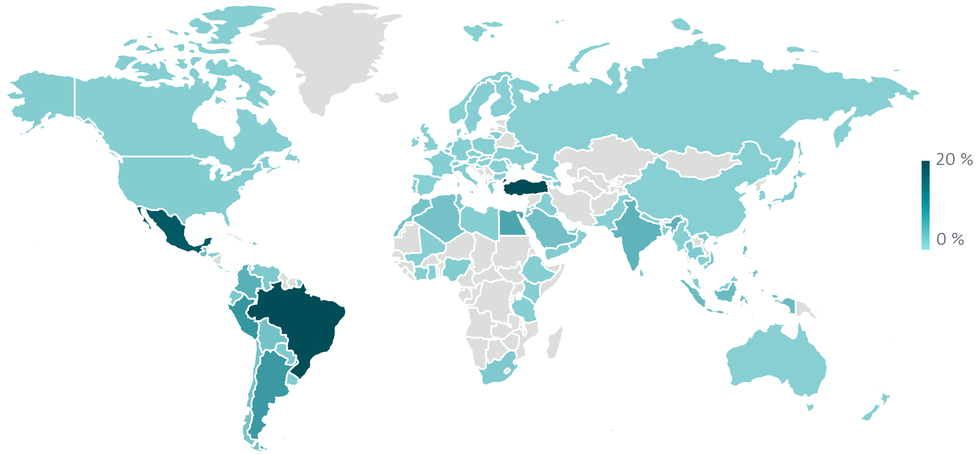
Les détections d'adwares sur Android ont augmenté de 160 %, en raison de l'apparition d'une nouvelle escroquerie et de l'essor d'applications potentiellement indésirables.

Une nouvelle menace Android sophistiquée, baptisée Kaleidoscope, inonde les appareils de publicités intrusives via une application jumelle trompeuse. Bien que son nom semble inoffensif, Kaléidoscope est en fait un stratagème conçu pour tromper les annonceurs et les app stores.

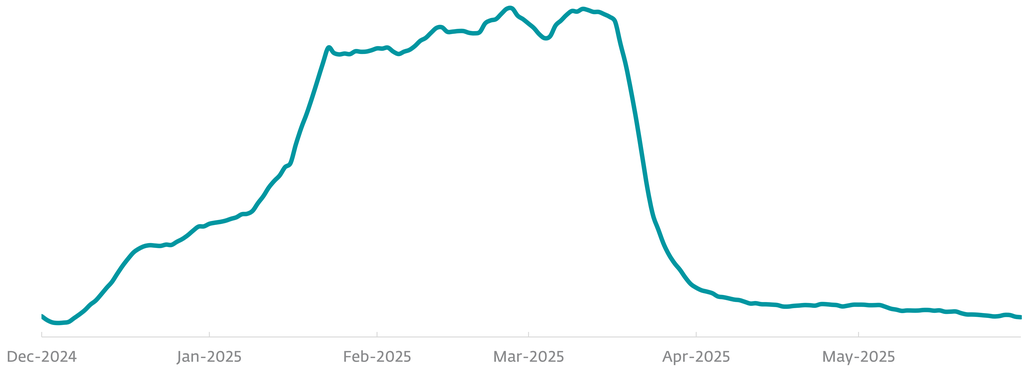
Kaleidoscope est une opération de fraude publicitaire sur Android découverte par **IAS Threat Lab**. Les cybercriminels à son origine créent deux versions quasiment identiques de la même application : une version inoffensive (leurre) est destinée aux app stores officiels et une version malveillante (jumeau maléfique) est distribuée par des app stores tiers. Ce jumeau maléfique génère des publicités intrusives et indésirables afin de gagner frauduleusement des revenus publicitaires.

ESET détecte cette menace en tant que variante .MPP de Android/TrojanDropper.Agent. Elle représente 28 % des détections dans l'ensemble de la catégorie des adwares Android. Kaleidoscope touche chaque mois un grand nombre d'utilisateurs d'Android dans le monde entier : selon les données télémétriques d'ESET, la plupart des victimes se trouvent en Amérique latine, en Turquie, en Égypte et en Inde, où les app stores tiers sont populaires. Les utilisateurs de ces régions installent involontairement des jumeaux malveillants, ce qui entraîne l'affichage de publicités intrusives et une dégradation des performances de leur appareil.

La méthode du jumeau maléfique utilisée par Kaléidoscope est une tactique astucieuse qui suit les étapes décrites dans les quatre sections suivantes.



Répartition géographique de Kaléidoscope au S1 2025



Tendance de détection de Kaleidoscope au S1 2025, moyenne mobile sur sept jours

Création d'une application jumelle leurre

Tout d'abord, les attaquants soumettent une application légitime (le jumeau leurre) dans les app stores officiels. Cette application est véritablement inoffensive ; il pourrait s'agir d'un simple jeu de puzzle ou d'un utilitaire. Comme il est disponible dans la boutique officielle, les utilisateurs lui font confiance.

Création du jumeau maléfique

Ensuite, les attaquants créent une autre version de la même application, mais cette version est malveillante (le jumeau maléfique). Elle utilise le même nom d'application et le même identifiant unique appelé « app ID », mais elle contient du code supplémentaire qui génère des impressions publicitaires frauduleuses. Celles-ci apparaissent de manière inattendue et intrusive, même lorsque l'application n'est pas activement utilisée.

Distribution du jumeau maléfique

Comme les app stores officiels bloquent activement les applications malveillantes connues, les attaquants diffusent le jumeau maléfique via des app stores ou des sites web tiers. Ils utilisent souvent des publicités et des offres trompeuses pour faire croire aux utilisateurs qu'il s'agit de la version légitime disponible sur les app stores officiels, ce qui les amène à télécharger la version jumelle maléfique.

Association du jumeau maléfique au jumeau leurre

La clé de la réussite de Kaleidoscope réside dans la façon dont le jumeau maléfique « fait semblant » d'être l'application leurre légitime. Les jumeaux partagent le même identifiant unique d'application, que les annonceurs et les systèmes automatisés utilisent pour identifier les applications. Par conséquent, le trafic frauduleux généré par le jumeau maléfique semble provenir de la version inoffensive et légitime. Les publicités intrusives sont bien réelles, mais non autorisées et générées par le jumeau maléfique, ce qui amène les annonceurs à payer les fraudeurs pour des publicités illégitimes.

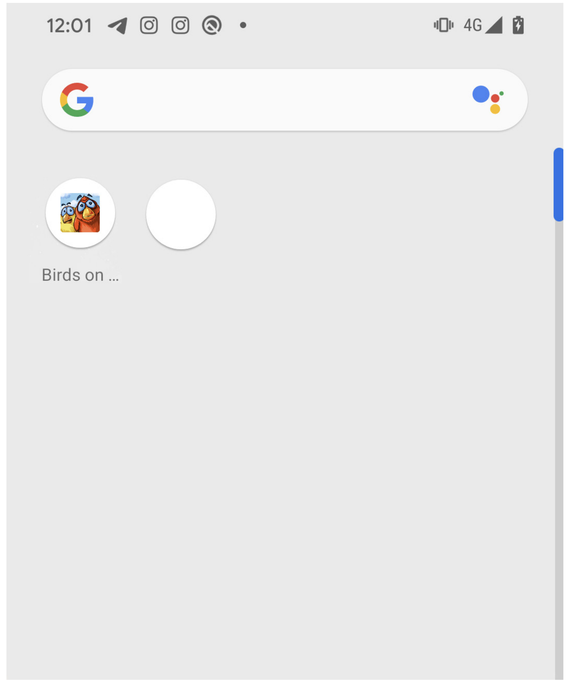
En d'autres termes, l'application jumelle maléfique vole l'identité de l'application légitime, ce qui permet aux fraudeurs de tirer profit de publicités qui semblent authentiques mais qui sont trompeusement intrusives.

Il est intéressant de noter que les icônes de certains jumeaux maléfiques sont très différentes de celles de leurs jumeaux leurres. Par exemple un cercle blanc sans nom alors que les jumeaux leurres ont une icône d'application plus standard.

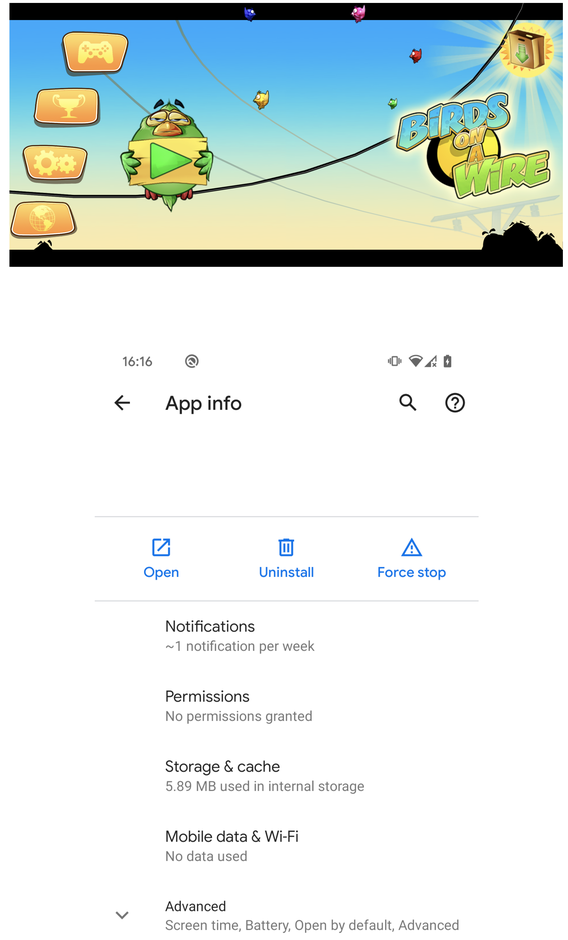
Lorsqu'elles sont ouvertes, ces applications fonctionnent également différemment. Par exemple, le fait d'appuyer sur l'icône du leurre lance le jeu Birds on a Wire. En revanche, le fait d'appuyer sur l'icône blanche du jumeau maléfique ne fait qu'afficher l'écran d'information sur l'application, sans interface utilisateur. Les deux applications sont présentées dans les visuels ci-contre.

Kaléidoscope n'est pas tout à fait nouveau. Il est l'évolution d'une fraude similaire découverte auparavant, appelée **Konfety**, qui détournait un cadre publicitaire appelé CaramelAds. Après la découverte de Konfety, les attaquants ont changé de stratégie. Ils ont supprimé les références à CaramelAds, et ont créé de nouveaux SDK avec des noms différents qui ont permis à Kaleidoscope de continuer à passer inaperçu, prouvant ainsi sa capacité à s'adapter en permanence.

Les utilisateurs peuvent se protéger efficacement en comprenant le fonctionnement de ce jumeau maléfique, en s'en tenant aux app stores officiels, en prêtant attention aux comportements inhabituels des applications et en gérant soigneusement les autorisations des applications.



L'icône de l'application du leurre est Birds on a Wire tandis que l'icône du jumeau maléfique est un cercle blanc

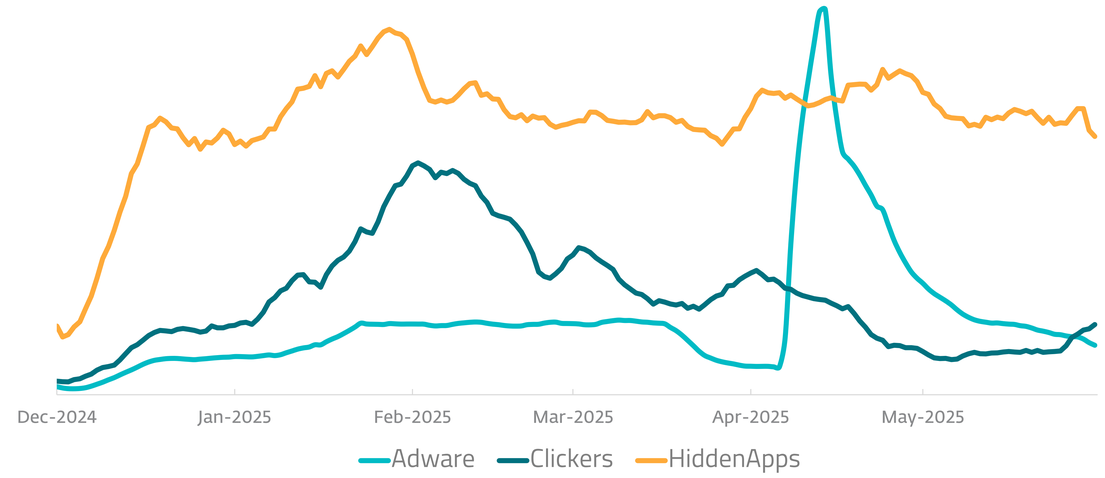


L'icône du leurre sert bien à lancer le jeu Birds on a Wire (en haut), tandis que l'icône blanche du jumeau maléfique affiche un écran d'information sur l'application (en bas)

Les menaces associées à la publicité continuent de générer des revenus grâce aux utilisateurs mobiles

Au premier semestre 2025, ESET a observé une augmentation significative de deux types de détections Android qui profitent des publicités : les adwares et les clickers. Ensemble, ces catégories ont augmenté de 160 %, dépassant de loin l'augmentation de 50 % observée pour tous les types de détections sur Android. Les adwares affichent des publicités non sollicitées sur les appareils des utilisateurs, tandis que les clickers génèrent des revenus publicitaires frauduleux en cliquant automatiquement sur des publicités à l'insu de l'utilisateur. Une troisième catégorie, les hiddenapps, sont des applications qui se cachent après leur installation et qui effectuent différentes actions malveillantes telles que l'affichage de publicités intrusives. Elle a cependant connu une baisse de 60 % des détections au cours de cette période. Au total, les adwares, les clickers et les hiddenapps représentaient 48 % de toutes les détections sur Android au S1 2025.

Certaines applications présentant un tel comportement sont classées par ESET dans la catégorie des applications potentiellement indésirables (PUA). Bien qu'elles ne soient pas des malwares, les PUA peuvent néanmoins avoir un comportement intrusif ou trompeur, comme l'affichage excessif de publicités, le ralentissement de l'appareil, le déchargement de la batterie et la collecte non autorisée de données, ce qui affecte négativement l'expérience de l'utilisateur et l'expose potentiellement à des risques pour sa sécurité et la protection de sa confidentialité. ESET Mobile Security permet aux utilisateurs de bloquer ou d'autoriser les PUA, offrant ainsi une certaine flexibilité à ceux qui sont prêts à tolérer certains comportements intrusifs pour utiliser les fonctionnalités principales d'une application. Nous recommandons cependant vivement d'activer la détection des PUA pour protéger votre appareil, votre confidentialité et votre sécurité.



Tendances de détection des adwares, clickers et hiddenapps sur Android au S2 2024 et S1 2025, en moyenne mobile sur sept jours

Android NFC Escroqueries

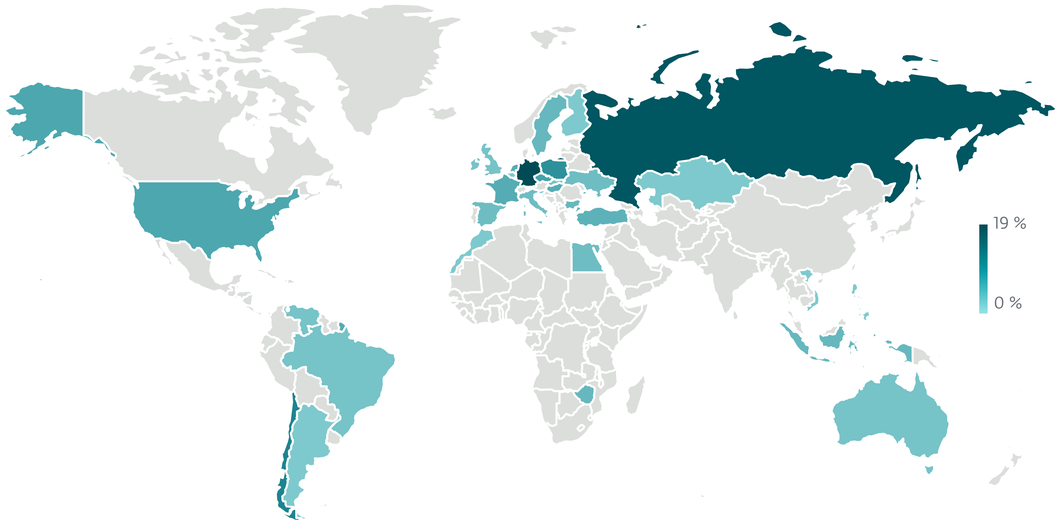
Évolution de la fraude à la technologie NFC : NGate, GhostTap et escroqueries par relais

La fraude à la technologie NFC a été multipliée par plus de trente-cinq, alimentée par des campagnes d'hameçonnage et des techniques de relais inventives.

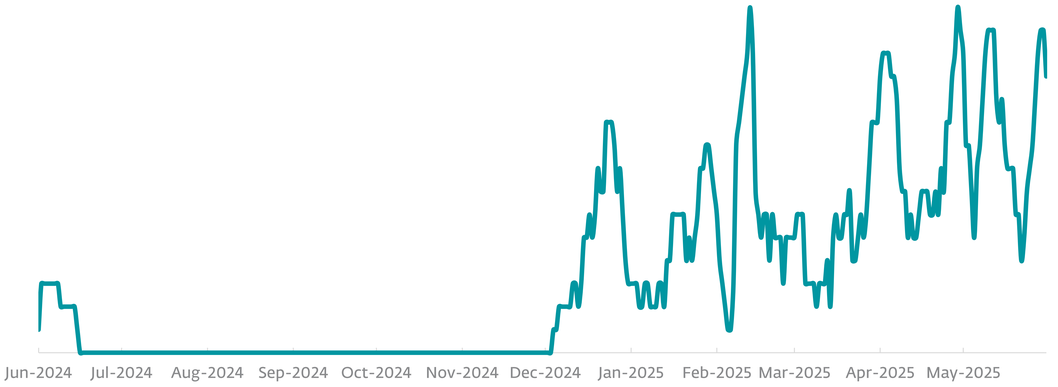
La technologie NFC (communication en champ proche) a transformé la manière dont des millions de personnes effectuent des paiements et utilisent des applications bancaires. Il suffit de rapprocher son téléphone ou une carte de paiement sans contact d'un terminal de paiement en magasin pour effectuer des achats ou d'un distributeur automatique de billets pour effectuer des retraits en l'espace de quelques secondes. La technologie NFC permet à un smartphone équipé d'applications telles que Google Pay et Apple Pay de communiquer avec un terminal de paiement pour effectuer facilement des paiements mobiles lorsqu'ils sont placés à proximité l'un de l'autre.

Lorsqu'elle est utilisée de manière légitime, la technologie NFC permet des paiements plus rapides et plus sûrs que les anciennes méthodes telles que les bandes magnétiques. Malheureusement, les cybercriminels ont également jeté leur dévolu sur la technologie NFC, créant une vague de malwares hautement spécialisés et de nouveaux systèmes de fraude qui l'exploitent.

Selon la télémétrie d'ESET, les escroqueries par NFC ont été multipliées par plus de trente-cinq au S1 2025 par rapport à S2 2024. Au cours de la période précédente, couverte par le Rapport général sur les menaces du S2 2024, nous n'avons enregistré qu'une seule détection par semaine et les escroqueries n'ont touché qu'un groupe



Répartition géographique des escroqueries et des malwares Android lés à la technologie NFC au S1 2025



Tendance de détection des malwares Android liés à la technologie NFC au S2 2024 et S1 2025, moyenne mobile sur sept jours

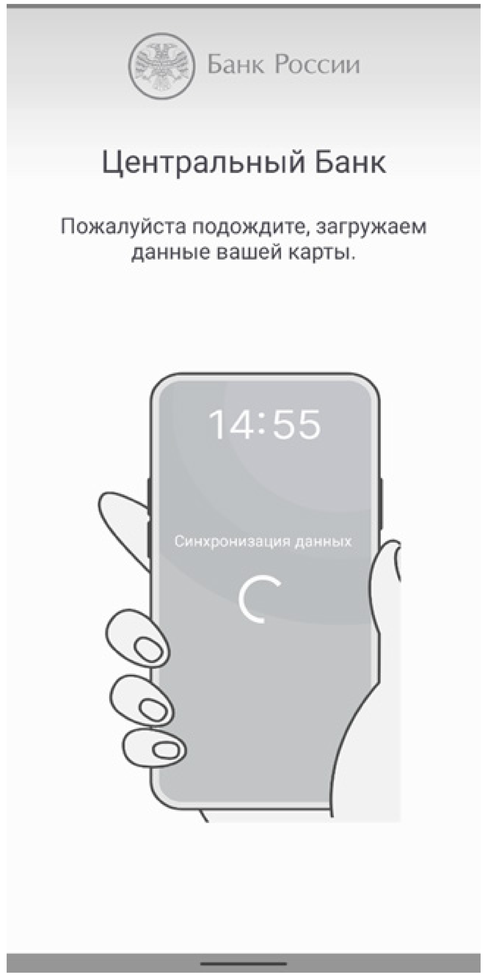
limité de détenteurs de cartes dans quelques régions. Au premier semestre 2025, cependant, les détections s'élevaient à plusieurs dizaines par semaine. Bien que les chiffres au niveau mondial restent modestes, ce bond met en évidence l'évolution rapide des méthodes des criminels et l'attention constante qu'ils portent à l'exploitation de la technologie NFC.

NGate : un pionnier des malwares NFC

En 2024, les chercheurs d'ESET **ont analysé** une nouvelle menace mobile, que nous avons appelée NGate. Une fois installé sur l'appareil de la victime, le malware relaie les signaux NFC de la carte de paiement de la victime à travers le téléphone compromis vers des appareils contrôlés par l'attaquant, ce qui permet aux criminels de retirer de l'argent à distance dans des distributeurs automatiques de billets. Il s'agit de l'un des premiers cas documentés de malware mobile utilisant la fonctionnalité de relais de données de NFC pour voler directement de l'argent sur les comptes bancaires des victimes.

À l'époque, NGate ciblait les clients de certaines banques en Tchécoslovaquie, en Pologne, en Hongrie et en Géorgie. NGate détourne un outil open-source appelé NFCGate, initialement prévu pour un usage universitaire. Il permet aux utilisateurs de capturer, d'analyser et de modifier les données de NFC entre les appareils, mais les cybercriminels ont rapidement reconnu son potentiel malveillant.

Depuis, la télémétrie d'ESET a également détecté NGate en Russie, en Allemagne et au Chili.

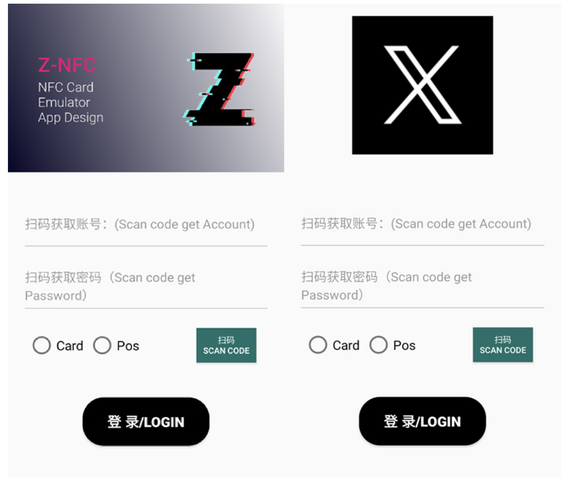


Application malveillante, détectée par ESET comme **Android/NGate**, qui imite l'application de la Banque centrale de Russie

GhostTap : des escroqueries par relais visant des portefeuilles numériques

Malheureusement, les acteurs de menaces se sont inspirés du succès de NGate et ont fait évoluer cette méthode. Une nouvelle technique, appelée **GhostTap** consiste pour les cybercriminels à utiliser secrètement les données de cartes stockées dans des portefeuilles numériques tels que Google Pay et Apple Pay. Les criminels déploient, par exemple, des messages d'hameçonnage convaincants qui invitent les victimes à saisir les détails de leur carte de paiement sur de faux sites web, puis leur demandent de communiquer le code de passe à usage unique destiné à confirmer le transfert d'une carte dans un portefeuille numérique. Avec les données et le code de la carte, les attaquants enregistrent les identifiants volés dans leurs propres portefeuilles Apple ou Google. Ils relaient ensuite ces portefeuilles chargés pour effectuer des paiements sans contact frauduleux partout dans le monde.

Les attaquants de GhostTap créent des transactions frauduleuses en rapprochant des appareils mobiles compromis de terminaux de paiement équipés de la technologie NFC. Ces transactions semblent légitimes, contournent les contrôles de sécurité traditionnels et permettent aux criminels d'encaisser rapidement de l'argent. GhostTap montre comment la fraude à la technologie NFC pourrait s'étendre massivement, avec les criminels mettant en œuvre des fermes à téléphones Android chargés de données de cartes compromises pour automatiser les transactions frauduleuses contre les banques et les commerçants dans le monde entier, qui ont déjà subi des pertes en raison des campagnes de fraude liées à GhostTap.

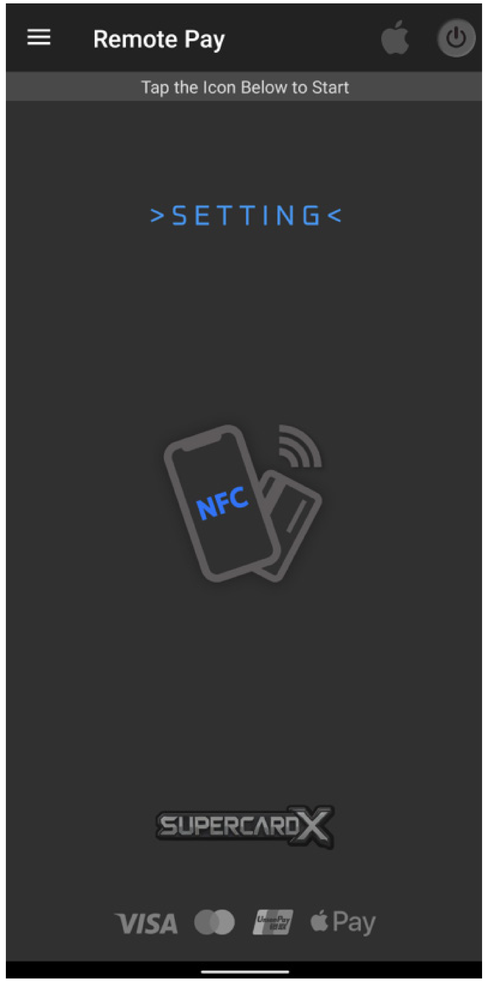


Outils **GhostTap**

Plusieurs groupes de cybercriminels chinois font la promotion active des **outils GhostTap** sur Telegram et sur les marchés du dark-web. Les criminels automatisent désormais les transactions frauduleuses par la technologie NFC et ciblent des institutions financières aux États-Unis, au Royaume-Uni, en Australie, au Canada, aux Émirats arabes unis et en Arabie saoudite.

SuperCard X : des malwares avec un modèle économique

Cette année, des chercheurs de **Cleafy** ont découvert une nouvelle menace appelée SuperCard X, dont le code est en grande partie similaire à celui de NGate. SuperCard X est diffusé via des attaques d'ingénierie sociale sophistiquées. Les victimes reçoivent des



SuperCard X capture des données de NFC lorsque les victimes rapprochent leur carte de paiement de leur téléphone compromis

SMS convaincants qui se font passer pour des alertes de sécurité bancaire pour les inciter à contacter les attaquants qui se font passer pour des représentants de la banque. Au cours de ces appels, les criminels gagnent la confiance des victimes et leur demandent d'installer une application malveillante déguisée en outil de sécurité.

Une fois installé, SuperCard X capture discrètement les données de NFC lorsque les victimes rapprochent leur carte de paiement de leur téléphone compromis, et les transmet instantanément à un autre appareil contrôlé par les attaquants. Les criminels utilisent ensuite ces données relayées pour effectuer des paiements sans contact frauduleux dans des magasins ou retirer de l'argent depuis des distributeurs automatiques.

Contrairement aux malwares précédents, l'outil est disponible en tant que service (MaaS). Cela signifie que les cybercriminels qui n'ont pas de compétences techniques approfondies peuvent facilement accéder à des outils de fraude à la technologie NFC et les déployer. SuperCard X fournit deux applications Android distinctes aux criminels : l'application Reader installée sur les appareils des victimes et l'application Tapper, contrôlée par les attaquants. Ces deux applications communiquent par l'intermédiaire d'un serveur de C&C sécurisé qui permet de relayer en temps réel et de manière transparente les données de NFC de la victime à l'attaquant.

L'une des principales innovations de SuperCard X est sa conception minimaliste, qui ne demande que des autorisations NFC de base. Contrairement aux malwares bancaires mobiles traditionnels, SuperCard X peut passer inaperçu parce qu'il se présente comme une application NFC inoffensive qui ne demande pas beaucoup d'autorisations. SuperCard X utilise par ailleurs une méthode de chiffrement sophistiquée qui empêche l'analyse et la détection du trafic malveillant par les chercheurs et les outils de sécurité. Ces tactiques avancées donnent à SuperCard X un avantage significatif sur les menaces plus anciennes.

ÉCLAIRAGE DE NOTRE EXPERT

Chaque itération de la fraude à la technologie NFC montre comment les attaquants s'adaptent aux nouvelles mesures de sécurité. Même les solutions avancées, comme l'authentification multifacteur ou la surveillance des transactions en temps réel, se heurtent à des difficultés lorsque les criminels relaient physiquement les données de la carte en quelques secondes. Les campagnes de smishing organisées, combinées à des interfaces de malwares très élaborées, rendent également la détection des fraudes encore plus difficile pour les utilisateurs ordinaires.

Nous nous attendons à ce que ces techniques criminelles évoluent encore. Certains groupes combinent déjà le vol de données de NFC avec d'autres moyens, telles que le smishing ou les escroqueries par centre d'appel, pour continuer à tromper des victimes. Néanmoins, les institutions financières vigilantes, les fabricants d'appareils et la communauté de la cybersécurité surveillent et réagissent à ces menaces. Les titulaires de cartes peuvent également bloquer une grande partie des attaques en téléchargeant des applications uniquement à partir d'app stores officiels, en vérifiant les autorisations des applications, en ignorant les liens suspects et en ne faisant jamais de paiement sans contact avec leur carte physique à moins d'être absolument certain de son utilisation légitime.

Lukáš Štefanko, Senior Malware Researcher chez ESET

Ransomwares

Guerre des gangs : quand les ransomwares s'entre-déchirent

Tandis que le nombre de gangs et d'attaques de ransomwares augmente, les groupes de ransomwares s'affrontent de plus en plus, ce qui touche plusieurs acteurs, y compris RansomHub, le principal Ransomware As a Service.

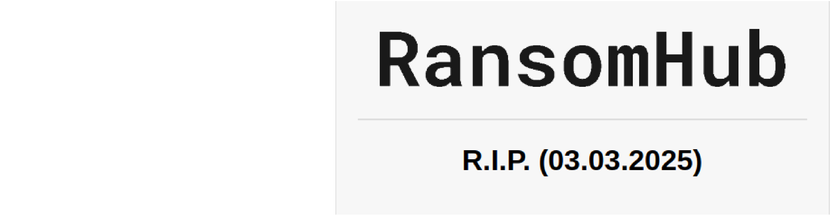
Au premier semestre 2025, les données résumées du service **ecrime.ch** pour 2024 ont montré que les attaques de ransomwares ont augmenté de 15 % et que le nombre de gangs de ransomwares a augmenté de 43 % par rapport à l'année précédente. De manière surprenante, selon **Chainalysis**, la valeur totale des paiements de rançons a pris la direction opposée, chutant de 35 %. Cette contradiction peut être le résultat des démantèlements et des escroqueries de sortie qui ont remanié la scène des ransomwares en 2024, et elle est également due en partie à une diminution de la confiance dans la pérennité des gangs et leur capacité à respecter leur part du marché .

Que les combats commencent !

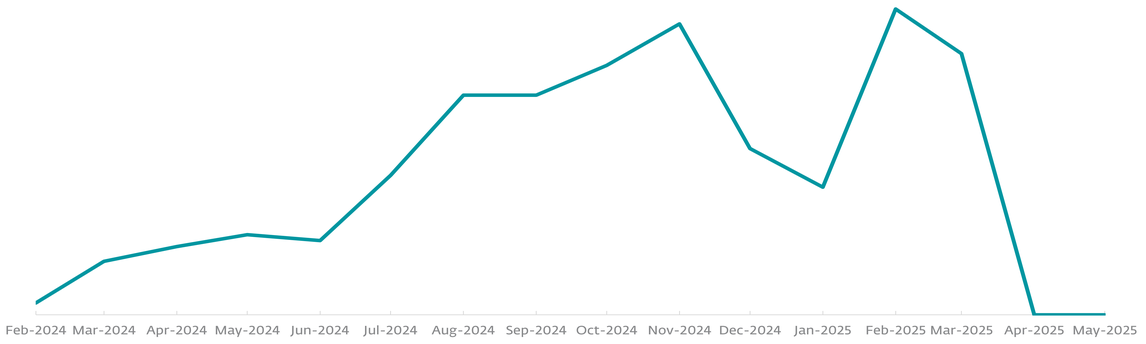
Si l'on considère l'évolution au S1 2025, cette évaluation reste valable. Le « nouvel ordre » récemment établi, avec la domination de RansomHub et l'accumulation d'un grand nombre d'affiliés à son service, a une fois de plus été perturbé en raison des luttes intestines et des défigurations de sites que les opérateurs de ransomwares se sont infligées les uns aux autres.

Les affrontements les plus visibles sont attribués au gang DragonForce, un groupe effronté comptant des dizaines de victimes sur son site de fuite de données. Bien qu'il ne soit qu'un acteur mineur jouissant d'une faible confiance de la part de ses affiliés, c'est ce groupe qui s'est lancé dans une campagne de vandalisme en mars, contre les sites web de BlackLock, Mamona et RansomHub, le RaaS numéro un à l'époque.

DragonForce est même allé jusqu'à prétendre que RansomHub avait volontairement rejoint son cartel, mais sans preuve. Cette affirmation a également été contredite lors d'un échange public animé sur le célèbre forum RAMP. Il est important de noter que le service, le site de fuite de données et les opérations de RansomHub n'ont pas redémarré depuis l'attaque.



Site de fuite de données RansomHub vandalisé



RansomHub est resté inactif après l'attaque et la défiguration par DragonForce

Ses affiliés, souvent d'anciens coconspirateurs de LockBit, se retrouvent donc à nouveau sans opérateur central.

Fuites de ransomwares de tous les côtés

Quelques jours après la défiguration du site de RansomHub, le site de fuite de données du ransomware Everest a lui aussi été pris pour cible, mais par un autre acteur de menaces, qui a laissé un message sarcastique : « Don't do crime CRIME IS BAD xoxo from Prague » (Ne commettez pas de crime, le crime est mauvais, bons baisers de Prague). La même formulation a ensuite remplacé le contenu du site de fuite de données de LockBit récemment relancé, avec un lien vers une archive des informations du gang. La base de données publiée comprenait les noms et les mots de passe en clair de dizaines d'administrateurs et d'affiliés utilisant le service RaaS, près de 60 000 adresses bitcoin uniques, des versions et des configurations utilisées par les affiliés, et plus de 4 400 messages documentant les négociations entre les criminels et leurs victimes.

Site de fuite de données de LockBit vandalisé

Un autre auteur de fuites, peut-être un membre mécontent du gang ou un chercheur qui a réussi à pénétrer dans les systèmes du groupe, a également **publié** des échanges de messages internes de l'opération de ransomware Black Basta s'étalant sur plusieurs semaines. Les données divulguées contenaient des informations sur les modèles d'hameçonnage du gang, les adresses de portefeuilles de cryptomonnaies, les sites de téléchargement de données et les identifiants des victimes.

Vers la fin du S1 2025, un nouveau compte **@GangExposed** sur X.com a relancé les ContiLeaks de 2022 et les TrickLeaks de 2023, en utilisant ces

Le domaine de blanchiment de cryptomonnaie Sinbad[.]io saisi par les forces de police

données pour doxxer les responsables et les membres du célèbre groupe de cybercriminels. Il s'agit notamment des cerveaux présumés connus sous les surnoms de Stern, Tramp et Target, qui ont des liens avec d'autres opérations de malwares en ligne telles que TrickBot, Black Basta et Royal Ransomware. L'identité d'au moins un des auteurs mentionnés a été **confirmée** par les forces de police allemandes.

Outre le « combat à mort » dans l'arène des ransomwares, les opérateurs et les affiliés ont également été activement poursuivis par les forces de police. Au premier semestre 2025, des suspects associés à plusieurs gangs tels que **DoppelPaymer**, **Nefilim**, **LockBit** et **Phobos/8Base** ont été arrêtés, extradés vers les États-Unis ou inculpés. Les autorités se sont également attaquées à l'infrastructure de soutien, en inculpant les opérateurs des sites de **blanchiment de cryptomonnaie** Blender.io et Sinbad.io pour avoir aidé à blanchir les revenus générés par les ransomwares, et ont **sanctionné** et **démantelé** l'hébergeur ZServers/XHost. Un affilié roumain de **Netwalker** a été condamné à une peine de 20 ans d'emprisonnement.

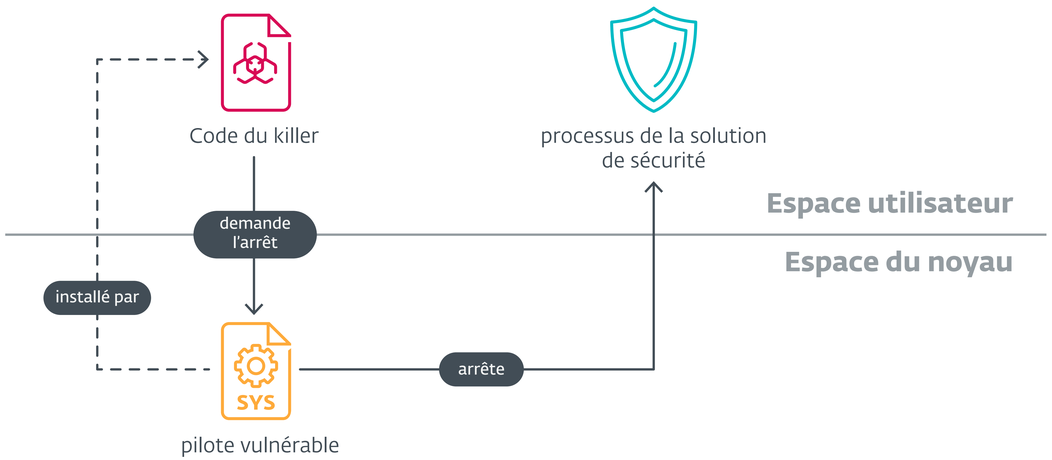
Autre nouvelle positive, le chercheur en sécurité Yohanes Nugroho a mis au point **Akira decryptor**, un nouveau déchiffreurs non conventionnel. Il exploite les spécificités de cette souche de ransomware et utilise des GPU très puissants pour déterminer les clés de déchiffrement par brute force. Le problème réside dans son déploiement, qui peut s'avérer un peu compliqué pour les victimes moins averties sur le plan technique.

Élargissement des boîtes à outils : EDR killers et détournement d'outils de RMM

Les gangs de ransomwares se vantent souvent de pouvoir contourner toutes les mesures de sécurité de leurs victimes. Pourtant, les solutions de détection et de réponse sur endpoints (EDR) semblent être une épine dans leur pied. Des épines si grosses, en fait, que plusieurs opérateurs de ransomwares ont développé de nouveaux outils, appelés EDR killers, conçus pour stopper, aveugler ou faire planter le produit de sécurité installé sur le système d'une victime.

Des acteurs moins matures ont tenté d'atteindre cet objectif en utilisant de simples scripts ou en détournant des outils légitimes tels que le détecteur de rootkits GMER ou PC Hunter. Les opérateurs de ransomwares plus avancés, cependant, développent leurs EDR killers autour de la technique BYOVD (utilisation d'un pilote vulnérable). Ces outils se composent généralement de deux parties : un composant « tueur » en mode utilisateur qui orchestre l'attaque, et un pilote légitime, vulnérable et signé, qui est installé et exploité par le composant tueur pour mettre fin aux processus de sécurité à partir du mode noyau.

Au S1 2025, les chercheurs d'ESET ont étudié l'un de ces EDR killer, **EDRKillShifter**, créé par le numéro un des RaaS à l'époque : RansomHub. Si les fonctionnalités d'EDRKillShifter ne diffèrent pas de celles des autres EDR killers, la protection du code présente une différence notable. Le shellcode, qui constitue la couche intermédiaire de la chaîne d'exécution, est protégé par un mot de passe de 64 caractères. Sans ce mot de passe, les chercheurs en sécurité ne peuvent pas accéder à la liste des processus ciblés ou au pilote détourné. Néanmoins, en tirant parti de la nature particulière d'EDRKillShifter, les chercheurs d'ESET ont pu identifier des liens entre les



Des EDR killers sophistiqués installent un pilote de noyau vulnérable qu'ils peuvent exploiter pour mettre fin aux processus de sécurité

affiliés de RansomHub et les gangs rivaux pour lesquels certains de ces affiliés travaillent également, à savoir Play, Medusa et BianLian.

EDRKillShifter n'est toutefois pas le seul outil sur le marché à viser les solutions EDR. Après leur montée en popularité, nous avons observé une augmentation du nombre et de la variété de ces EDR killers utilisés par des affiliés de ransomwares. MS4Killer d'Embargo, BadRentdrv2 et TFSysMon-Killer sont d'autres EDR killers bien connus. Ces deux derniers sont même disponibles publiquement sur GitHub.

Une autre tendance constante parmi les groupes de ransomwares observée par les chercheurs d'ESET est le détournement d'outils légitimes de surveillance et de gestion à distance (RMM), que les entreprises utilisent généralement pour gérer les postes à distance, et stopper les menaces internes et les fuites de données. Anydesk, MeshAgent et SimpleHelp figurent parmi les outils fréquemment utilisés. Hormis le cas où ces outils sont légitimement déployés par l'organisation, leur installation dans l'environnement devrait servir de signal d'alarme et déclencher une réaction immédiate afin d'atténuer leur éventuel détournement par un adversaire.

Le ransomware Interlock adopte ClickFix

Les gangs de ransomwares tentent de suivre les dernières évolutions, et il n'est donc pas surprenant que ClickFix, une technique d'ingénierie sociale en plein essor, ait attiré leur attention. Comme décrit **dans une section précédente** de ce rapport, ces attaques affichent une fausse erreur afin de manipuler les victimes pour qu'elles copient, collent et exécutent des commandes malveillantes sur leur appareil.

Utilisé à l'origine par des courtiers d'accès initiaux, ClickFix a probablement déjà contribué à des attaques de ransomwares, mais il a fallu attendre S1 2025 pour qu'un auteur de ransomwares l'utilise directement dans une **campagne**. Le ransomware Interlock a utilisé ClickFix pour se faire passer pour des outils informatiques tels que MS Teams et Advanced IP Scanner. Des commandes malveillantes téléchargeaient de faux programmes d'installation et ouvraient des sites légitimes au premier plan, tout en installant d'autres malwares ou en créant des portes dérobées PowerShell en arrière-plan.

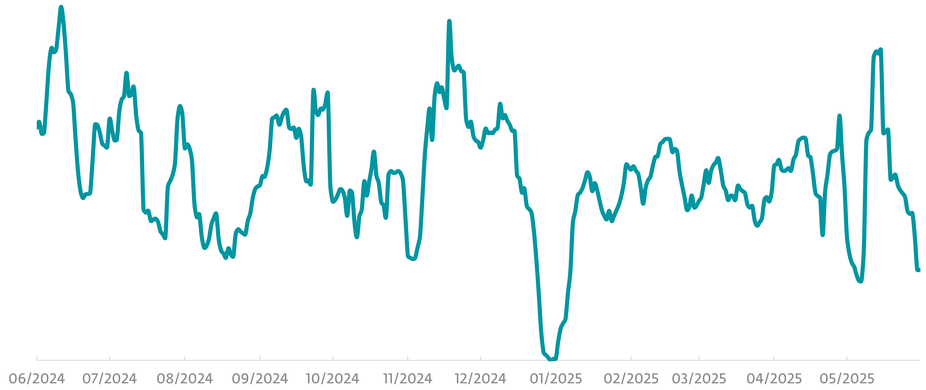
ÉCLAIRAGE DE NOTRE EXPERT

Alors que le premier trimestre 2025 a connu une croissance massive du nombre d'attaques signalées, la cessation soudaine des activités de RansomHub y a mis un point d'arrêt. Lorsque RansomHub est apparu en 2024 et a attiré les affiliés de LockBit et de BlackCat, les conditions étaient réunies pour qu'il connaisse une croissance rapide. Aujourd'hui, en revanche, le paysage des ransomwares est en proie au chaos, plus en raison de rivalités que des actions des forces de police. Nous pensons qu'avec le temps, un nouvel acteur dominant apparaîtra, mais aussi que les luttes intestines actuelles ne s'arrêteront pas de sitôt. DragonForce a peut-être attiré l'attention, mais il n'a pas gagné la confiance. Ses fausses affirmations selon lesquelles RansomHub aurait volontairement rejoint son « cartel » ne font qu'accroître son manque de crédibilité.

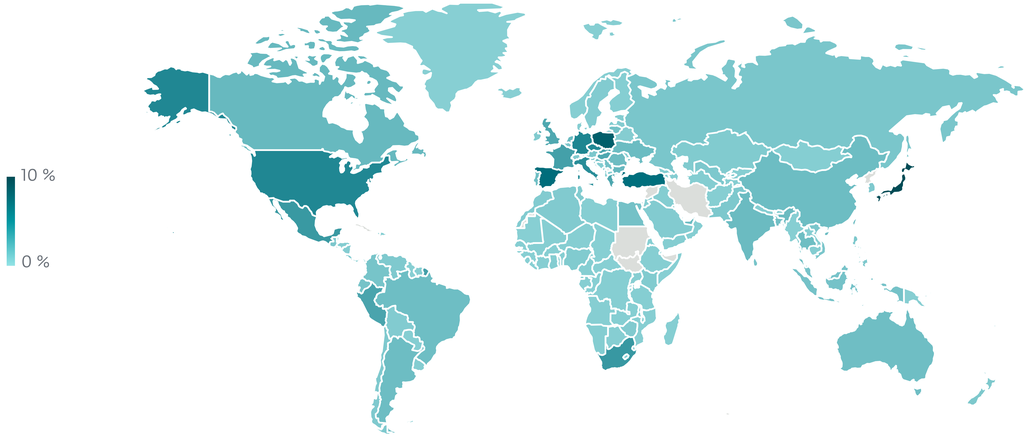
Jakub Souček, Senior Malware Researcher chez ESET

Télémétrie

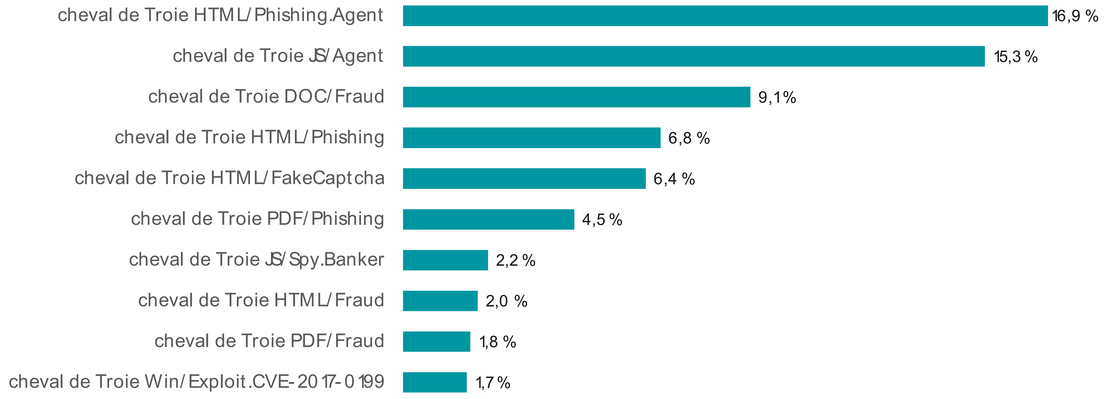
Toutes les menaces



Tendance de détection de toutes les menaces au S2 2024 et S1 2025, moyenne mobile sur sept jours

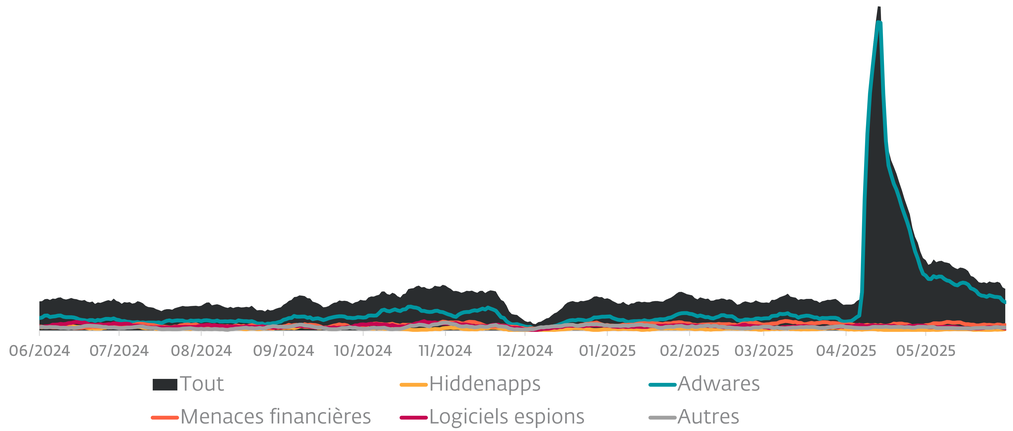


Répartition géographique des détections de malwares au S1 2025

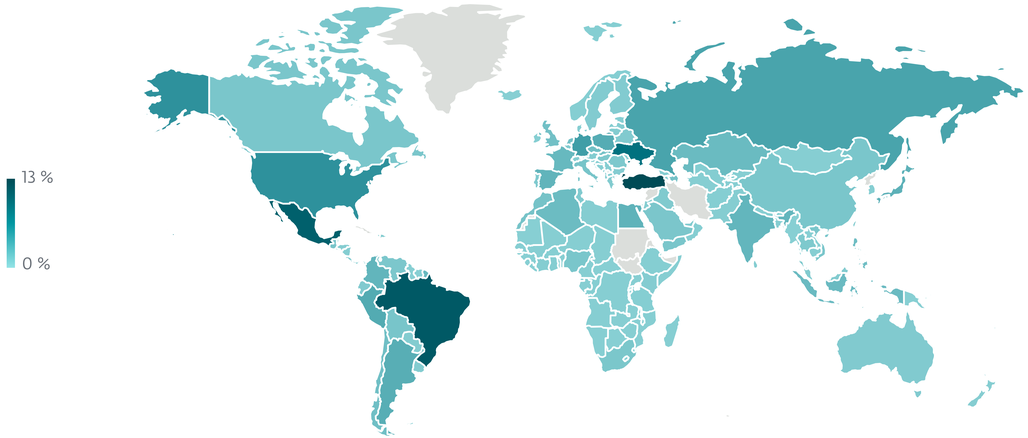


Top 10 des malwares détectés au S1 2025 (% des détections de malwares)

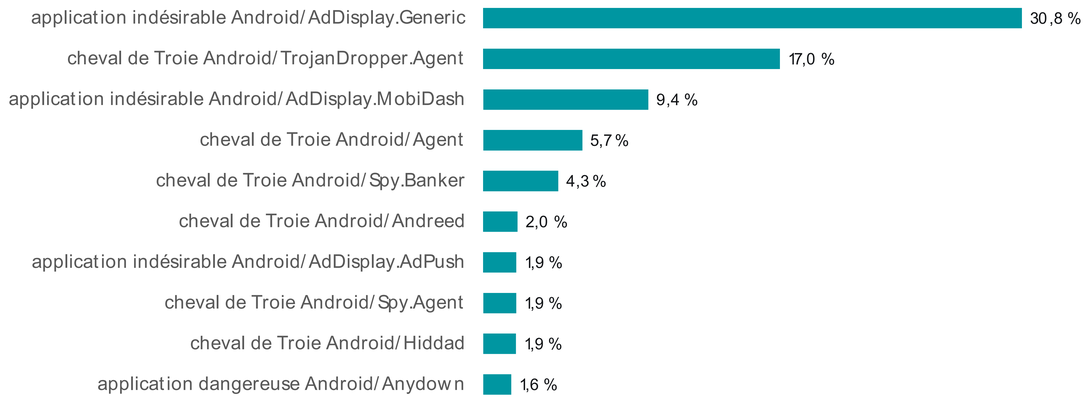
Android



Tendances de certaines catégories de détections sur Android au S2 2024 et S1 2025, moyenne mobile sur sept jours (les clickers, les extracteurs de cryptomonnaie, les ransomwares, les applications frauduleuses, les chevaux de Troie par SMS et les stalkerwares sont combinés dans la ligne de tendance Autres)[1]



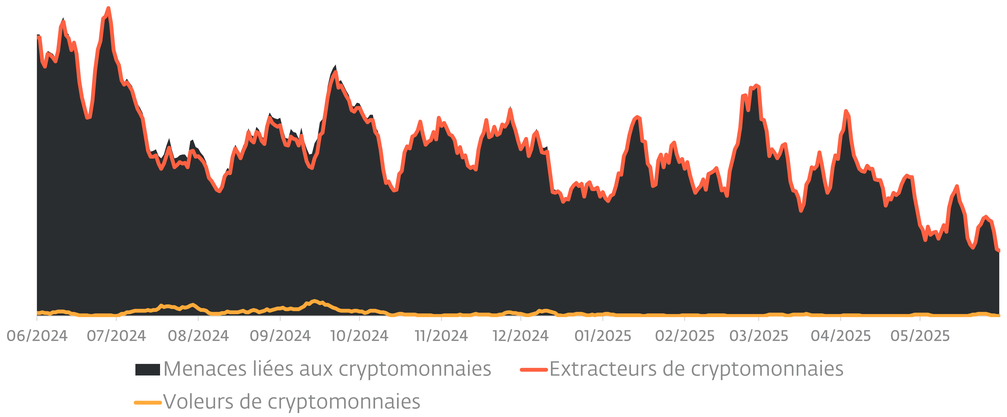
Répartition géographique des détections sur Android au S1 2025



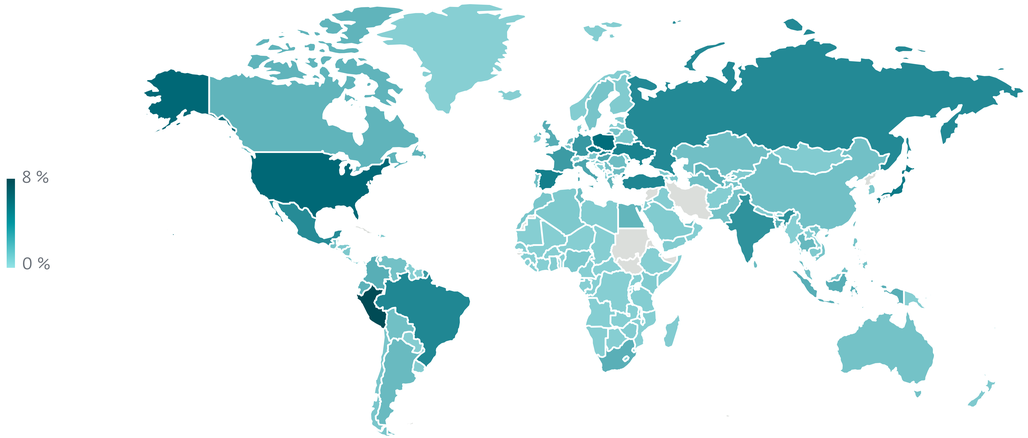
Top 10 des détections sur Android au S1 2025 (% des détections sur Android)

[1] La baisse du nombre de détections en décembre 2024 est due à une erreur de communication dans l'un des modules de nos produits de cybersécurité mobiles. Malgré ce problème, la sécurité et la protection des appareils Android sont restées pleinement efficaces et sans faille pendant cette période.

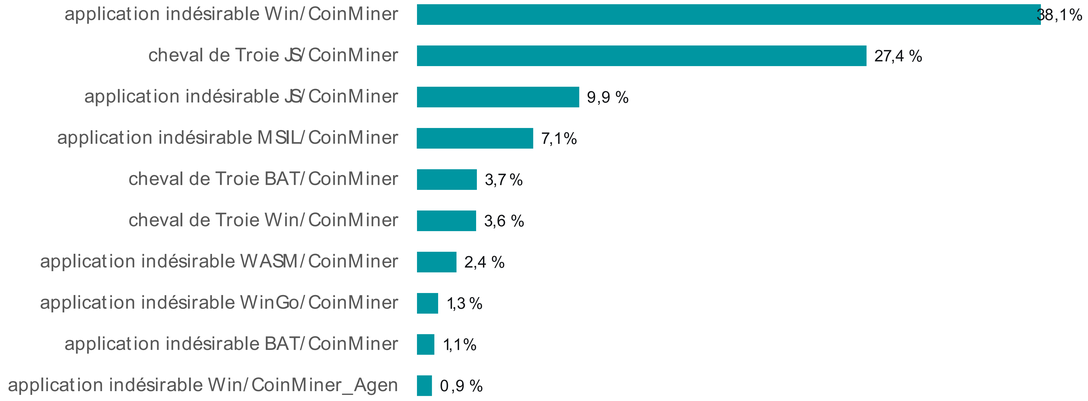
Menaces liées aux cryptomonnaies



Tendance de détection des menaces liées aux cryptomonnaies au S2 2024 et S1 2025, moyenne mobile sur sept jours



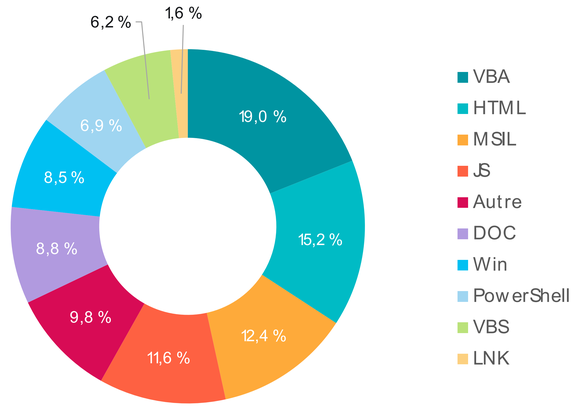
Répartition géographique des détections de menaces liées aux cryptomonnaies au S1 2025



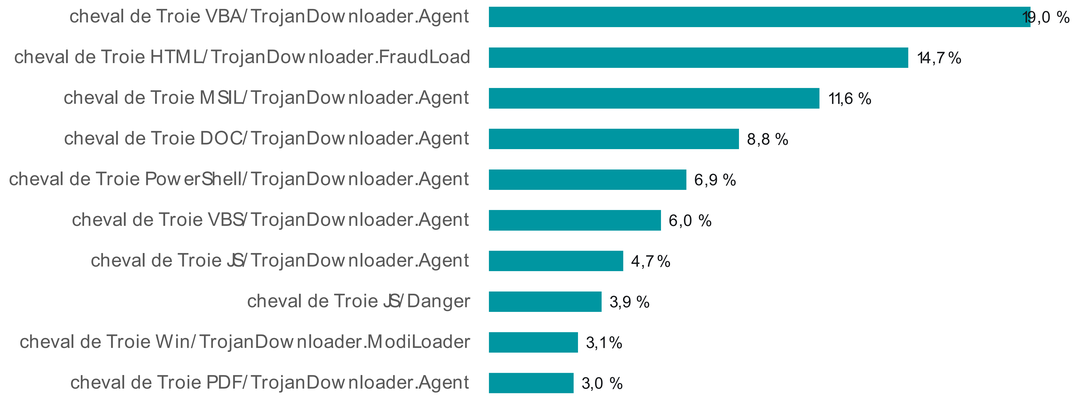
Top 10 des détections de menaces liées aux cryptomonnaies au S1 2025 (% des détections de menaces liées aux cryptomonnaies)

Téléchargeurs

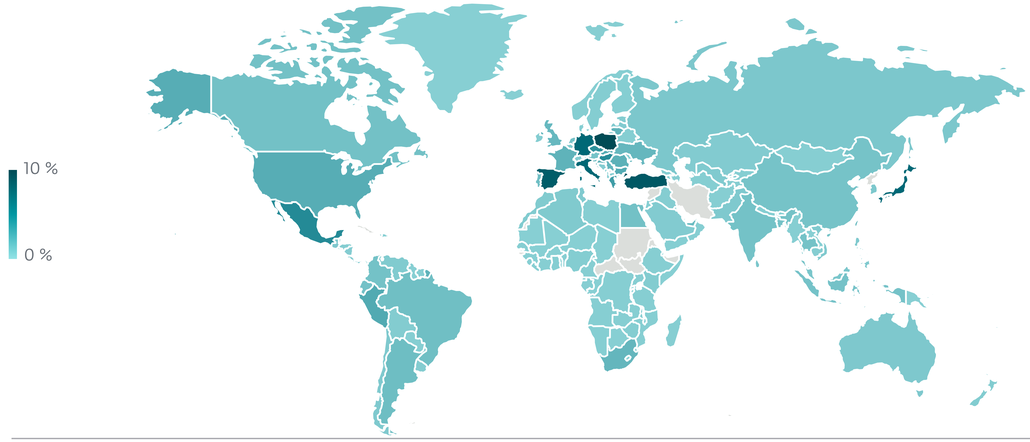
Tendance de détection des téléchargeurs au S2 2024 et S1 2025, en moyenne mobile sur sept jours



Détections des téléchargeurs par type de détection au S1 2025



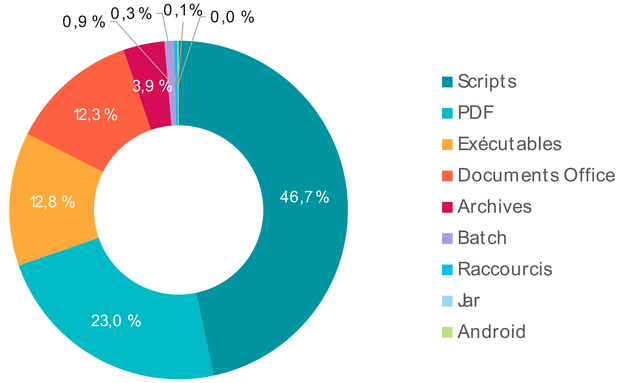
Top 10 des détections de téléchargeurs au S1 2025 (% des détections de téléchargeurs)



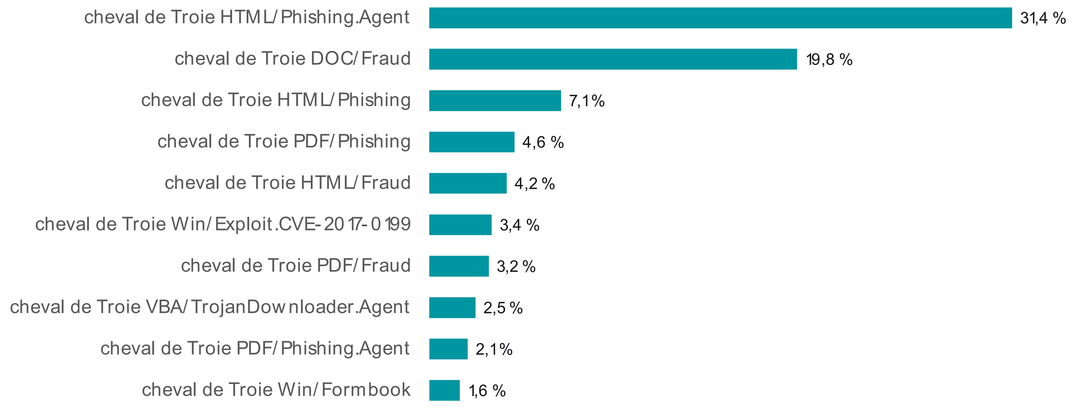
Répartition géographique des détections de téléchargeurs au S1 2025

Menaces par email

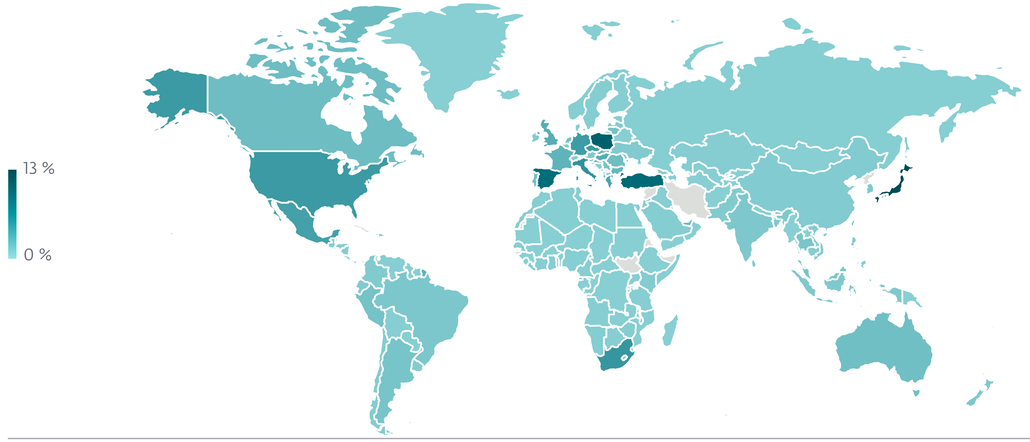
Tendance de détection d'emails malveillants au S2 2024 et S1 2025, moyenne mobile sur sept jours



Principaux types de pièces jointes d'emails malveillants au S1 2025

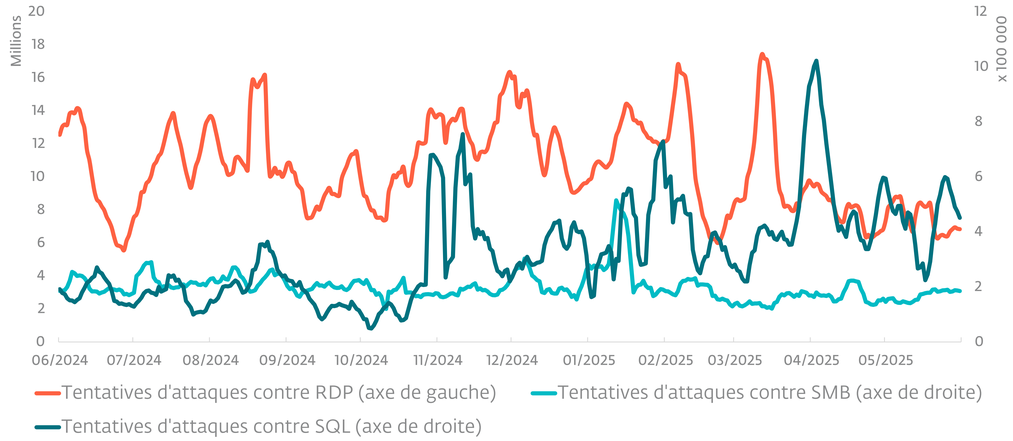


Top 10 des menaces détectées dans les emails au S1 2025

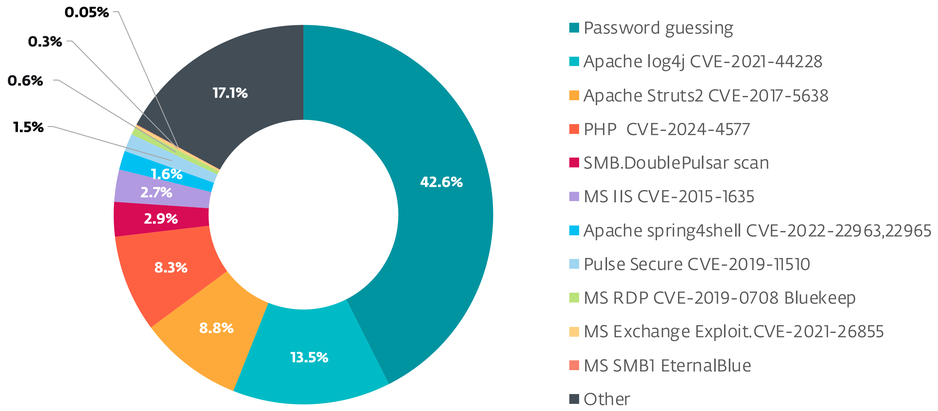


Répartition géographique des détections de menaces par email au S1 2025

Exploitations de vulnérabilités

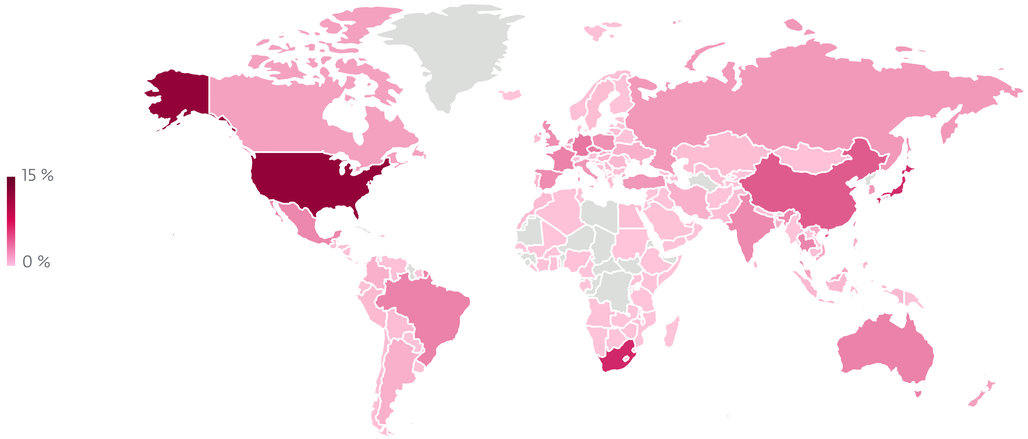


Tendances des tentatives d'attaque RDP, SMB et SQL au S2 2024 et S1 2025, moyenne mobile sur sept jours

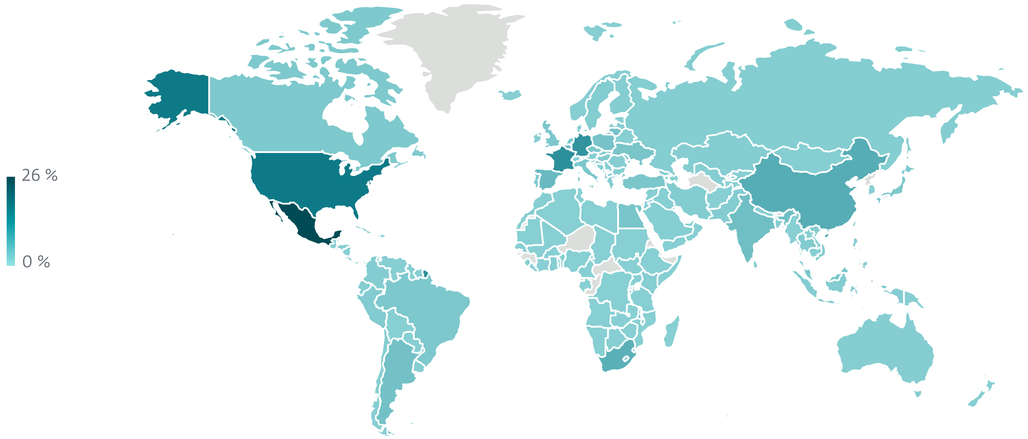


Vecteurs d'intrusions réseau externes signalés par des clients uniques au S1 2025

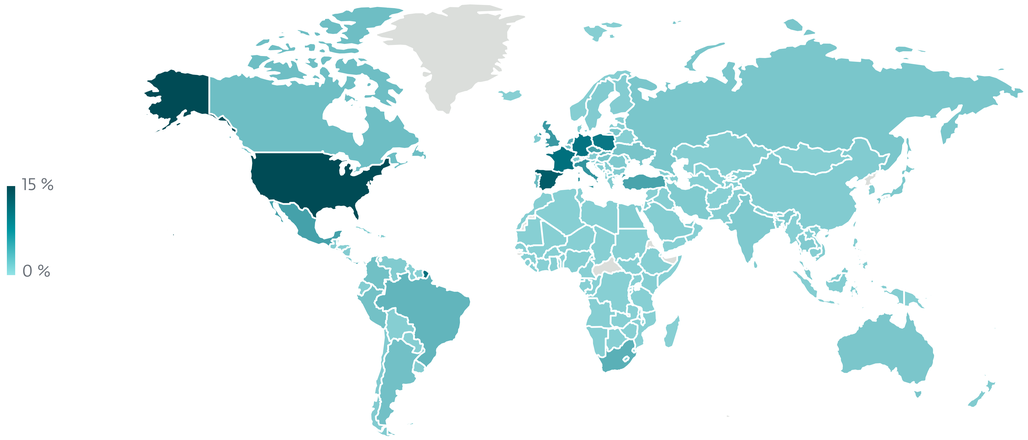
Exploitations de vulnérabilités



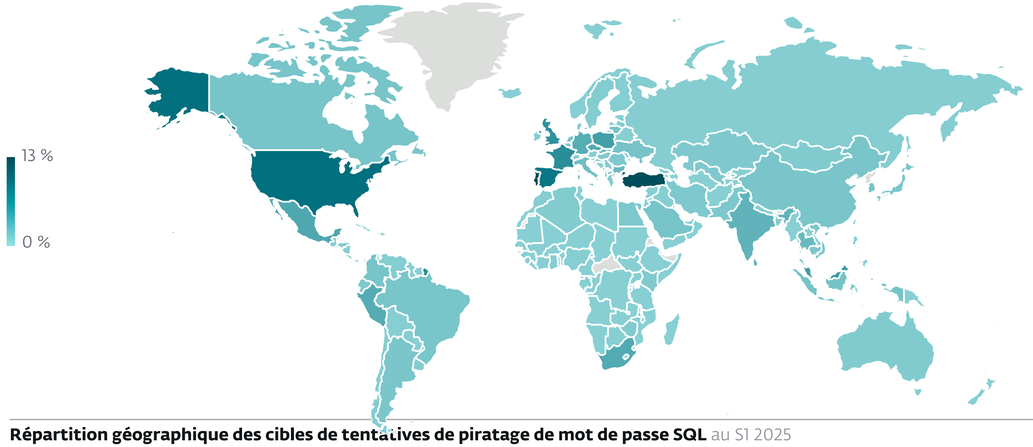
Répartition géographique des sources de tentatives de piratage de mot de passe RDP au S1 2025



Répartition géographique des cibles de tentatives de piratage de mot de passe SMB au S1 2025



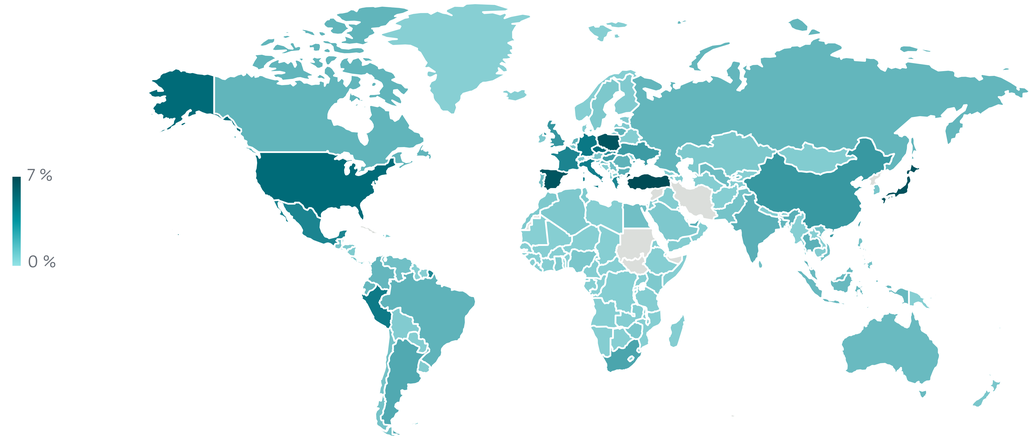
Répartition géographique des cibles de tentatives de piratage de mot de passe RDP au S1 2025



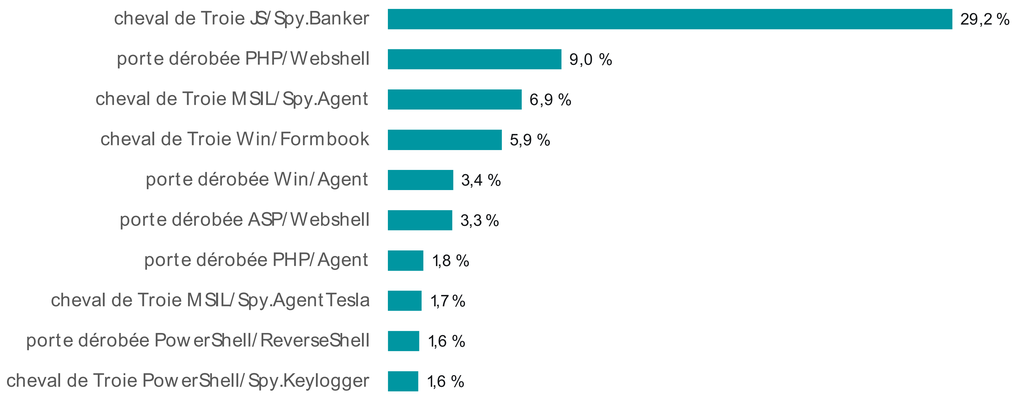
Répartition géographique des cibles de tentatives de piratage de mot de passe SQL au S1 2025

Infostealers

Tendance de détection des infostealers au S2 2024 et S1 2025, moyenne mobile sur sept jours

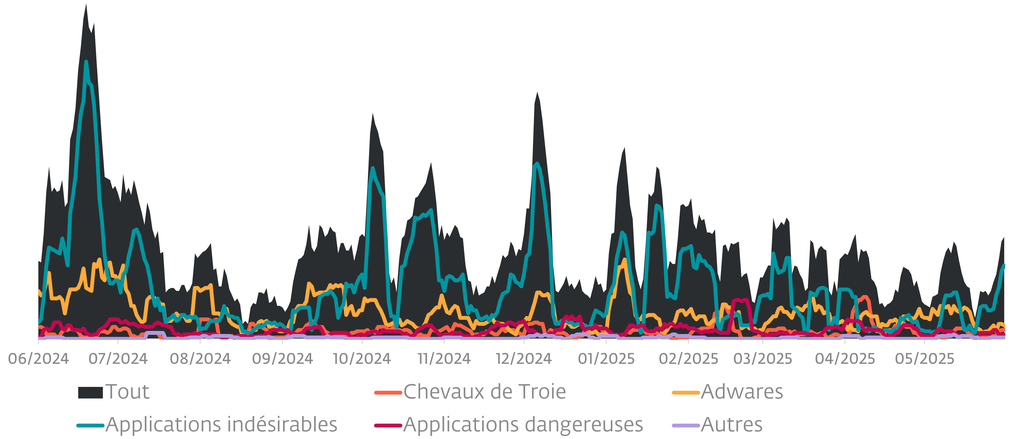


Répartition géographique des détections d'infostealers au S1 2025

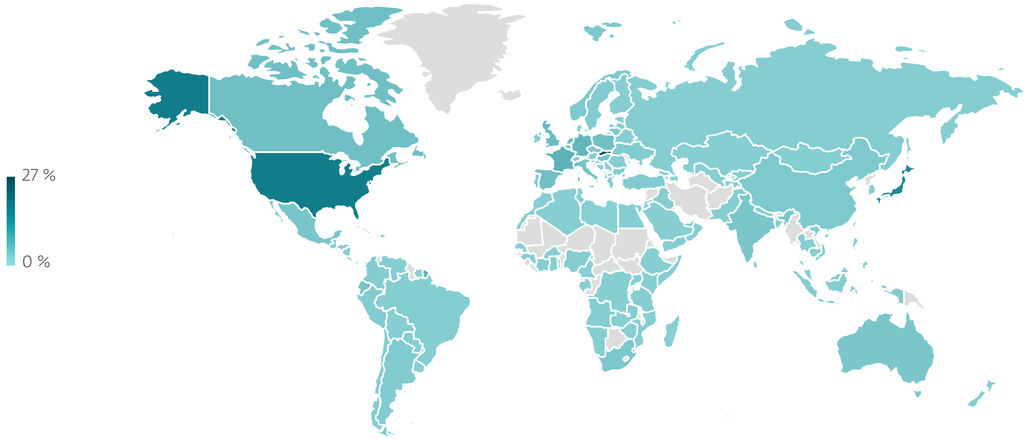


Top 10 des familles d'infostealers au S1 2025 (% des détections d'infostealers)

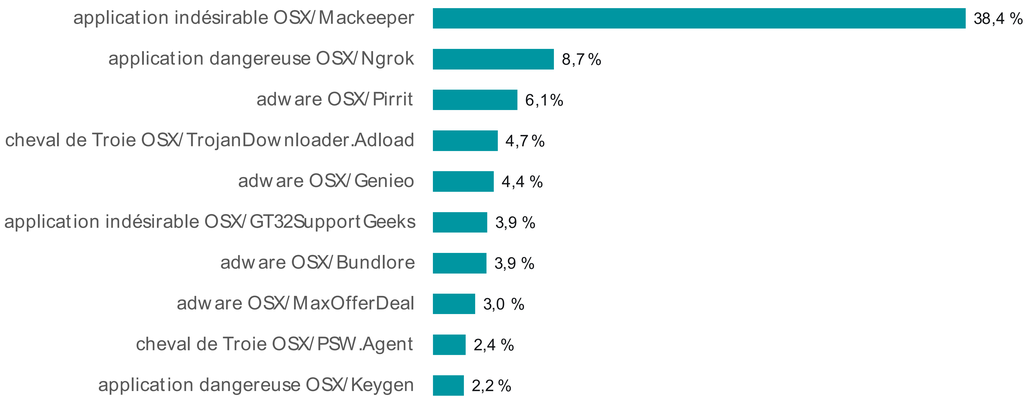
macOS



Tendance de détection sur macOS au S2 2024 et S1 2025, moyenne mobile sur sept jours

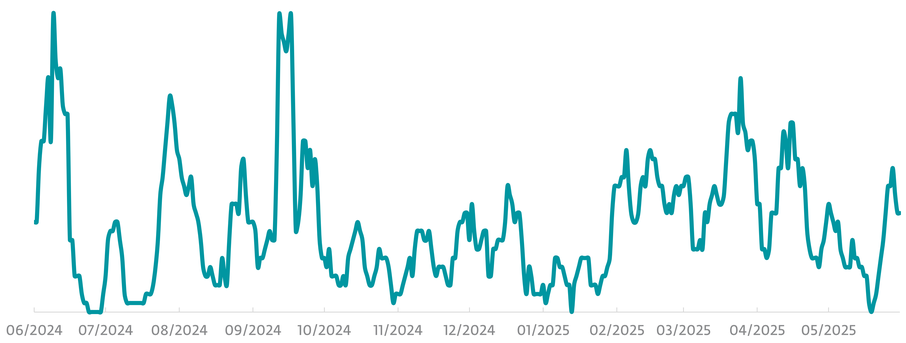


Répartition géographique des détections sur macOS au S1 2025

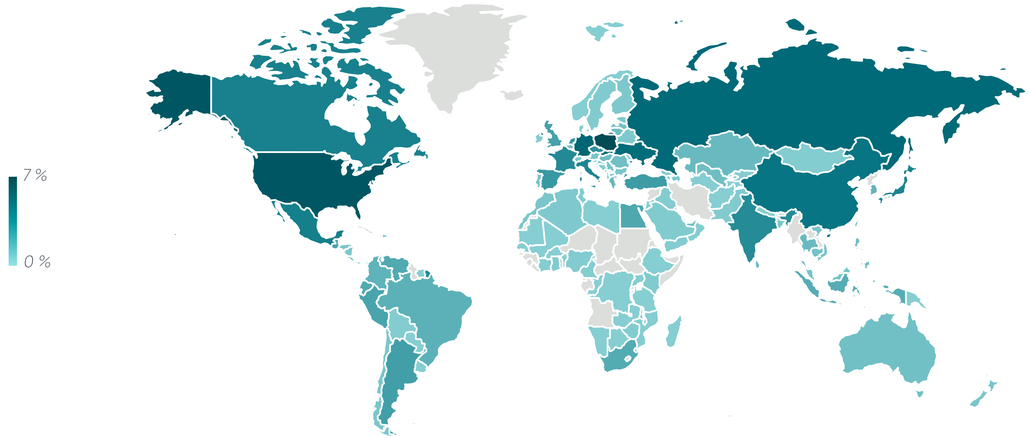


Top 10 des détections sur macOS au S1 2025 (% des détections sur macOS)

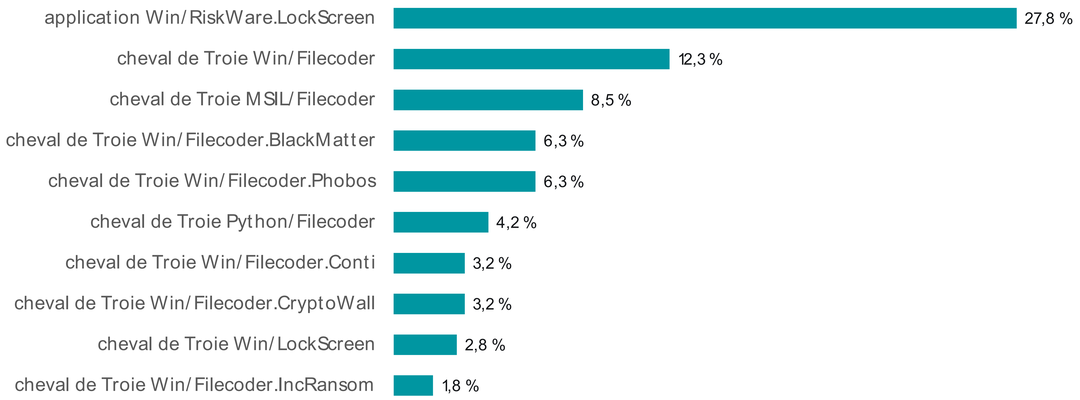
Ransomwares



Tendance de détection des ransomwares au S2 2024 et S1 2025, moyenne mobile sur sept jours

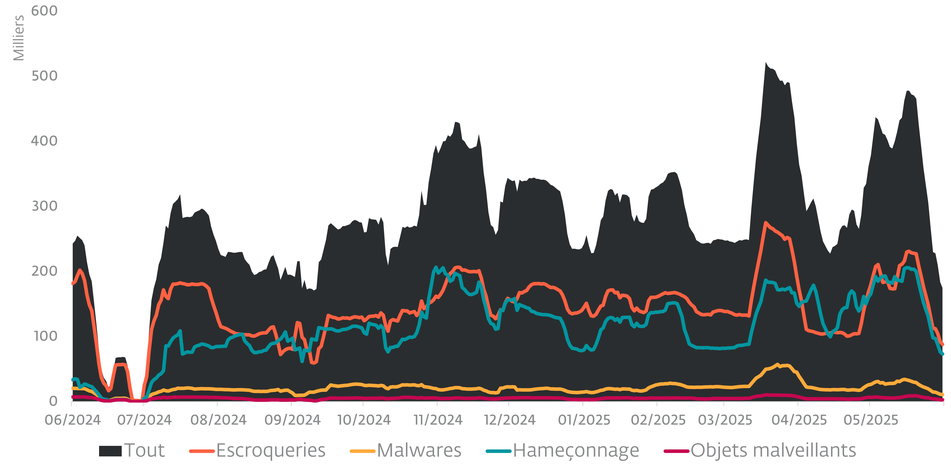


Répartition géographique des détections de ransomwares au S1 2025

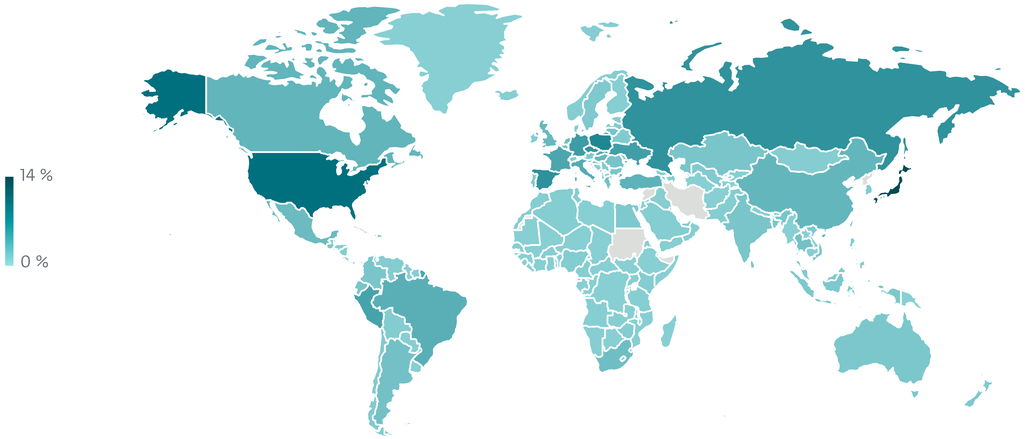


Top 10 des familles de ransomwares au S1 2025 (% des détections de ransomwares)

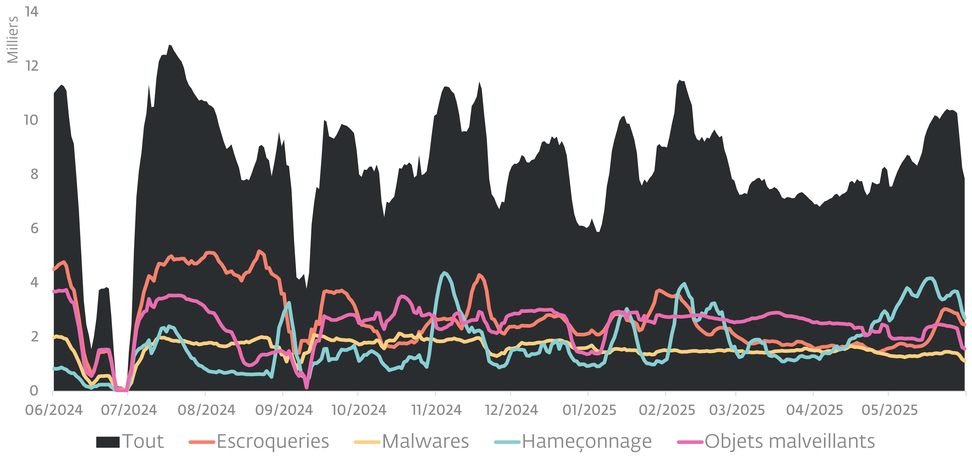
Menaces web



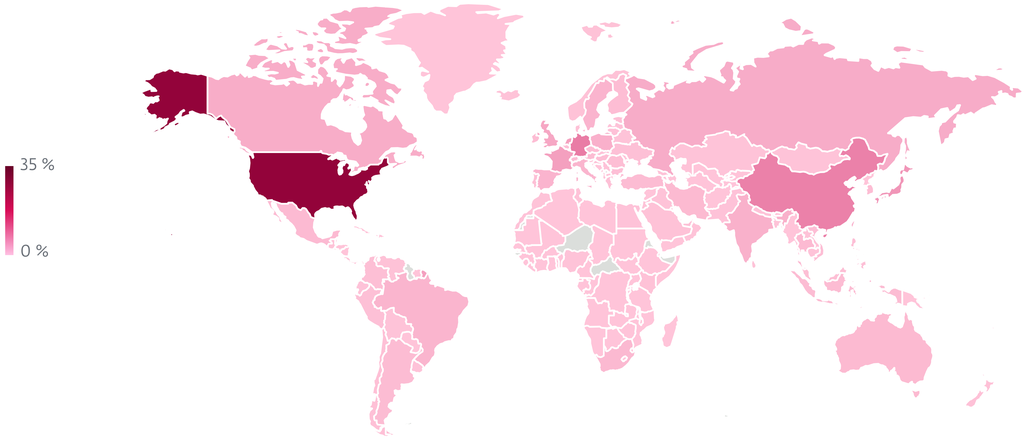
Tendance de détection des menaces Web au S2 2024 et S1 2025, moyenne mobile sur sept jours[2]



Répartition mondiale des blocages de menaces web au S1 2025



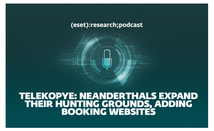
Tendance de blocage d'URL uniques au S2 2024 et S1 2025, moyenne mobile sur sept jours[2]



Répartition mondiale de l'hébergement de domaines bloqués au S1 2025

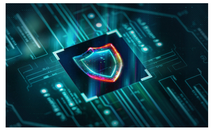
[2] La forte baisse du nombre de détections entre fin juin et début juillet 2024 a été causée par un problème de courte durée dans les connexions à nos bases de données statistiques ; cela n'a pas eu d'impact sur la protection contre les menaces.

Recherches



Podcast ESET Research : encore Telekopye

Jetez un œil sur le monde obscur de la cybercriminalité où des groupes d'escrocs surnommés « Néandertaliens » utilisent la boîte à outils Telekopye pour piéger des victimes sans méfiance qu'ils appellent des « Mammouths »



Enquête sur l'UEFI Secure Boot : présentation de CVE-2024-7344

Description d'une application UEFI signée permettant de contourner la protection UEFI Secure Boot

PlushDaemon compromet la chaîne d'approvisionnement d'un service de VPN coréen

Les chercheurs d'ESET ont découvert une attaque contre la chaîne d'approvisionnement d'un fournisseur de VPN en Corée du Sud par un nouveau groupe APT sponsorisés par la Chine que nous avons baptisé PlushDaemon

DeceptiveDevelopment cible les développeurs indépendants

Les chercheurs d'ESET ont analysé une campagne diffusant des malwares accompagnés de défis à relever lors d'entretiens d'embauche

Danabot : analyse d'un empire déchu

ESET Research partage ses conclusions sur le fonctionnement de Danabot, un infostealer récemment neutralisé dans le cadre d'une opération de police multinationale

Remue-ménage chez les infostealers, Nomani et nouveau vecteur d'attaques mobiles

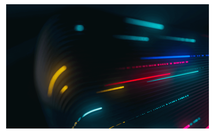
Des changements importants dans le paysage des infostealers, un nouveau vecteur d'attaques contre iOS et Android, et une augmentation massive des escroqueries à l'investissement sur les médias sociaux

Operation AkaiRyū : MirrorFace invite l'Europe à l'Expo 2025 et relance la porte dérobée ANEL

Les chercheurs d'ESET ont découvert une activité de MirrorFace qui s'est étendue au-delà de son intérêt habituel pour le Japon pour cibler un institut diplomatique d'Europe centrale avec la porte dérobée ANEL

Operation FishMedley

Les chercheurs d'ESET décrivent une opération d'espionnage mondiale menée par FishMonger, le groupe APT affilié à I-SOON



Vous vous souviendrez du jour où vous avez enfin attrapé FamousSparrow

Les chercheurs d'ESET découvrent l'ensemble des outils utilisés par le groupe APT FamousSparrow, y compris deux versions non documentées de SparrowDoor, la porte dérobée caractéristique du groupe

BladedFeline chuchote dans l'obscurité

Les chercheurs d'ESET ont analysé une campagne de cyberespionnage menée par BladedFeline, un groupe APT sponsorisé par l'Iran et probablement lié à OilRig

Mouvements chez RansomHub

Les chercheurs d'ESET découvrent de nouveaux liens entre les affiliés de RansomHub et les gangs rivaux Medusa, BianLian et Play

TheWizards usurpe SLAAC pour mener des attaques de type « adversary-in-the-middle »

Les chercheurs d'ESET ont analysé Spellbinder, un outil de déplacement latéral utilisé pour réaliser des attaques de type « adversary-in-the-middle »

Operation RoundPress

Les chercheurs d'ESET découvrent une opération d'espionnage menée par la Russie contre des serveurs de messagerie Web à l'aide de vulnérabilités XSS

ESET participe à une opération mondiale de perturbation des activités de Lumma Stealer

Notre surveillance intensive de dizaines de milliers d'échantillons malveillants a contribué à cette opération mondiale

Rapport général sur les menaces du S2 2024

Une présentation du paysage des menaces au S2 2024 telle que perçue par la télémétrie d'ESET et du point de vue des experts en détection des menaces et en recherche d'ESET

Rapport général sur les menaces de Q4 2024 – Q1 2025

Un aperçu des activités de certains groupes APT analysés par ESET Research au cours de Q4 2024 et de Q1 2025

Crédits

Équipe

Peter Stančík, Team Lead
Klára Kobáková, Managing Editor

Aryeh Goretsky
Branislav Ondrášik
Bruce P. Burrell
Hana Matušková
Nick FitzGerald
Ondrej Kubovič
Rene Holt
Zuzana Pardubská

Contributeurs

Dušan Lacika
Jakub Kaloč
Jakub Souček
Jakub Tomanek
Lukáš Štefanko
Tomáš Procházka

À propos des données de ce rapport

Les statistiques et les tendances des menaces présentées dans ce rapport reposent sur les données de télémétrie mondiales d'ESET. Sauf indication contraire, les données incluent les détections quelle que soit la plateforme ciblée.

Elles excluent les détections d'applications potentiellement indésirables, d'applications potentiellement dangereuses et les adwares, sauf dans les sections plus détaillées spécifiques à des plateformes, et dans la section sur les extracteurs de cryptomonnaie.

Ces données ont pour objectif d'être le plus impartiales possible et de maximiser l'intérêt des informations fournies.

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

À propos d'ESET

ESET, entreprise européenne de cybersécurité reconnue mondialement, se positionne comme un acteur majeur dans la protection numérique grâce à une approche technologique innovante et complète. Fondée en Europe et disposant de bureaux internationaux, ESET combine la puissance de l'intelligence artificielle et l'expertise humaine pour développer des solutions de sécurité avancées, capables de prévenir et contrer efficacement les cybermenaces émergentes, connues et inconnues.

Ses technologies, entièrement conçues dans l'UE, couvrent la protection des terminaux, du cloud et des systèmes mobiles, et se distinguent par leur robustesse, leur efficacité et leur facilité d'utilisation, offrant ainsi une défense en temps réel 24/7 aux entreprises, infrastructures critiques et utilisateurs individuels.

Grâce à ses centres de recherche et développement et son réseau mondial de partenaires, ESET propose des solutions de cybersécurité intégrant un chiffrement ultra-sécurisé, une authentification multifactorielle et des renseignements approfondis sur les menaces, s'adaptant constamment à l'évolution rapide du paysage numérique.

Pour plus d'informations, consultez **www.eset.com/fr** et suivez-nous sur **LinkedIn**, **Facebook** et **Instagram**.

WeLiveSecurity.com/fr/

@ESETresearch

GitHub ESET

Rapports généraux sur les menaces et rapports sur les activités des APT

Digital Security
Progress. Protected.

(eset):research