Autoroute d'attaques

Une analyse approfondie du trafic DNS malveillant

Akamai

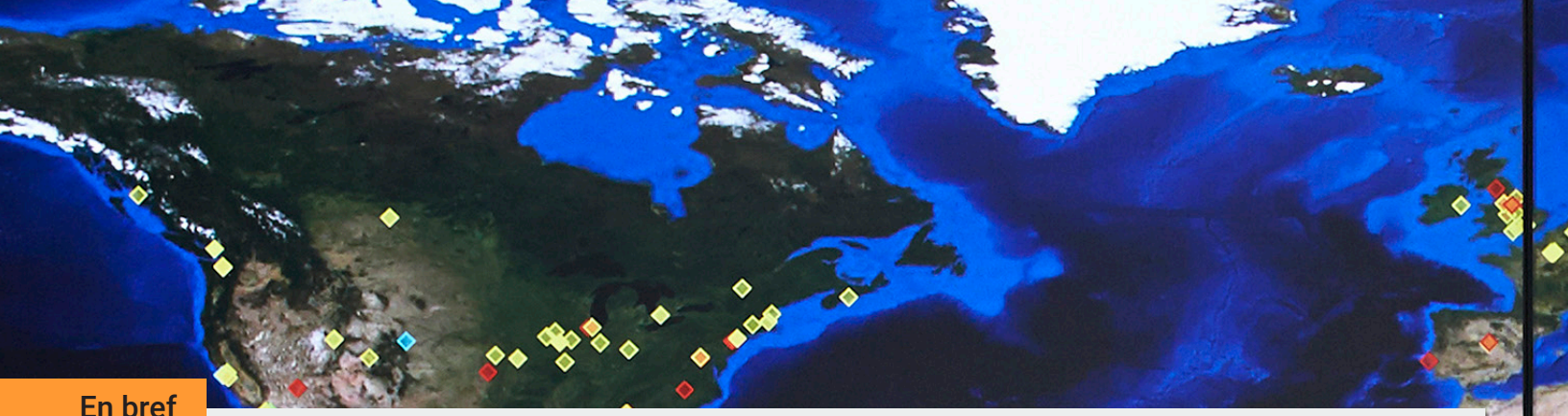
Table des matières

Serveurs de noms de domaine : une autoroute pour le trafic d'attaque

Le DNS (système de noms de domaine) est un élément essentiel de l'infrastructure Internet depuis ses débuts. Lorsque nous utilisons Internet, que ce soit à domicile ou au travail, la plupart de nos requêtes doivent être traitées par le DNS pour que nous puissions accéder à notre destination sur le Web. Sans surprise, les pirates choisissent souvent d'exploiter cette infrastructure pour mener leurs attaques, qu'il s'agisse d'une menace qui accède à des serveurs de commande et contrôle (C2) dans l'attente de commandes, ou de l'exécution de code à distance sur un domaine afin de télécharger des fichiers malveillants sur une machine. En raison de son omniprésence, le DNS est devenu un élément important de l'infrastructure d'attaque.

En tant que spécialiste de la sécurité informatique, Akamai bénéficie d'un point de vue unique qui lui permet d'observer les entreprises et les utilisateurs domestiques et de les protéger contre le trafic DNS malveillant qui pourrait compromettre le système et entraîner le vol d'informations. Ce rapport analyse en détail le trafic malveillant qui cible les particuliers et les entreprises dans le monde entier. En analysant le trafic DNS malveillant, ainsi que la corrélation avec les groupes d'attaque et leurs outils, les organisations peuvent obtenir des informations importantes sur les menaces les plus répandues dans leur environnement. Ces informations peuvent aider les professionnels de la sécurité à évaluer l'état de leurs défenses et à identifier leurs lacunes afin de contrer les techniques et les méthodes utilisées contre leur entreprise. S'ils ne le font pas, ils s'exposent à des violations pouvant entraîner la perte de données confidentielles, des pertes financières ou des sanctions pour non-conformité. Alors que le coût de la cybercriminalité devrait atteindre un montant record de l'ordre de 10 500 milliards de dollars par an d'ici 2025, les organisations doivent se préparer en amont pour empêcher les attaques.

En analysant le trafic DNS malveillant des entreprises et des particuliers, nous avons pu détecter plusieurs campagnes d'attaques, comme FluBot, un logiciel malveillant Android qui s'est propagé d'un pays à l'autre dans le monde entier, ainsi que la prédominance de divers groupes d'attaque qui ciblent les entreprises. Le meilleur exemple est peut-être la présence significative du trafic C2 lié aux courtiers d'accès initial (IAB), qui pénètrent les réseaux d'entreprise et monétisent leur accès en le vendant à d'autres cybercriminels, par exemple à des groupes de ransomware-as-a-service (RaaS). Nous observons ces activités sur l'autoroute de l'information qu'est le DNS et les partageons pour le bénéfice de nos lecteurs.



En bref

Selon nos données, entre 10 % et 16 % des entreprises ont connu un trafic C2 sur leur réseau au cours d'un trimestre donné. La présence d'un trafic C2 indique la possibilité d'une attaque en cours ou d'une violation, les menaces allant des botnets chargés de voler des informations aux IAB.

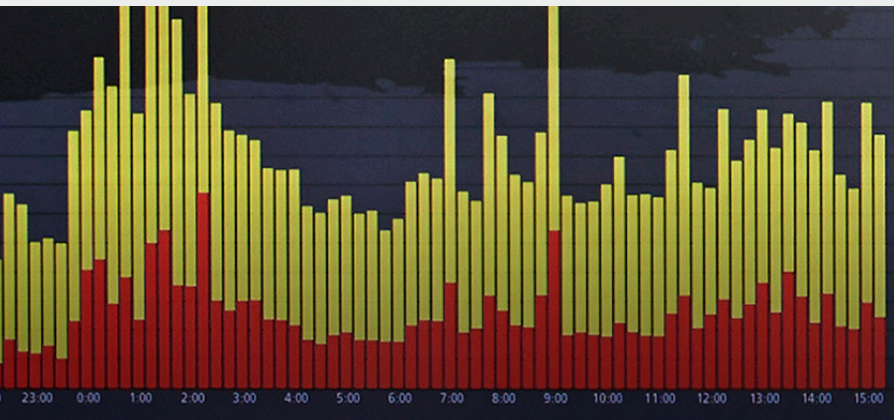
Quelque 26 % des terminaux infectés ont été atteints par des domaines de C2, notamment des domaines Emotet et QakBot, via un IAB identifié. Les IAB présentent un risque important pour les organisations, car leur rôle principal est de créer une violation initiale et de vendre l'accès aux groupes de ransomware et à d'autres groupes d'attaque.

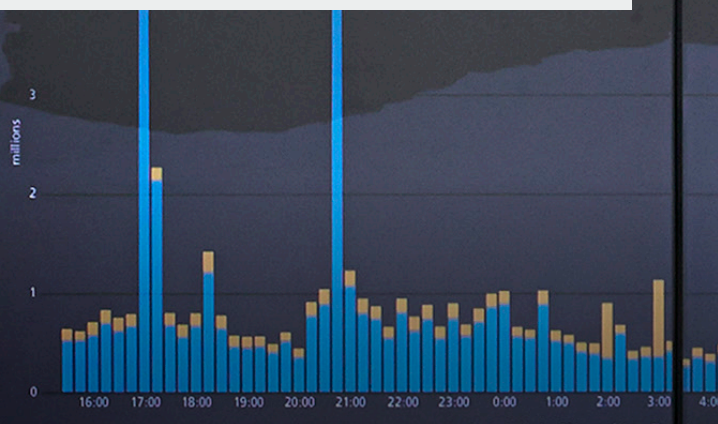
Les terminaux NAS (stockage en réseau) constituent des cibles idéales, car ils sont moins susceptibles de recevoir des correctifs et contiennent de nombreuses données précieuses. Nos données montrent que les attaquants exploitent ces terminaux par le biais de QSnatch : 36 % des terminaux affectés dans des réseaux d'entreprise atteints par des domaines de C2 étaient liés à cette menace.

Au total, 30 % des entreprises concernées font partie du secteur industriel, soit deux fois plus que le deuxième plus grand segment de marché, ce qui met en évidence les répercussions concrètes des cyberattaques, telles que des problèmes et des perturbations de la chaîne d'approvisionnement au quotidien. Des réglementations telles que la directive européenne sur la sécurité des réseaux et des systèmes d'information 2 (SRI 2) pourraient aider à limiter les attaques contre les secteurs essentiels ou les infrastructures stratégiques tels que le secteur industriel.

Les attaques contre les réseaux domestiques ciblent non seulement les terminaux traditionnels comme les ordinateurs, mais aussi les téléphones mobiles et l'Internet des objets (IoT). Une part importante de trafic d'attaque est liée aux logiciels malveillants mobiles et aux botnets IoT.

Grâce à notre analyse des données DNS, nous avons constaté une explosion du logiciel malveillant FluBot en Europe, au Moyen-Orient et en Afrique (EMEA), en Amérique latine (LATAM) et dans la région Asie-Pacifique/Japon (APJ). Les techniques d'ingénierie sociale de ce programme malveillant et son utilisation de plusieurs langues de l'Union européenne (UE) sont quelques-uns des facteurs qui ont contribué à la flambée de l'infection.





Terminologie de l'analyse du trafic DNS d'Akamai

Edge DNS et l'infrastructure DNS d'Akamai observent jusqu'à 7 000 milliards de requêtes DNS par jour. Pour protéger ses utilisateurs professionnels et les particuliers, Akamai bloque les demandes qui redirigent les terminaux vers des domaines diffusant des logiciels malveillants ou vers des sites susceptibles de dérober des informations. L'examen de ces transactions DNS malveillantes nous permet également de classer ces domaines en trois catégories (logiciels malveillants, sites d'hameçonnage et C2), et de réaliser une analyse approfondie visant à déterminer les menaces actuelles les plus importantes pour les entreprises et les utilisateurs domestiques.

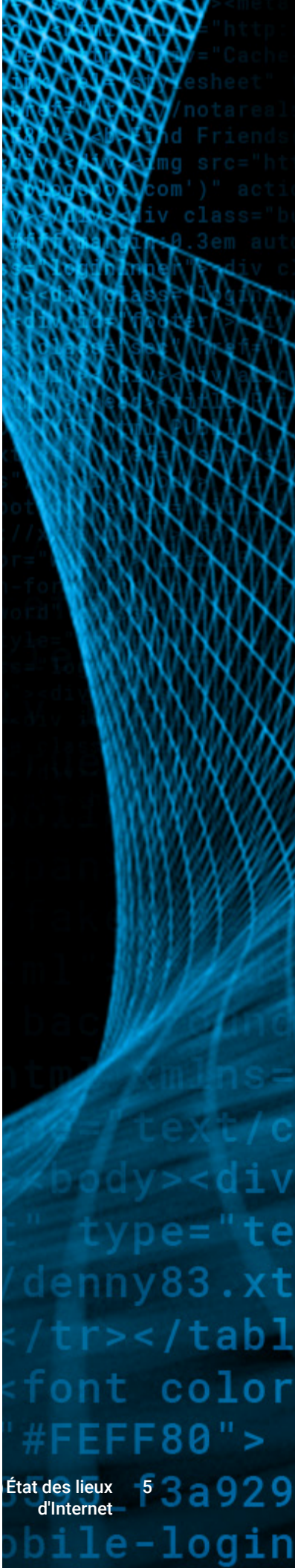
Un minutieux échantillonnage des données du trafic DNS malveillant nous permet de tirer des conclusions pertinentes sur les menaces les plus répandues. Notre protection couvre deux populations : d'un côté, les entreprises dont Akamai sécurise les réseaux et de l'autre, les utilisateurs domestiques qui accèdent à Internet sur leur réseau personnel et sont exposés à des menaces telles que la prise de contrôle des terminaux par des botnets à des fins malveillantes, par exemple pour gagner de l'argent grâce au minage de cryptomonnaie.

Dans un premier temps, nous allons définir les termes *sites d'hameçonnage*, *logiciel malveillant* et *C2*, et expliquer comment nous les utilisons dans ce rapport.

Un site d'hameçonnage est un domaine lié à un kit d'hameçonnage qui imite l'identité visuelle d'entreprises de commerces de détail, de banques, de sociétés de haute technologie ou d'autres entités pour inciter les utilisateurs à divulguer des informations telles que des identifiants et des informations à caractère personnel. Akamai observe ce trafic via le DNS pour protéger les entreprises et les particuliers contre le vol d'identité et la perte d'informations.

Un logiciel malveillant désigne un ou plusieurs domaines malveillants qui diffusent ou contiennent des fichiers malveillants. Cette catégorie comprend également des sites qui hébergent du code JavaScript malveillant et des sites Web compromis qui diffusent des publicités indésirables ou redirigent les utilisateurs vers une page contenant ce genre de publicités. De nombreuses attaques actuelles nécessitent le téléchargement d'un fichier malveillant sur un terminal à partir d'une source externe pour leur charge utile initiale ou pour télécharger la phase suivante d'une attaque en cours. L'observation et le blocage de ce trafic peuvent contribuer à protéger une entreprise contre une infection initiale ou une attaque en cours.

Dans le contexte de l'analyse du trafic DNS, le **C2** est un domaine utilisé pour communiquer avec les terminaux infectés afin d'envoyer des commandes, puis de contrôler le terminal. Après la compromission initiale, les attaquants établissent des communications C2 entre le système infecté et un serveur qu'ils contrôlent pour envoyer des commandes supplémentaires (téléchargement et propagation d'autres programmes malveillants, exfiltration de données, arrêt et redémarrage du système, etc.) et continuer ainsi à compromettre la sécurité du système ou du réseau. La détection du trafic C2 est essentielle, car elle signale une attaque en cours qu'il est encore temps d'atténuer. En outre, le blocage de domaines associés aux serveurs C2 évite l'établissement de communications C2 et empêche le logiciel malveillant de télécharger d'autres instructions ou commandes, réduisant ainsi les risques d'exécution d'activités malveillantes sur votre réseau.



Danger à venir : l'omniprésence du trafic malveillant dans les organisations

D'après l'analyse du trafic DNS effectuée par Akamai, nous pouvons constater que 13 % des terminaux ont tenté de communiquer au moins une fois avec des domaines associés à des logiciels malveillants au cours du quatrième trimestre 2022 (figure 1). En outre, 6 % des terminaux ont communiqué avec des domaines liés à l'hameçonnage. Dans le domaine du C2, sur lequel nous allons nous concentrer dans ce rapport, nous avons observé une tendance à la hausse tout au long de l'année, avec une très légère baisse au cours du quatrième trimestre.

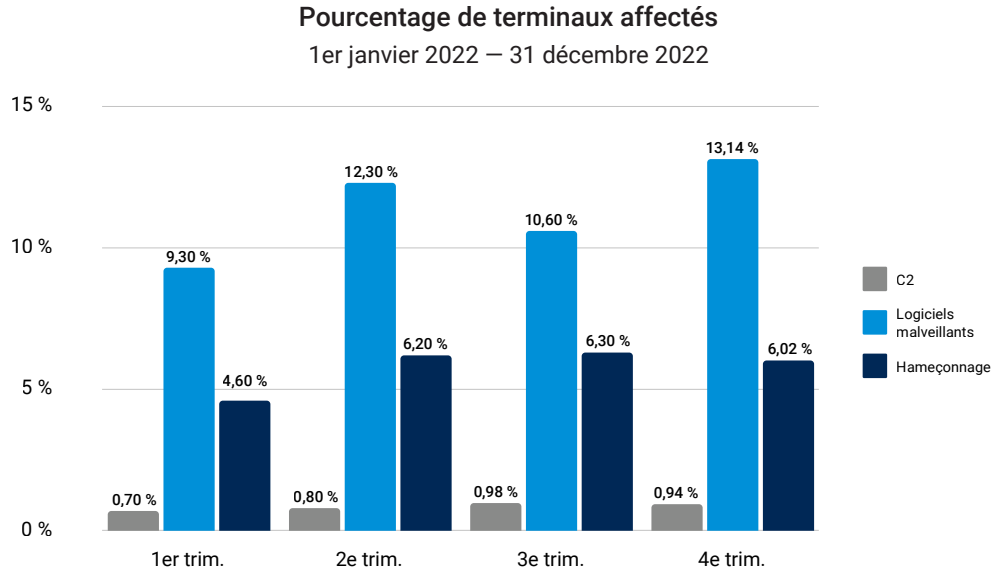


Figure 1 : de plus en plus de terminaux protégés atteignent des destinations malveillantes

Notez que la figure 1 fait uniquement référence à des terminaux individuels qui ont tenté de communiquer avec des domaines malveillants. Il est important de souligner la différence entre les terminaux qui communiquent avec des destinations malveillantes (qui peuvent être utilisés par les attaquants pour télécharger des programmes malveillants) et les terminaux qui communiquent avec des domaines de C2 (généralement utilisés pendant une attaque en cours pour faciliter la communication entre les attaquants et les programmes malveillants, et qui peuvent servir à télécharger des programmes malveillants supplémentaires afin de poursuivre un cycle d'attaques). Cette disparité peut indiquer qu'il existe des différences entre les tentatives d'infiltration du réseau, qui peuvent être bloquées lors de la première tentative de téléchargement de logiciels malveillants sur un appareil, et les infiltrations réussies (qui, dans nos données, ne sont peut-être pas passées par le DNS) ou les attaques en cours, qui peuvent communiquer avec un domaine de C2 pour exécuter l'attaque.

Ce rapport se concentre sur le trafic C2 comme indicateur potentiel d'une situation où un attaquant a réussi à s'infiltrer dans un terminal. Pour comprendre la prévalence de ces attaques, nous devons étudier les données sous un autre angle. Plutôt que d'observer les terminaux individuels, nous pouvons regrouper les données par organisation pour examiner à quelle fréquence une attaque en cours (indiquée par l'existence d'un trafic C2) apparaît dans l'ensemble de données.

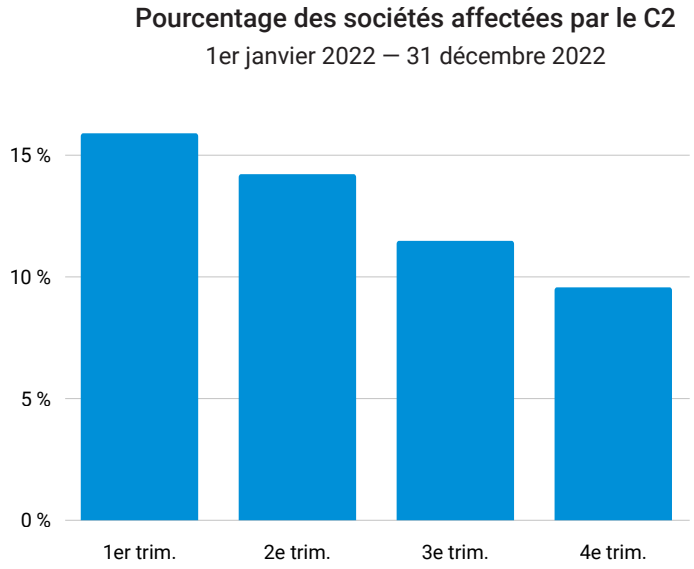


Figure 2 : une analyse du trafic C2 malveillant montre le pourcentage d'entreprises dont au moins un terminal a communiqué avec un domaine de C2 au cours de l'année

> **Selon nos données DNS, 10 % à 16 % des organisations ont connu au moins un cas de trafic C2 en dehors de leur réseau au cours d'un trimestre donné.**

Selon nos données DNS, entre 10 % à 16 % des organisations ont connu au moins un cas de trafic C2 en dehors de leur réseau, au cours d'un trimestre donné (figure 2). Cela peut indiquer que des programmes malveillants tentent de communiquer avec un opérateur et constitue un signe potentiel de violation. Ce trafic C2 a été bloqué par notre solution, mais des attaques réussies pourraient avoir entraîné l'exfiltration de données, des attaques par ransomware et plus encore. Au premier semestre 2022, 2,3 milliards de souches de logiciels malveillants ont été détectées, avec une moyenne de 1 501 par jour. Notre étude met en évidence l'efficacité de l'utilisation du DNS pour empêcher les programmes malveillants de progresser sur un réseau ou de causer des dommages.

Les courtiers d'accès initial représentent une menace importante pour les organisations

Les attaques en plusieurs étapes sont désormais incontournables dans l'écosystème actuel (figure 3). Les attaquants réussissent mieux lorsqu'ils sont capables de travailler ensemble (ou de s'embaucher), ou lorsqu'ils peuvent combiner différents outils en une seule attaque. Le C2 est essentiel dans le succès de ces attaques. Elles peuvent être utilisées non seulement pour la communication, mais également pour faciliter le téléchargement d'une charge utile et du programme malveillant pour la prochaine étape afin de faire avancer l'attaque. La chaîne d'attaques par ransomware Emotet/TrickBot/Ryuk observée ces dernières années illustre parfaitement cet exemple. Emotet infiltre tout d'abord le réseau de la victime, puis, une fois l'accès initial établi, communique avec un domaine pour télécharger la charge utile de TrickBot afin d'obtenir des données personnelles, des informations d'identification, etc. Si la victime est considérée comme une cible de grande valeur pour les attaquants, le programme malveillant communique avec ses serveurs C2 et télécharge la charge utile finale : le ransomware Ryuk.

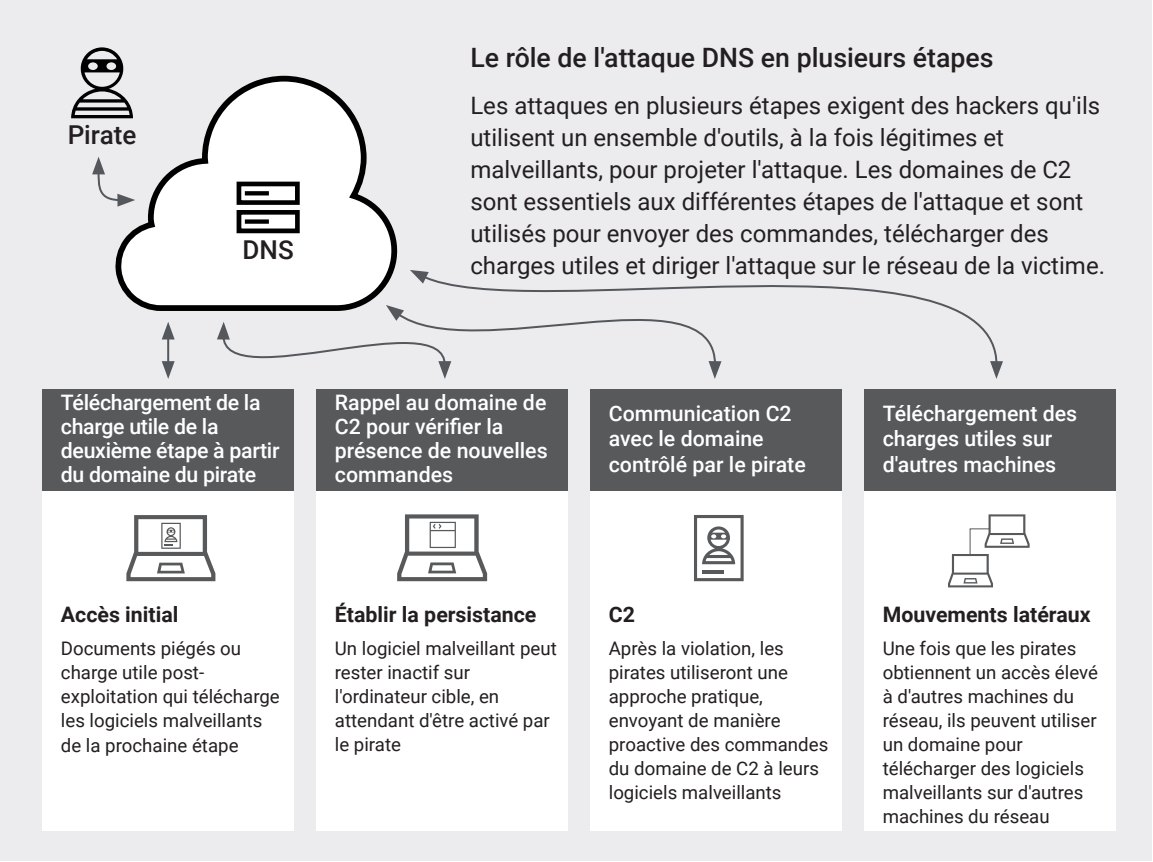


Figure 3 : le rôle du C2 dans chaque étape de l'attaque

Il est important de tenir compte de cette chaîne d'événements lors de l'évaluation des informations de ce rapport. La communication C2 peut se produire à différents stades de l'attaque. Notre analyse récente des méthodes utilisées par les groupes de ransomware actuels, par exemple le groupe Conti, a montré que les pirates sophistiqués confiaient souvent des tâches manuelles aux opérateurs pour faire avancer rapidement et efficacement une attaque. La capacité à visualiser et bloquer le trafic C2 est essentielle pour stopper une attaque en cours.

Les domaines de C2 que nous avons observés peuvent être classés en domaines attribuables ou non à une famille de menaces/un groupe d'attaque spécifique. Dans cette section, nous nous pencherons sur les domaines de C2 associés à un type de menace et aiderons les lecteurs à évaluer le niveau de risque en fonction des capacités et des méthodes de chaque groupe. Notez que certaines de ces familles de logiciels malveillants peuvent correspondre à plusieurs cas d'utilisation, selon la façon dont les pirates les utilisent pendant une attaque.

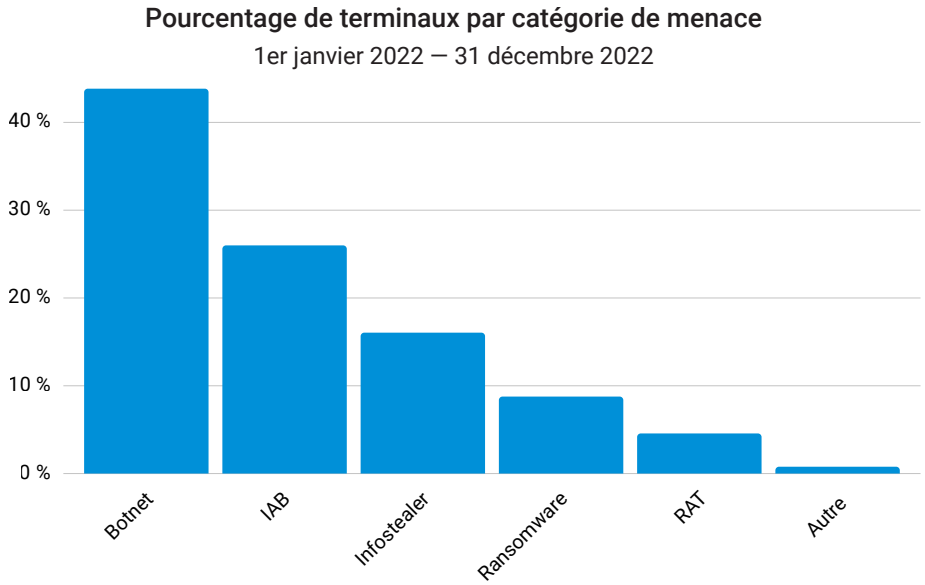


Figure 4 : les entreprises sont principalement ciblées par les botnets, suivis des IAB et des infostealers

Dans la figure 4, les groupes d'attaque sont classés en IAB, botnets et RaaS. Nos données révèlent que les IAB représentent l'une des principales menaces pour les réseaux d'entreprise, tout comme les botnets destinés à l'exfiltration de données.

Courtiers d'accès initial
Les courtiers d'accès initial (IAB) cherchent avant tout à offrir un point d'entrée initial à d'autres cybercriminels, notamment des groupes de ransomware, pour pénétrer dans les réseaux des entreprises. persistance, exécution à distance de la charge utile après l'intrusion et exfiltration de données.

Groupes de ransomware-as-a-service
Ces groupes permettent à d'autres pirates (y compris ceux qui ne disposent pas de l'expertise technique nécessaire) de devenir des affiliés et d'utiliser leur ransomware moyennant un paiement.

Botnets
Les pirates utilisent les botnets à des fins multiples : minage de cryptomonnaie, attaques DDoS, exfiltration de données, déploiement de programmes malveillants, mouvements latéraux, etc.

Infostealers
Les infostealers collectent divers types de données : noms d'utilisateur, mots de passe, informations système, identifiants bancaires, cookies, etc.

Nous observons également des ransomwares, des outils d'accès à distance (RAT) et des infostealers. Tous ont un rôle important à jouer dans les différentes étapes de l'attaque. Et grâce aux outils disponibles sur les marchés clandestins pour les cybercriminels novices et expérimentés qui leur permettent d'entrer et de rester cachés dans le réseau, et de poursuivre l'attaque, les entreprises sont plus que jamais exposées à la cybercriminalité. À mesure que nous étudions ces groupes, nous établissons également les intersections où ils opèrent ainsi que les répercussions et les impacts potentiels sur les organisations.

Groupes de courtiers d'accès initial

Les courtiers d'accès initial (IAB) sont un type de cybercriminels qui se consacrent principalement à fournir un point d'entrée initial à d'autres cybercriminels et attaquants pour qu'ils puissent pénétrer dans les réseaux des entreprises. Bien que plusieurs groupes de cybercriminels utilisent des méthodes de violation similaires (exploitation des vulnérabilités liées au VPN et au RDP, recours aux attaques en force, collecte d'identifiants compromis, envoi d'e-mails d'hameçonnage liés à des programmes malveillants, etc.), les IAB se spécialisent dans la pénétration de ces systèmes infectés et la vente de cet accès à d'autres groupes d'attaque plutôt que dans l'exécution de l'ensemble de l'attaque. Les groupes de ransomwares à l'origine de LockBit, Darkside, Conti et BlackByte, entre autres, auraient eu recours à des IAB dans le cadre de leurs activités. Une étude de 2023 a révélé que le prix de vente moyen d'un accès initial s'élevait à environ 2 800 dollars américains.

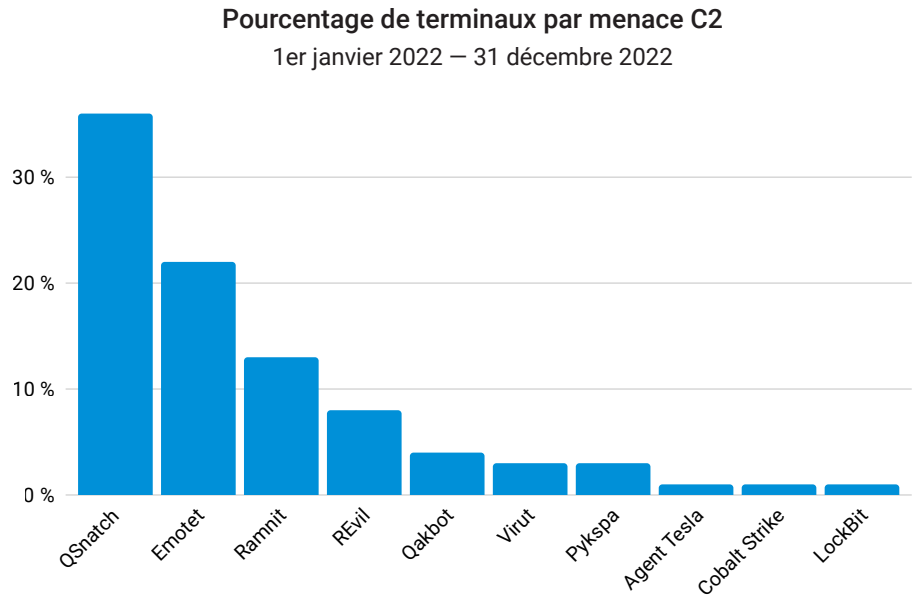
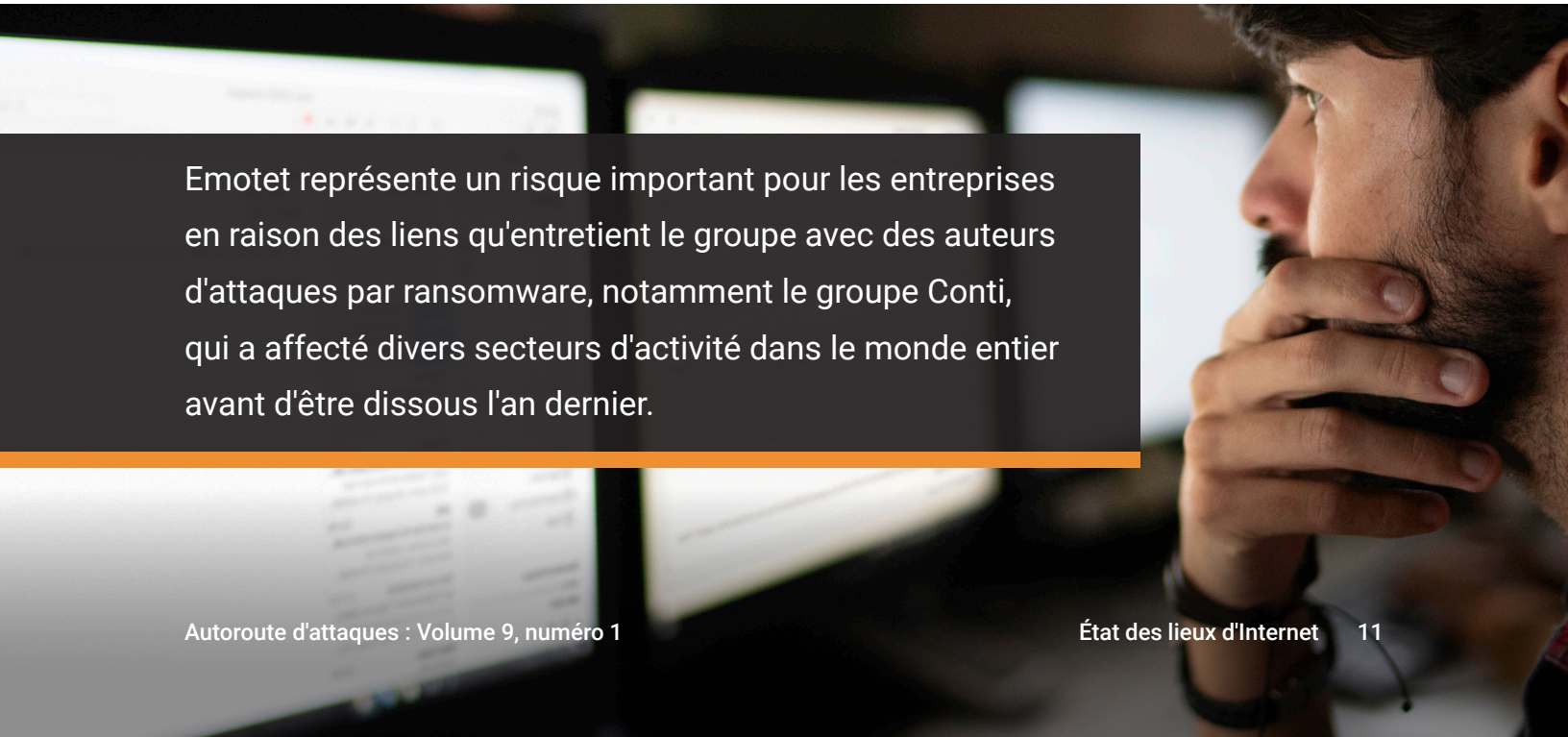


Figure 5 : QSnatch, Emotet et Ramnit sont les principales familles de C2 observées dans le trafic réseau des entreprises

D'après nos données DNS (figure 5), 26 % des terminaux infectés ont été atteints par des domaines liés à des IAB, par exemple Qakbot (4 % des terminaux infectés) et Emotet (22 % des terminaux infectés). Les IAB jouent un rôle important dans le modèle économique des RaaS et dans l'écosystème de la cybercriminalité. Les cybercriminels qui ont recours aux ransomwares ont besoin d'un accès à distance et d'informations d'identification, non seulement pour infiltrer les réseaux de leurs victimes, mais également pour s'y déplacer latéralement, établir la persistance, obtenir des droits d'accès, etc. Ils utilisent les IAB pour effectuer les tâches chronophages de reconnaissance, d'analyse des cibles potentielles et d'infection initiale. La disponibilité immédiate d'accès sur le marché clandestin élimine cette étape et réduit le niveau d'expertise ainsi que le temps nécessaires pour lancer une attaque. Elle permet une multitude d'attaques potentielles contre les organisations cibles visées, qui se traduisent par des demandes de rançons, des vols d'informations confidentielles et sensibles, des actes d'espionnage et des violations de données.

Emotet apparaît comme l'un des IAB les plus importants dans nos données. Emotet représente un risque important pour les organisations en raison des liens du groupe avec des auteurs d'attaques par ransomware, notamment le groupe Conti, qui a affecté divers secteurs d'activité dans le monde entier avant d'être dissous l'an dernier. Au fil des ans, Emotet a ajouté de nouveaux modules d'attaque par déni de service distribué (DDoS) ou de vol d'e-mails, et a étendu ses cibles visées. Emotet, qui était à l'origine un cheval de Troie/botnet bancaire offrant une multitude de fonctionnalités, est devenu un malware-as-a-service (MaaS) distribuant des menaces telles que le cheval de Troie bancaire IcedID, TrickBot et le ransomware UmbreCrypt. Il semble également que le groupe TrickBot utilise Emotet pour distribuer plusieurs souches de ransomware, notamment Ryuk, ProLock et Conti. Le cadre MITRE ATT&CK propose un aperçu plus détaillé des techniques utilisées par Emotet.



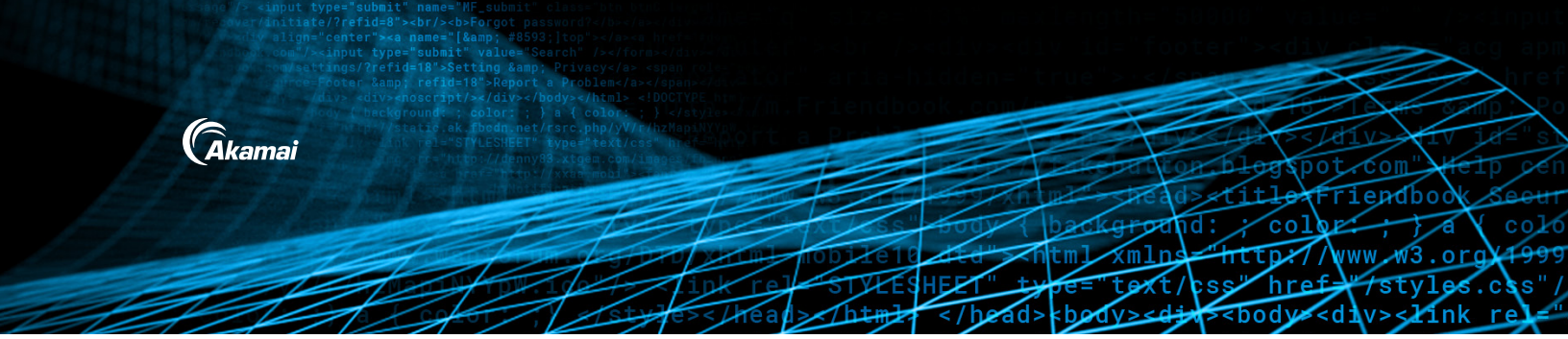
Emotet représente un risque important pour les entreprises en raison des liens qu'entretient le groupe avec des auteurs d'attaques par ransomware, notamment le groupe Conti, qui a affecté divers secteurs d'activité dans le monde entier avant d'être dissous l'an dernier.

Le deuxième IAB le plus important observé dans les données est Qakbot. Ce groupe est connu pour avoir collaboré avec le groupe de ransomware Black Basta, qui aurait affecté au moins 50 organisations de diverses régions du monde. L'équipe de Qakbot est réputée pour ses capacités de vol d'informations et pour disséminer des programmes malveillants de deuxième étape servant à compromettre davantage la sécurité du système. Selon des études, Qakbot utilise Cobalt Strike, un outil légitime de test de pénétration utilisé par les équipes rouges et usurpé par leurs adversaires, pour réaliser toutes sortes d'activités malveillantes après l'intrusion et pour faciliter l'accès à l'environnement de la victime par une porte dérobée. Il s'agit d'une technique de plus en plus utilisée par les IAB ces dernières années. Le cadre MITRE ATT&CK fournit des informations supplémentaires sur les techniques utilisées par Qakbot pendant son attaque.

Groupes de botnets

Dans notre analyse, les botnets représentent le plus grand groupe de types de menaces, soit 44 % du trafic C2 analysé. Toutes sortes d'attaquants sont représentés dans ce groupe, et il faut garder à l'esprit que tous les botnets ne sont pas identiques. Les variantes les plus inoffensives implantent des mineurs de cryptomonnaie ou exploitent la machine de la victime pour mener des attaques DDoS. Bien que ces menaces représentent un coût en soi, les botnets que nous avons détectés dans les entreprises peuvent être utilisés pour exfiltrer des données et lancer des attaques en plusieurs étapes, ce qui présente un risque plus important. Les botnets peuvent se propager latéralement dans le réseau et servir à déployer des ransomwares, comme c'est le cas de TrickBot. Ils peuvent aussi se spécialiser dans le vol d'informations et la collecte d'identifiants.

C'est précisément ce que fait QSMatch, le plus grand botnet présent dans les environnements d'entreprise : exfiltrer des données de terminaux connectés au réseau. D'après nos données, QSMatch représentait 36 % des terminaux infectés. Ce programme malveillant cible spécifiquement QNAP, un type de terminal NAS utilisé par les entreprises pour sauvegarder ou stocker des fichiers. Bien que la méthode d'infection soit encore inconnue, les chercheurs supposent que QSnatch infecte les terminaux en exploitant les vulnérabilités des micrologiciels ou en lançant des attaques en force contre des terminaux utilisant un nom d'utilisateur/mot de passe par défaut. Les entreprises utilisant QNAP doivent donc veiller à maintenir leur micrologiciel à jour (une fois infecté, QSnatch empêcherait l'installation de correctifs et désactiverait les solutions de sécurité) et à modifier immédiatement les mots de passe par défaut. Les attaquants utilisent QSnatch à diverses fins : extraction d'identifiants, enregistrement de mots de passe, accès à distance et exfiltration de données, pour n'en citer que quelques-unes. Les pirates peuvent cibler les terminaux de stockage, car ils contiennent des informations sensibles et leur infection empêche les entreprises de réaliser des sauvegardes en cas d'attaque par ransomware. Cette alerte CISA détaille les tactiques et les contre-mesures à mettre en œuvre.



Groupes de ransomware-as-a-service

Dans notre analyse du trafic DNS, 9 % des terminaux infectés qui ont communiqué avec des familles C2 ont accédé à des domaines associés à des groupes de RaaS. Ce type de groupe de cybercriminels permet à d'autres pirates (y compris ceux qui ne disposent pas de l'expertise technique nécessaire) de devenir l'un de leurs affiliés et d'utiliser leur ransomware moyennant un paiement. Les organisations affectées par des ransomwares sont exposées à d'innombrables conséquences, qui ne se limitent pas à la perte de données confidentielles. Elles sont potentiellement confrontées à des coûts de restauration, des frais juridiques, des amendes, des temps d'arrêt entraînant une perte de productivité et une atteinte à la marque et à la réputation. Cybersecurity Ventures estime que le coût des attaques par ransomware pourrait atteindre environ 265 milliards de dollars américains par an d'ici 2031. Le rapport Akamai sur les menaces par ransomware dans le monde met également en évidence les effets paralysants des ransomwares au-delà des pertes financières, notamment les perturbations de la chaîne d'approvisionnement, et le fait que, dans certains cas, les ransomwares peuvent tuer.

L'un des groupes de RaaS les plus actifs est le gang REvil, qui est devenu célèbre pour avoir ciblé un fournisseur de logiciels de gestion informatique lors d'une attaque de la chaîne d'approvisionnement qui a affecté plus de 1 500 fournisseurs de services gérés. L'arrestation de plusieurs membres du groupe par le gouvernement russe a permis de mettre un terme à leurs activités. Cependant, quelques mois après le démantèlement, des chercheurs en sécurité ont observé que le site de fuites de REvil était redevenu actif et publiait des informations sur ses dernières victimes en date, notamment des universités américaines. Les chercheurs ont avancé l'hypothèse que ce n'était peut-être pas le même gang REvil qui menait cette campagne et ont mis en garde contre des États-nations qui se feraient passer pour le groupe REvil afin de dissimuler leurs activités. En termes de tactique, REvil est connu pour personnaliser son flux d'attaque en fonction des victimes visées, ce qui démontre le niveau de connaissance que le groupe possède de ses cibles. Pour en savoir plus sur les tactiques, les techniques et les procédures liées à REvil, lisez cet article de MITRE.

> **Les pirates peuvent cibler les terminaux de stockage, car ils contiennent des informations sensibles et leur infection empêche les entreprises de réaliser des sauvegardes en cas d'attaque par ransomware.**

LockBit est un autre groupe de RaaS que nous avons découvert lors de notre analyse du trafic DNS. Après la « disparition » de Conti, le groupe LockBit est devenu l'un des fournisseurs de RaaS les plus actifs. Auparavant (de novembre 2019 à mars 2022), il s'agissait de l'opérateur de RaaS ayant ciblé le plus grand nombre d'organisations après Conti, comme l'explique ce rapport.

Le gang LockBit se targue de disposer d'un mécanisme de cryptage plus rapide que les autres groupes de RaaS et affirme avoir infecté plus de 12 000 entreprises avec son programme LockBit 2.0. En juin 2022, le groupe a publié LockBit 3.0, qui intègre des fonctionnalités supplémentaires, notamment un programme de recherche de bugs. Il aurait également exploité la vulnérabilité Log4j pour obtenir un accès initial à ses cibles, ce qui souligne l'importance d'appliquer des correctifs. Les organisations qui ne corrigent pas ce type de failles de sécurité risquent davantage d'être infectées par LockBit. LockBit continue de se réinventer : un ajout récent appelé tactique de triple extorsion consiste à crypter les fichiers, à les publier sur des sites de fuites et à lancer des attaques DDoS si les victimes refusent de payer la rançon.

Outils de travail

Les outils identifiés dans cette section jouent un rôle spécifique dans une attaque, que ce soit en accédant au système, en obtenant des informations ou en élevant les privilèges. L'arsenal observé chez divers groupes d'attaque exige souvent une communication pour fonctionner comme des infostealers et des outils d'accès à distance (RAT). En connaissant ces outils et les tactiques utilisées par les groupes d'attaques, les spécialistes de la sécurité peuvent comprendre le processus d'attaque et se préparer en conséquence.

Infostealers

Conçus pour obtenir différents types de données (noms d'utilisateur, mots de passe, informations système, informations d'identification bancaires, cookies, etc.), les infostealers demeurent l'une des offres de MaaS les plus fréquemment utilisées dans les attaques. Les pirates qui ne disposent pas des connaissances et/ou des compétences techniques nécessaires peuvent facilement acquérir des infostealers à un coût relativement faible et lancer leurs propres attaques.

Dans la liste des familles de programmes malveillants C2, nous avons observé que 16 % de terminaux ayant accédé à un domaine de C2 connu avaient communiqué avec des infostealers. Ramnit (13 % des terminaux infectés) n'est pas un infostealer de plus. Sa force réside dans sa grande modularité, qui permet aux pirates d'utiliser diverses fonctionnalités, telles que le vol d'autres données sensibles et le téléchargement/déploiement d'autres programmes malveillants, pour atteindre son objectif final ou poursuivre l'attaque. En 2021, Ramnit était considéré comme le cheval de Troie bancaire le plus utilisé et, selon des informations récentes, un autre logiciel malveillant présente un code similaire à celui de Ramnit.

La présence d'infostealers dans votre réseau est un signe indiquant que vos identifiants sont potentiellement en danger. Les informations dérobées peuvent être revendues sur des marchés clandestins et utilisées par d'autres pirates pour obtenir un accès initial. Les groupes de ransomware peuvent déployer un infostealer par le biais d'une attaque d'hameçonnage ou d'un botnet pour obtenir des informations d'identification valides, louer une licence d'accès à un infostealer sur un forum clandestin proposant des MaaS, ou acheter un accès réseau via des IAB. Dans certains cas, les opérateurs d'infostealers peuvent devenir des IAB et vendre des identifiants collectés de grande valeur (comme un accès VPN ou RDP) au plus offrant ou à d'autres acteurs malveillants qui peuvent lancer une attaque bien plus sophistiquée.

Outils d'accès à distance

Plusieurs groupes d'attaque ont exploité Cobalt Strike dans le cadre de leurs activités. Les pirates peuvent utiliser ce puissant RAT de différentes façons : reconnaissance, élévation des privilèges, mouvement latéral dans le réseau, établissement de connexions persistantes, exécution de charges utiles à distance après l'intrusion (comme des ransomwares) et exfiltration de données. Bien que cet outil soit principalement utilisé après une intrusion pour le mouvement latéral et l'exfiltration, il peut aussi être le vecteur d'accès initial, car il dispose d'un module d'hameçonnage ciblé. Les groupes connus pour avoir utilisé cet outil sont Conti, Qakbot, TrickBot et Emotet, pour n'en nommer que quelques-uns. Cet ensemble de règles YARA a été créé pour vérifier l'utilisation malveillante de l'outil et faciliter la détection de Cobalt Strike dans un environnement.

Nos données indiquent également la présence d'Agent Tesla dans le trafic C2. Ce RAT vendu sur le marché clandestin est un outil attrayant pour les cybercriminels en raison de son prix abordable et de sa simplicité d'utilisation. Les attaquants peuvent l'utiliser pour collecter les informations d'identification de différents navigateurs, réaliser des captures d'écran et enregistrer les touches du clavier. L'une de ses tactiques les plus notables est la récupération de formulaire, qui permet aux pirates de collecter des informations personnelles identifiables et d'autres informations sensibles. Ces informations dérobées peuvent ensuite être utilisées à des fins d'usurpation d'identité ou de fraude. PCrisk a publié des détails supplémentaires sur les techniques d'Agent Tesla et sur son impact sur les utilisateurs affectés.

Le paysage des activités montre des campagnes sporadiques de programmes malveillants tout au long de l'année

Sur une année, nous avons constaté des fluctuations dans les activités des programmes malveillants C2 (figure 6). Un exemple concret : Emotet s'est avéré particulièrement actif en janvier et février 2022, suite à sa résurgence en novembre 2021. Cette accélération de l'activité témoigne d'une campagne de grande envergure menée pour l'aider à regagner son statut après des mois d'inactivité. Dans les mois qui ont suivi son retour, Emotet a amélioré ses tactiques en incluant des moyens de contourner la décision de Microsoft de désactiver les macros Visual Basic for Applications. Certaines sources indiquent qu'Emotet est redevenu inactif entre juillet et novembre 2022 ; nos observations montrent une baisse du trafic C2 en juillet, comme en témoigne le pourcentage moins élevé de terminaux infectés communiquant avec des domaines Emotet. Cela peut indiquer que le groupe est resté actif tout au long de l'année, ou bien il peut s'agir d'un programme malveillant installé qui continue de communiquer avec une infrastructure obsolète. Les observations que nous réaliserons en 2023 pourront nous aider à déterminer si le groupe Emotet est réellement devenu inactif.

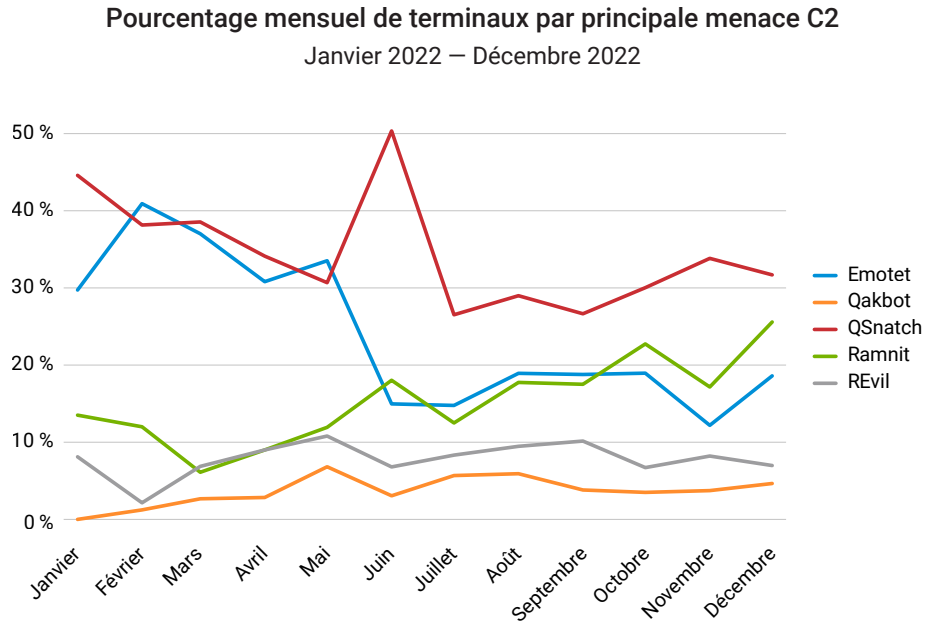


Figure 6 : le graphique d'évolution mensuelle montre que QSnatch a été actif tout au long de l'année 2022

> **Emotet a été particulièrement actif au mois de janvier et février 2022, après sa résurgence en novembre 2021. Cette accélération de l'activité témoigne d'une campagne de grande envergure menée pour l'aider à regagner son statut après des mois d'inactivité.**

QSnatch est resté actif tout au long de l'année, avec un pic autour du mois de juin, ce qui montre l'omniprésence de cette menace. Il existe plusieurs raisons pour lesquelles les serveurs NAS sont des cibles de choix pour les pirates : tout d'abord, ils contiennent des données sensibles ; deuxièmement, il y a moins de risques que les serveurs NAS reçoivent des correctifs ; troisièmement, ces terminaux sont potentiellement plus accessibles dans le réseau d'une organisation et peuvent servir de base pour des mouvements latéraux. Bien que des améliorations aient été apportées ces dernières années, notamment grâce aux solutions de sécurité intégrées, les cybercriminels les ont contournées en désactivant les produits de sécurité installés et/ou en empêchant la mise à jour des terminaux avec de nouveaux correctifs. Ces terminaux restent donc vulnérables contre les nouvelles souches de ce programme malveillant.

Nous avons également constaté une augmentation de la présence de Ramnit dans les réseaux d'entreprise entre août et décembre, ce qui est inquiétant, car ce programme malveillant peut dérober un large éventail d'informations sensibles que les pirates peuvent ensuite revendre à d'autres acteurs malveillants pour de futures attaques.

QSnatch et Emotet : des menaces communes à toutes les régions

Afin de déterminer les menaces prédominantes par région, nous avons examiné le pourcentage de terminaux qui communiquent avec des domaines de C2 dans chaque région (figure 7). Chaque pourcentage est lié au nombre de terminaux affectés par région, qui varie également d'une région à l'autre. Il est intéressant de noter que nous constatons des tendances similaires dans toutes les régions, avec très peu de valeurs aberrantes. Nous recommandons donc à chaque région de suivre les recommandations indiquées dans la section « Conclusion et recommandations » ou dans les sections précédentes, où sont présentés tous les groupes de programmes malveillants.

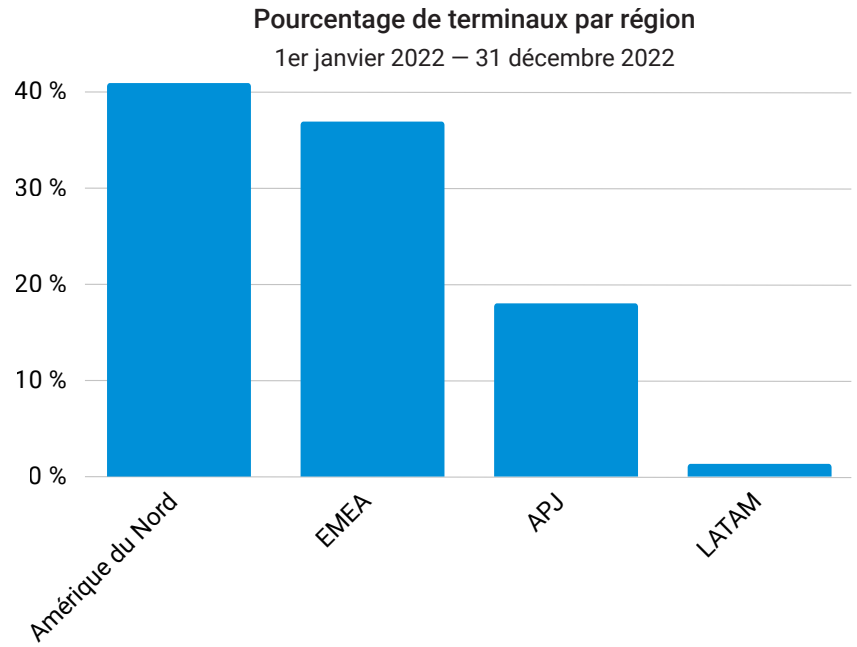


Figure 7 : l'Amérique du Nord (41 %) arrive en tête du nombre de terminaux affectés par région, suivie de la zone EMEA (37 %) et de la région APJ (18 %)

Amérique du Nord

La majorité des organisations du monde entier ont été victimes de ces deux principales menaces : QSnatch et Emotet. En Amérique du Nord, environ 29 % des terminaux affectés dans la région ont été touchés par Emotet, tandis que 33 % ont été touchés par QSnatch (figure 8). Selon un rapport de Dark Reading, une recherche sur Shodan a montré que 300 000 terminaux QNAP étaient connectés à Internet, ce qui en fait une cible attrayante. En outre, les terminaux NAS tels que QNAP peuvent servir de sauvegardes et de serveurs de fichiers ou multimédias.

Ramnit, Qakbot et REvil constituent d'autres menaces majeures en Amérique du Nord, ce qui est intéressant quand on sait que les IAB comme Emotet ont ouvert la voie à d'autres infections, y compris (mais pas seulement) aux ransomwares.

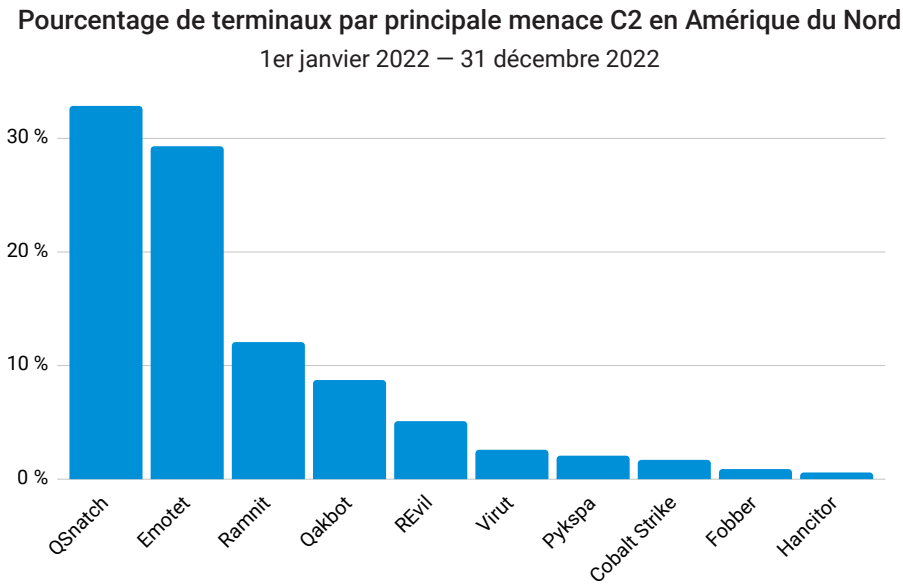
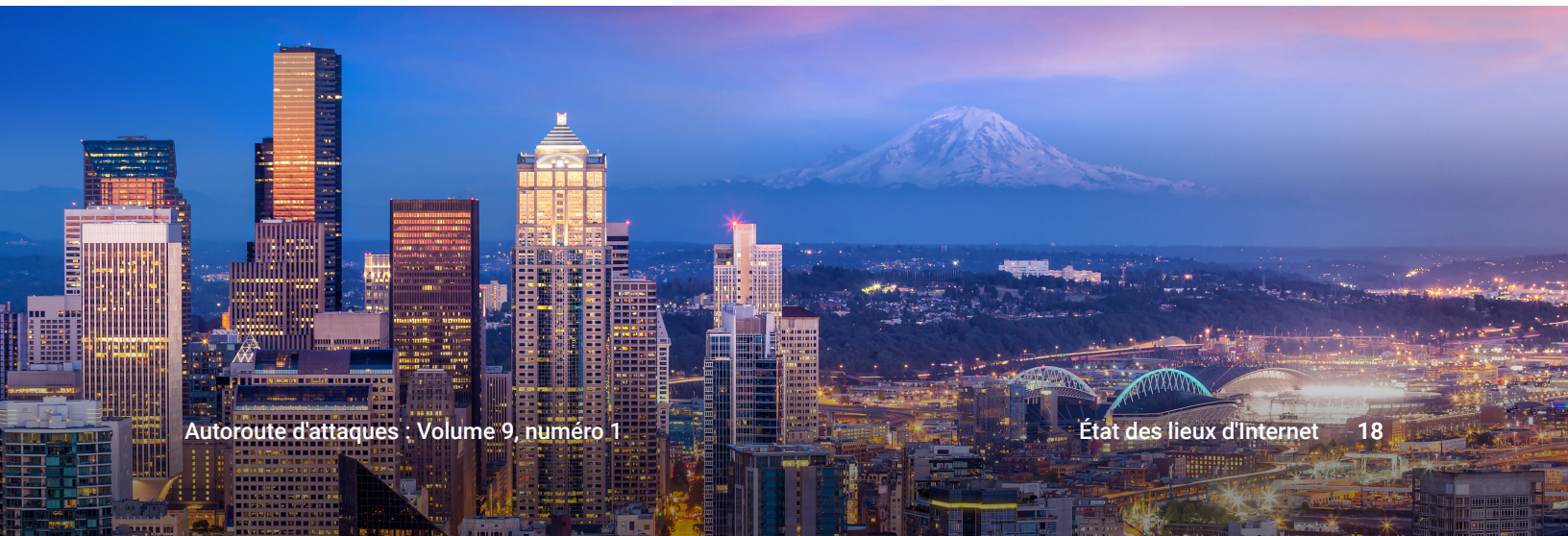


Figure 8 : la majorité des terminaux affectés dans les organisations nord-américaines ont accédé au moins une fois à des domaines liés à QSnatch, Emotet et Ramnit



Europe, Moyen-Orient et Afrique

La zone EMEA affiche le pourcentage le plus élevé de terminaux affectés, juste après l'Amérique du Nord. Les principales menaces observées dans la région (figure 9) incluent QSnatch (28 %) et Ramnit (21 %). Il n'est pas surprenant de constater la progression de Ramnit dans la région étant donné que, par le passé, ses opérateurs ont ciblé des établissements bancaires/financiers en Italie, au Royaume-Uni et en France. Dans l'une de ses itérations, la configuration de Ramnit a inclus des pays de l'UE comme principaux objectifs. De fait, si l'on compare le nombre de terminaux affectés par Ramnit dans le monde, la région EMEA reste la première cible des infections par Ramnit. Le pourcentage de terminaux infectés par Emotet était également élevé dans la région (19 %).

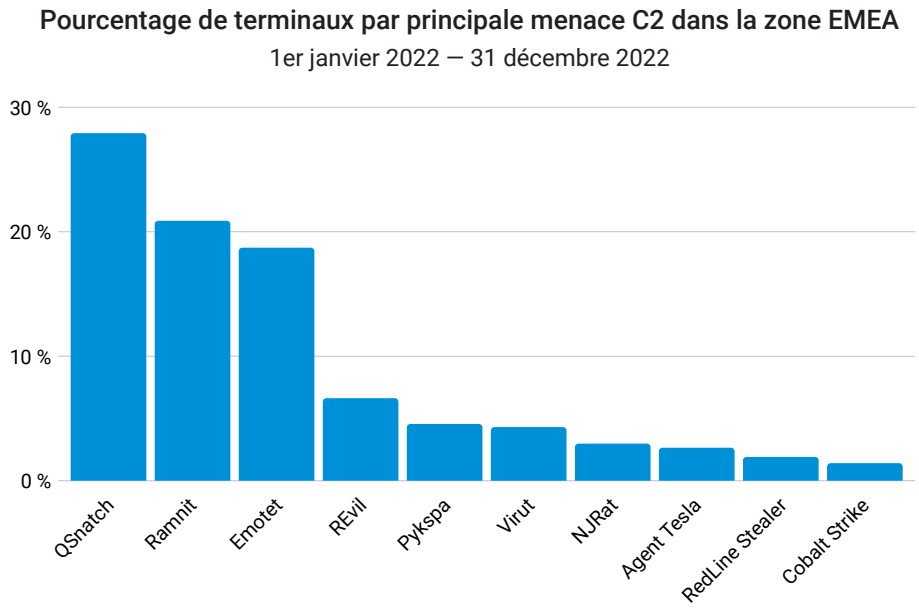


Figure 9 : davantage de terminaux ont accédé au C2 Ramnit dans la zone EMEA que dans d'autres régions, ce qui augmente considérablement les risques pour les entreprises de cette région

Asie-Pacifique/Japon

Nous avons constaté que les infections par QSnatch avaient eu un impact considérable dans la région APJ (figure 10). Lorsqu'on compare les chiffres de chaque zone géographique, on observe que la région APJ occupe la deuxième position en termes de terminaux infectés par QSnatch, juste derrière l'Amérique du Nord. D'autre part, la région APJ devrait également surveiller les souches de ransomware REvil et LockBit, qui comptent parmi les cinq principales menaces affectant des terminaux dans la région. Bien que des membres du gang REvil aient été arrêtés l'année dernière, ce logiciel malveillant a de nouveau été détecté plusieurs mois plus tard. Il est possible que d'anciens membres ayant accès au code aient tenté de le faire revivre. Il n'est pas surprenant d'observer des menaces par ransomware (largement motivées par des raisons financières) comme LockBit et REvil. Si les opérateurs de RaaS continuent d'utiliser des IAB comme Emotet, les ransomwares demeureront un grave problème de sécurité pour les entreprises de tous les secteurs et de toutes les régions.

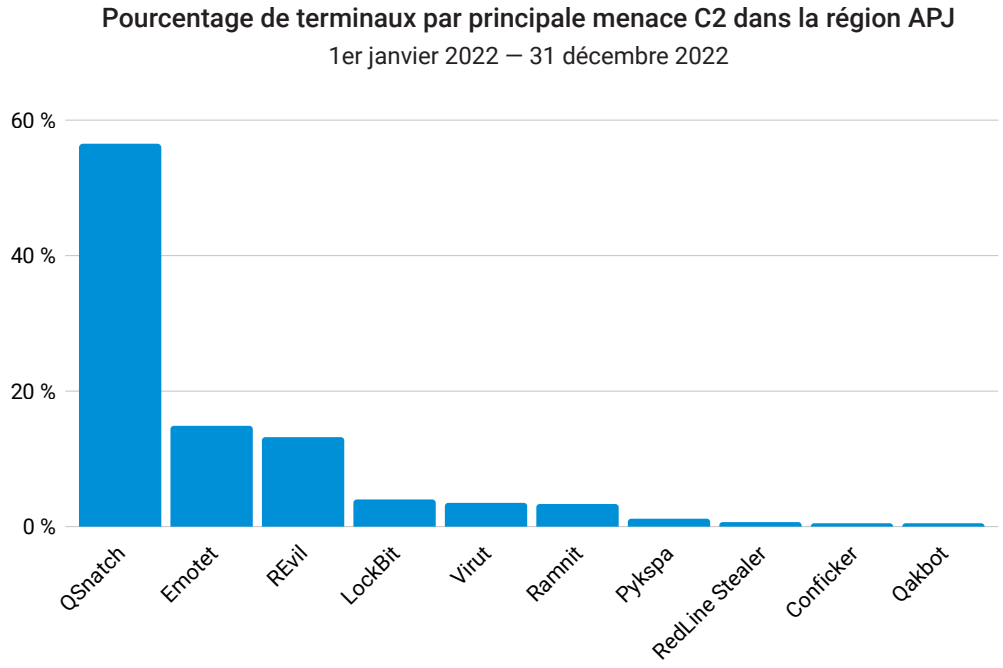


Figure 10 : Akamai a observé un nombre important d'infections par QSnatch dans la région

Amérique latine

Intéressons-nous à présent aux tendances dans la région LATAM. Bien que cette région affiche le moins grand nombre de terminaux affectés, cela ne signifie pas nécessairement qu'elle soit moins ciblée ou impactée. Comme le reste du monde, cette région a été affectée par QSnatch et Emotet (figure 11). Un simple examen de cette zone révèle qu'Agent Tesla, Virut et Ramnit sont omniprésents.

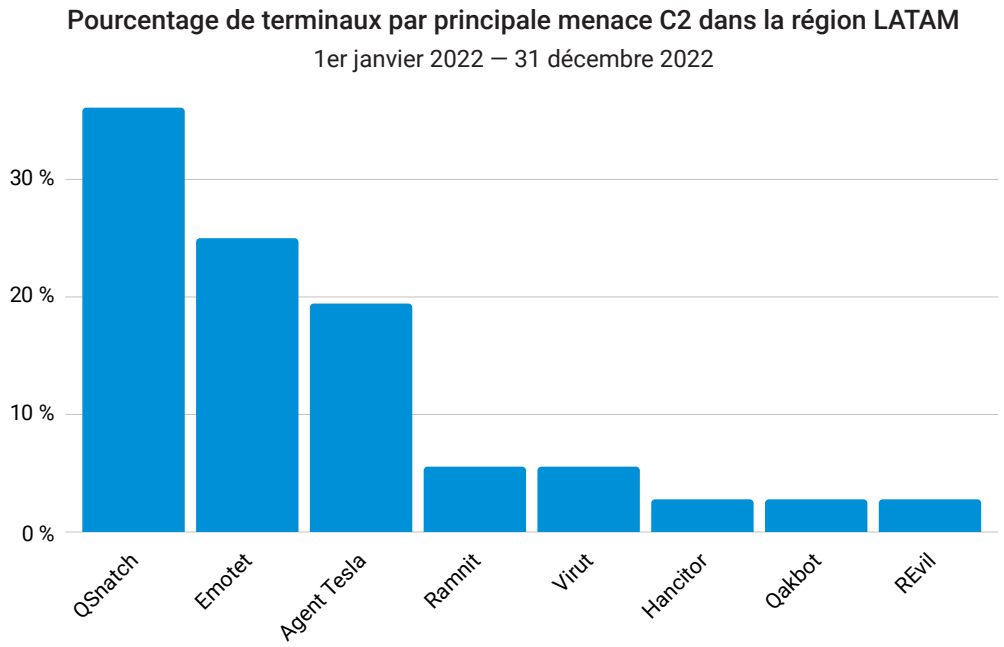


Figure 11 : les tendances mondiales se reflètent dans l'écosystème des menaces de la région LATAM

La répartition par région permet non seulement de constater les similitudes, mais aussi d'identifier les menaces propres à chaque région. Bien que QSnatch demeure la principale famille de menaces, les quatre autres menaces principales sont différentes en fonction des régions, avec un mélange d'Emotet, REvil, Ramnit et Agent Tesla. Il est important de connaître les menaces régionales pour décider des priorités de vos équipes de gestion des failles de sécurité et de tests de pénétration.

Tendances par secteur et segment de marché : le secteur industriel fortement touché par les courtiers en accès initial et les botnets

L'analyse des tendances par secteur nous permet de voir le niveau de risque de chaque segment de marché et de les comparer aux autres secteurs. Au lieu d'examiner le nombre de terminaux affectés, nous avons regroupé les terminaux par client afin de déterminer le nombre d'entreprises affectées par segment de marché (figure 12). D'après nos données DNS, nous avons constaté que plus de 30 % des organisations analysées ayant connu un trafic C2 malveillant font partie du secteur industriel. Les entreprises de services aux entreprises (15 %), de haute technologie (14 %) et de commerce (12 %) ont également été affectées. Les deux principaux segments de marché de nos données DNS (industrie et services aux entreprises) se retrouvent dans les principaux secteurs d'activité touchés par le ransomware Conti, que nous avons abordé dans notre rapport sur les menaces par ransomware dans le monde. Dans ce rapport, nous avons analysé en détail les victimes du ransomware Conti et en avons établi le profil en fonction du segment de marché, du chiffre d'affaires et de la région pour illustrer les tendances en matière d'attaque de cette menace prolifique.

> **D'après nos données DNS, nous avons constaté que plus de 30 % des organisations analysées ayant connu un trafic C2 malveillant font partie du secteur industriel. Les entreprises des secteurs des services aux entreprises (15 %), de la haute technologie (14 %) et du commerce (12 %) ont été également touchées.**

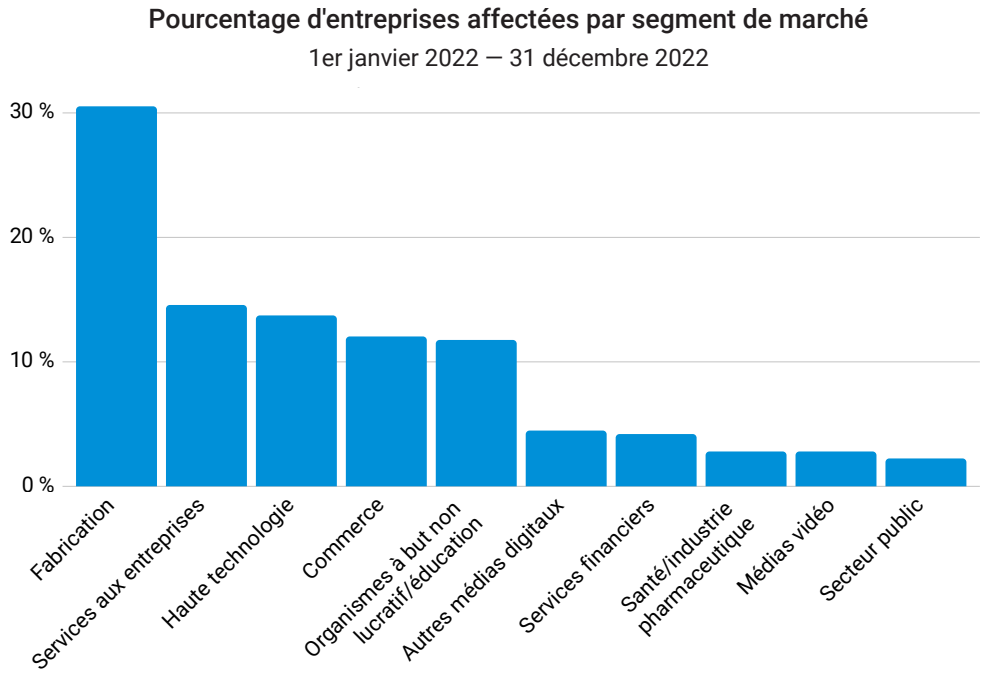


Figure 12 : les secteurs industriels, des services aux entreprises et de la haute technologie sont les plus affectés par les infections C2

Il est inquiétant de constater que le secteur industriel est fortement affecté par diverses attaques C2, car il est considéré comme une infrastructure stratégique et que les attaques réussies sur ce secteur peuvent avoir des répercussions concrètes, par exemple en perturbant la chaîne d'approvisionnement. Les données ne montrent pas de raisons spécifiques pour lesquelles le secteur industriel est le segment le plus touché, mais une enquête plus approfondie sur les types de menaces dans ce secteur pourrait permettre de mieux en comprendre les motifs.

Nous constatons que certains pays adoptent des réglementations pour renforcer la sécurité dans des secteurs stratégiques comme le secteur industriel. La directive européenne SRI 2 a renforcé les normes de cybersécurité et les exigences de sécurité, notamment l'analyse des risques et les politiques de sécurité des systèmes d'information, la sécurité de la chaîne d'approvisionnement et la gestion des incidents pour les secteurs essentiels (énergie, transports, banque, santé, etc.). Elle a également élargi la liste des secteurs concernés.

Pourcentage de terminaux par principale menace C2 dans le secteur industriel

1er janvier 2022 — 31 décembre 2022

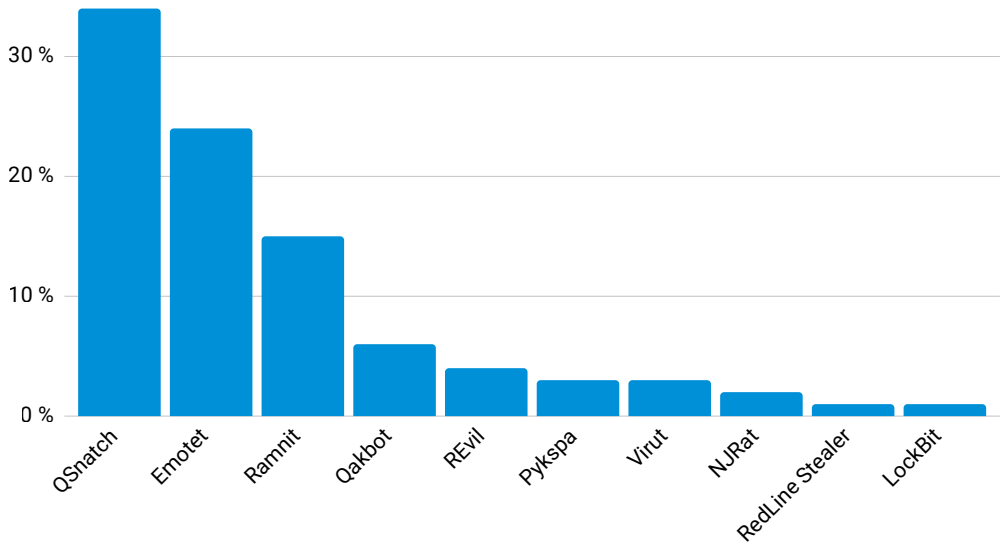


Figure 13 : les principales familles de menaces C2 détectées dans le secteur industriel sont QSnatch, Emotet et Ramnit

Un examen approfondi du secteur industriel révèle que QSnatch, les IAB et Ramnit sont quelques-uns des principaux domaines de C2 auxquels les organisations ont accédé dans ce secteur (figure 13). La présence d'IAB dans les réseaux d'entreprise peut indiquer que les pirates recueillent des renseignements sur leurs cibles potentielles et, une fois qu'ils ont accès à des machines compromises, qu'ils vendent ces données à d'autres cybercriminels comme les groupes de RaaS. On observe également des infostealers dans la liste des logiciels malveillants C2 qui menacent ce secteur. L'une des menaces à surveiller est RedLine Stealer, un programme malveillant capable de collecter des informations de navigateur telles que des identifiants et des informations de carte de crédit, actuellement vendu en tant que MaaS pour un abonnement mensuel de 100 à 150 dollars américains. Selon une étude de Group-IB, cet infostealer a collecté environ 35 585 412 journaux, qui peuvent contenir des comptes d'authentification unique, entre le deuxième semestre 2021 et le premier semestre 2022. En outre, les domaines de C2 liés à cet infostealer ont augmenté de 409 % rien qu'au troisième trimestre 2022.

Les tendances par secteur sont toujours intéressantes à suivre. Ce qui se passe dans un segment de marché n'est souvent qu'une étape sur le parcours des cybercriminels, qui s'en prendront bientôt à tous les segments de marché. Nous observons parfois que des attaquants se concentrent sur une technologie très répandue dans un secteur donné. D'autres fois, ils s'en prennent aux entreprises qui sont les plus susceptibles de payer ou à celles qui payeraient le plus. Nous avons également constaté qu'ils prenaient pour cibles des secteurs qui, traditionnellement, investissent assez peu dans la cybersécurité. La morale est qu'il vaut mieux vérifier son alarme anti-incendie lorsque l'on voit de la fumée chez son voisin.

Les utilisateurs domestiques victimes d'attaques

Les pirates jettent leur dévolu sur les entreprises, car elles offrent une meilleure rentabilité lorsqu'ils parviennent à violer la sécurité de leurs réseaux. Ils utilisent un large éventail d'outils et de tactiques pour infiltrer un périmètre d'entreprise, maintenir des connexions persistantes et, dans certains cas, exfiltrer des informations confidentielles. C'est pourquoi, comme nous l'avons vu dans la section précédente, nous observons des menaces comme les infostealers et les IAB dans les réseaux d'entreprise. Le scénario est toutefois différent dans les réseaux domestiques, en termes de menaces employées et de but poursuivi.

Les utilisateurs domestiques représentent une population qui n'est souvent pas aussi bien protégée qu'un environnement d'entreprise, mais n'offre pas le même rendement monétaire. Les attaquants le savent et recherchent des moyens de monétiser leur capacité à infecter plus facilement les terminaux domestiques. Par exemple, ils lancent des campagnes à grande échelle dans l'espoir de compromettre autant de terminaux que possible, alors que les attaques contre les entreprises sont hautement ciblées. Une fois que ces terminaux domestiques sont intégrés à un immense botnet, les pirates peuvent mobiliser ces terminaux zombies pour exécuter d'innombrables activités cybercriminelles à l'insu de l'utilisateur, comme le spamming et le lancement d'attaques DDoS contre des organisations. Et pour que les botnets atteignent leur objectif ou que les cybercriminels puissent louer leurs botnets, ils doivent infecter un maximum de terminaux. Une autre façon pour les pirates d'obtenir un gain financier en attaquant les utilisateurs domestiques est d'utiliser les ressources informatiques des terminaux infectés à des fins de minage de cryptomonnaie.

> **Une fois que ces terminaux sont intégrés à un immense botnet, les pirates peuvent mobiliser ces terminaux zombies pour exécuter d'innombrables activités cybercriminelles à l'insu de l'utilisateur, comme le spamming et le lancement d'attaques DDoS contre des organisations.**

Les réseaux domestiques affichent un trafic important de botnets

Au fur et à mesure que nous nous concentrons sur les utilisateurs domestiques, nous examinons le trafic DNS malveillant des réseaux domestiques en analysant un échantillon anonyme des millions de requêtes signalées par des attaques malveillantes des six derniers mois, afin d'identifier les menaces dont les utilisateurs devraient s'inquiéter. On constate que les principales menaces sont des botnets, ce qui pourrait expliquer comment les pirates exploitent les terminaux IoT à différentes fins, que nous aborderons dans les sections suivantes.

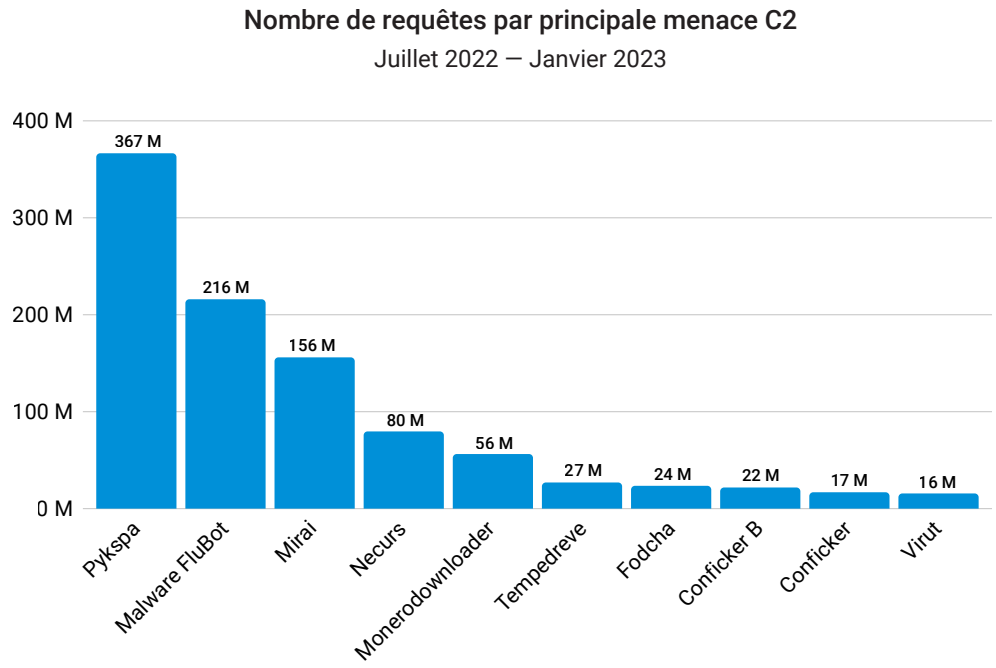


Figure 14 : Pykspa, FluBot et Mirai sont les trois principaux botnets observés dans le trafic DNS des réseaux domestiques

Pykspa : propagation via les réseaux sociaux

D'après nos données, Pykspa a représenté 367 millions de requêtes DNS signalées au niveau mondial (figure 14). Cette menace se propage via Skype en envoyant des liens malveillants aux contacts des utilisateurs affectés. Dans certains cas, lorsque Twitter est ouvert dans l'onglet du navigateur, il crée également un tweet avec un lien de téléchargement vers le programme malveillant. Il utilise par ailleurs un algorithme de génération de domaine (DGA) pour établir une communication C2. Par le passé, Pykspa v2 a utilisé un sous-ensemble de son algorithme DGA pour éviter d'être détecté et rester dans le réseau plus longtemps.

Ses capacités d'accès par une porte dérobée permettent à un attaquant de se connecter à un système distant pour exécuter des commandes arbitraires telles que le téléchargement de fichiers, l'arrêt de processus et la propagation par divers moyens (lecteurs mappés, partages réseau, etc.). Pykspa interroge également la configuration de Skype pour collecter des informations personnelles sur les utilisateurs concernés. Il empêche également les utilisateurs d'accéder à certains sites Web, notamment si ces derniers contiennent des chaînes liées à des solutions de protection contre les logiciels malveillants. Il est intéressant de noter qu'il vérifie l'interface linguistique de Skype de l'utilisateur affecté et que, s'il s'agit de l'une des nombreuses langues qu'il surveille, notamment l'allemand, l'anglais, l'espagnol, le français et l'italien, le programme malveillant procède à des ajustements du message Skype spammé en conséquence.

FluBot : un botnet de programmes malveillants Android

Le logiciel malveillant FluBot constitue la principale famille de programmes malveillants C2 après Pykspa. Il infecte principalement les téléphones Android en envoyant des SMS qui incitent les utilisateurs à cliquer sur un lien malveillant, ce qui déclenche par la suite le téléchargement du programme malveillant. Pour se propager, le logiciel malveillant FluBot télécharge les listes de contacts des utilisateurs affectés sur le serveur C2 et envoie également les contacts des victimes en utilisant le même leurre d'ingénierie sociale. La présence de FluBot sur le terminal des utilisateurs compromet leurs informations bancaires et financières, car ce logiciel malveillant est capable de superposer une fausse page lorsque les utilisateurs accèdent à des applications bancaires légitimes. Ces informations d'identification peuvent ensuite être utilisées afin d'usurper l'identité des utilisateurs ou d'effectuer des transactions frauduleuses.

Ce logiciel malveillant utilise divers leurres d'ingénierie sociale. Il incite parfois les utilisateurs à cliquer sur un lien pour vérifier le statut de leur livraison de colis ; dans d'autres cas, il les invite à télécharger une fausse application de messagerie vocale en les informant qu'ils ont reçu un message vocal. Il peut également se faire passer pour une mise à jour de sécurité et inviter les utilisateurs à cliquer sur le lien. Une fois que les utilisateurs cliquent sur le lien, il leur demande de télécharger une application, qui demande l'autorisation d'accéder aux listes de contacts, de passer des appels téléphoniques, etc. Ce qui rend cette menace si dangereuse, c'est qu'elle demande également l'autorisation d'accéder aux services d'accessibilité, ce qui permet aux pirates de contrôler les saisies sur l'écran et éventuellement d'installer d'autres applications. Il est conseillé aux utilisateurs de réinitialiser les paramètres par défaut de leur terminal afin de supprimer ce logiciel malveillant.

Mirai : le potentiel de l'Internet des objets utilisé pour provoquer des perturbations à grande échelle

Dans notre étude, Mirai suit de près le programme malveillant FluBot, avec 156 millions de requêtes DNS signalées. Connu pour cibler les terminaux IoT dotés de ports telnet ouverts, Mirai est devenu tristement célèbre pour avoir perpétré une attaque DDoS contre l'un des plus grands fournisseurs de DNS. Il s'agit d'un ver se répandant automatiquement qui recherche des terminaux vulnérables utilisant les combinaisons de nom d'utilisateur et de mot de passe par défaut. À un moment donné, il a accumulé plus de 100 000 terminaux zombies, que les pirates ont utilisés dans des attaques DDoS contre des cibles de grande envergure. Lors d'une de ses attaques précédentes, Mirai a utilisé 145 000 terminaux pour attaquer une entreprise technologique. Cet exemple montre comment les terminaux non sécurisés peuvent être manipulés pour commettre des cyberattaques et provoquer des perturbations à grande échelle contre les entreprises.

En 2016, le groupe derrière Mirai a publié le code source du programme, sans doute pour empêcher les autorités de remonter jusqu'aux auteurs d'origine (et donc éviter d'être arrêtés). Suite à cela, d'autres groupes ont commencé à utiliser le code de Mirai, le modifiant et lui ajoutant des fonctionnalités telles que la possibilité d'infecter les systèmes. La publication du code a notamment eu pour conséquence l'émergence de nouvelles variantes, comme Okiru, Satori, Masuta et PureMasuta, qui ont elles aussi pour objectif le lancement d'attaques DDoS. Bien qu'il soit utile de redémarrer le terminal infecté, car le programme malveillant est constamment à la recherche de terminaux, il y a une forte probabilité de réinfection si l'utilisateur ne modifie pas son mot de passe.

Necurs : distributeur de programmes malveillants et vendeur d'accès

Détecté pour la première fois en 2012, le botnet Necurs est à l'origine de 80 millions de requêtes signalées au cours des six derniers mois. Il constitue une menace sérieuse pour les utilisateurs domestiques comme pour les entreprises grâce à sa capacité à distribuer des charges utiles d'autres programmes malveillants comme Dridex, TrickBot et Locky. Il est important de souligner que ce botnet vend également l'accès à des ordinateurs infectés à d'autres groupes dans le cadre de ses offres de location de botnet. Comme la plupart des botnets, il utilise un algorithme DGA afin de générer de nombreux domaines pour ses serveurs C2 et de continuer à fonctionner malgré le blocage de domaines.

En plus de distribuer des ransomwares et des chevaux de Troie bancaires, Necurs est utilisé pour distribuer diverses attaques de spams (escroqueries via des sites de rencontre russes, envoi de spams pharmaceutiques, etc.). Dans le cadre de ses investigations, Microsoft a suivi les activités de ce botnet et a découvert qu'en seulement 58 jours, il avait envoyé environ 3,8 millions de spams. En 2020, les activités du botnet Necurs ont été perturbées par la collaboration entre les forces de l'ordre et la communauté de la sécurité.

Monerodownloader : un botnet de minage

Le minage de cryptomonnaie est l'une des nombreuses activités qui permettent aux pirates de réaliser des bénéfices. La popularité croissante de la cryptomonnaie Monero parmi les cybercriminels est l'une des raisons qui explique pourquoi nous observons des botnets conçus spécifiquement dans ce but. Les pirates préfèrent cette cryptomonnaie à d'autres, car sa chaîne n'est pas aussi exposée et garantit l'anonymat, évitant ainsi qu'on remonte jusqu'à eux. Bien qu'on sache très peu de choses sur le réseau Monerodownloader, on sait que l'une de ses tactiques consiste à collecter des informations et à se connecter à des serveurs C2 pour exécuter la charge utile réelle.

Les systèmes qui n'ont pas reçu de correctif sont vulnérables à des menaces comme les mineurs de cryptomonnaie Monero. D'autres mineurs de Monero similaires exploitent les vulnérabilités, se présentent comme des logiciels gratuits pour inciter les utilisateurs à télécharger le mineur et sont capables de se déplacer latéralement dans le réseau et d'infecter d'autres terminaux pour engranger un maximum de bénéfices. Bien que la description du mouvement latéral s'applique davantage aux entreprises qu'aux utilisateurs domestiques, cela nous donne un aperçu de la façon dont les mineurs de cryptomonnaie fonctionnent pour optimiser l'infection.

Principales menaces par région : les botnets continuent de régner en maître dans les réseaux domestiques

Examinons de plus près nos données régionales pour déterminer quels botnets sont les plus répandus par région en fonction du trafic DNS des réseaux domestiques et étudier les facteurs qui contribuent à cette tendance.

Amérique du Nord

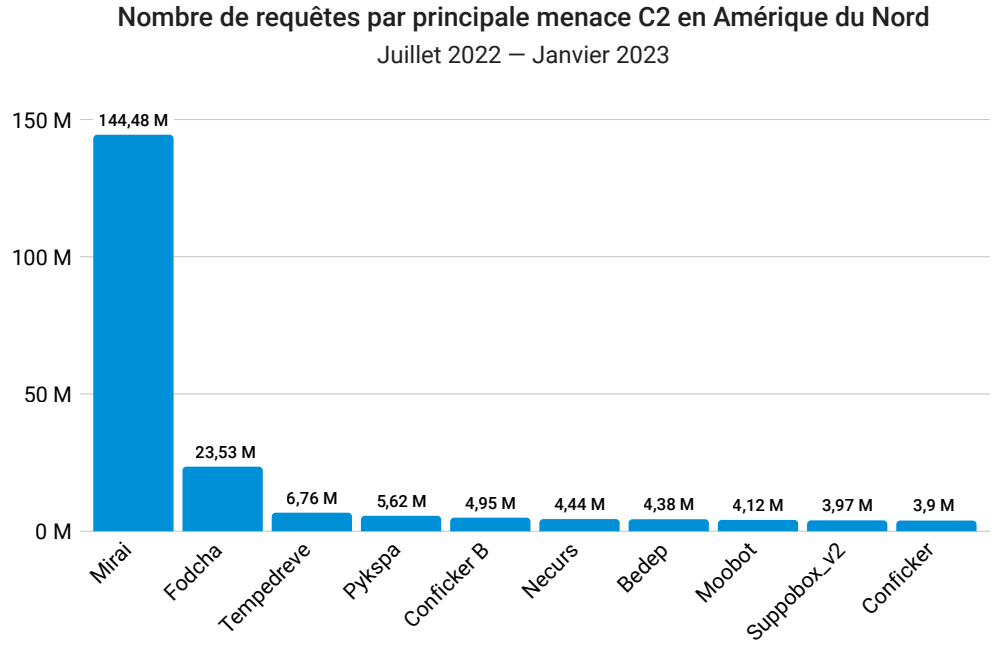


Figure 15 : Mirai continue de faire des vagues en Amérique du Nord, probablement en raison des terminaux IoT non sécurisés

En Amérique du Nord, plus de 144 millions de demandes liées au botnet Mirai ont été observées sur les réseaux domestiques (figure 15). Ce botnet cible les terminaux IoT vulnérables qui utilisent encore les noms d'utilisateur et les mots de passe par défaut. Le volume élevé de requêtes en provenance de cette région peut être dû à la popularité ou à la forte utilisation de terminaux IoT dans les foyers. Rien qu'en 2022, on estime que les ménages américains possédaient en moyenne 22 terminaux connectés, un chiffre en légère baisse par rapport à l'année précédente (25). Compte tenu de la hausse annoncée des connexions IoT en Amérique du Nord (5,4 milliards d'ici 2025), il est fort probable qu'émergent d'autres menaces comme Mirai, ou des variantes similaires ciblant les terminaux IoT non sécurisés.

Cette menace signifie que les cybercriminels peuvent utiliser les terminaux des utilisateurs domestiques à leur insu pour commettre des crimes. Cependant, les organisations pâtissent également des effets des attaques DDoS et des campagnes de spams malveillants lancées par des botnets comme Mirai. Il est toujours judicieux de changer le nom d'utilisateur et le mot de passe par défaut de vos terminaux pour les protéger contre Mirai et d'autres attaques de ce type.

Europe, Moyen-Orient et Afrique

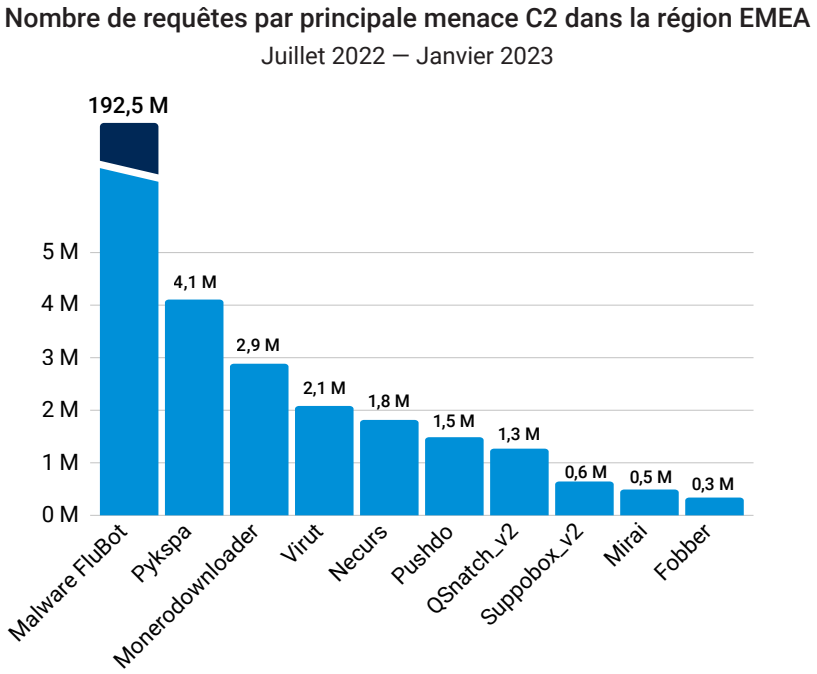


Figure 16 : nous avons constaté une explosion du logiciel malveillant FluBot dans la région EMEA, probablement en raison de sa tactique de propagation et de l'utilisation de plusieurs langues européennes dans son leurre d'ingénierie sociale

Dire que le logiciel malveillant FluBot se propage comme un feu de forêt dans la région EMEA serait un euphémisme. On observe un volume impressionnant de requêtes DNS dans cette région (environ 193 millions). Notre analyse du trafic DNS nous a permis d'observer ces infections dans la zone EMEA (figure 16). La tactique de propagation du smishing, une forme d'hameçonnage qui consiste à envoyer un SMS à la liste de contacts de la victime, joue un rôle important. En outre, le botnet dupe les utilisateurs en les incitant à télécharger une application liée à la livraison d'un colis ou une application de messagerie vocale, qui est en réalité le logiciel malveillant. FluBot demande également des autorisations supplémentaires et enregistre secrètement les informations d'identification bancaires/financières des utilisateurs à leur insu. Des utilisateurs auraient été ciblés en Espagne, en Allemagne, en Finlande et au Royaume-Uni, entre autres. Le SMS est également écrit dans plusieurs autres langues de l'UE, comme l'allemand et le hongrois, ce qui pourrait être l'un des facteurs expliquant pourquoi ce programme malveillant s'est multiplié en Europe.

Amérique latine

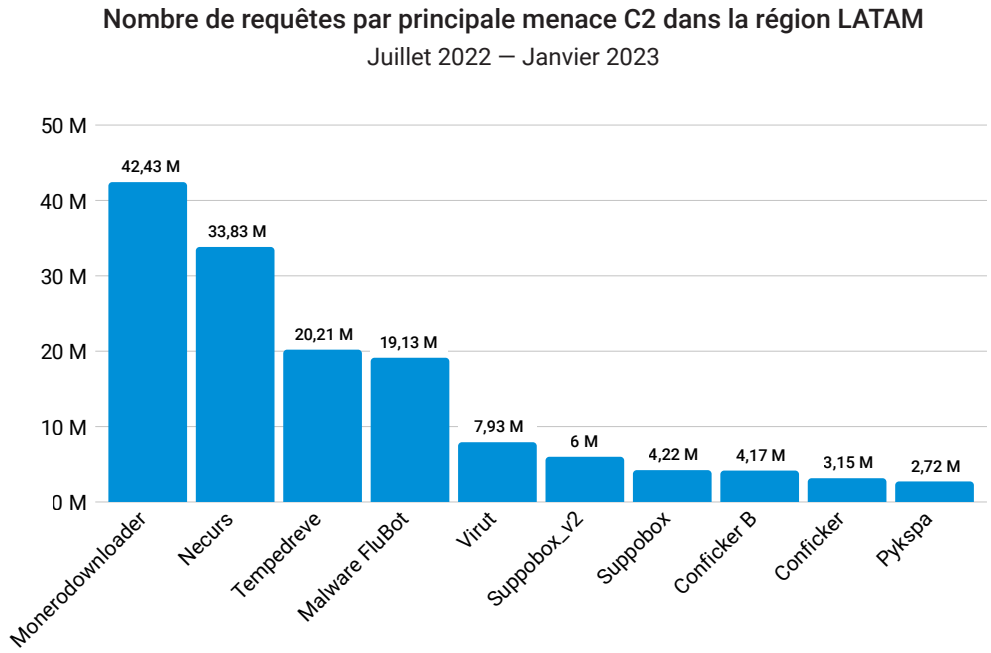


Figure 17 : le botnet de minage de cryptomonnaie Monerodownloader est devenu la principale menace en Amérique latine, probablement en raison du taux élevé d'adoption des cryptomonnaies dans la région

Contrairement à l'Amérique du Nord et à la zone EMEA, la région LATAM affiche une répartition plus diversifiée des botnets (figure 17). Monerodownloader, un botnet de minage de cryptomonnaie, est au premier rang des groupes de botnet actifs, avec 42 millions de requêtes signalées, suivi de Necurs (34 millions) et de Tempreve (20 millions). Le fort taux d'adoption des cryptomonnaies dans cette région, alimenté par une inflation élevée et des envois de fonds importants, pourrait expliquer pourquoi des botnets comme Monerodownloader arrivent en tête de liste. Les cybercriminels peuvent exploiter les ressources des terminaux des utilisateurs à leur insu pour miner des cryptomonnaies et s'enrichir. Il est également intéressant de noter que FluBot est l'une des principales menaces observées dans le trafic DNS, ce qui montre la prévalence de ce botnet même en dehors de la région EMEA, où nous avons observé un trafic important.

Asie-Pacifique/Japon

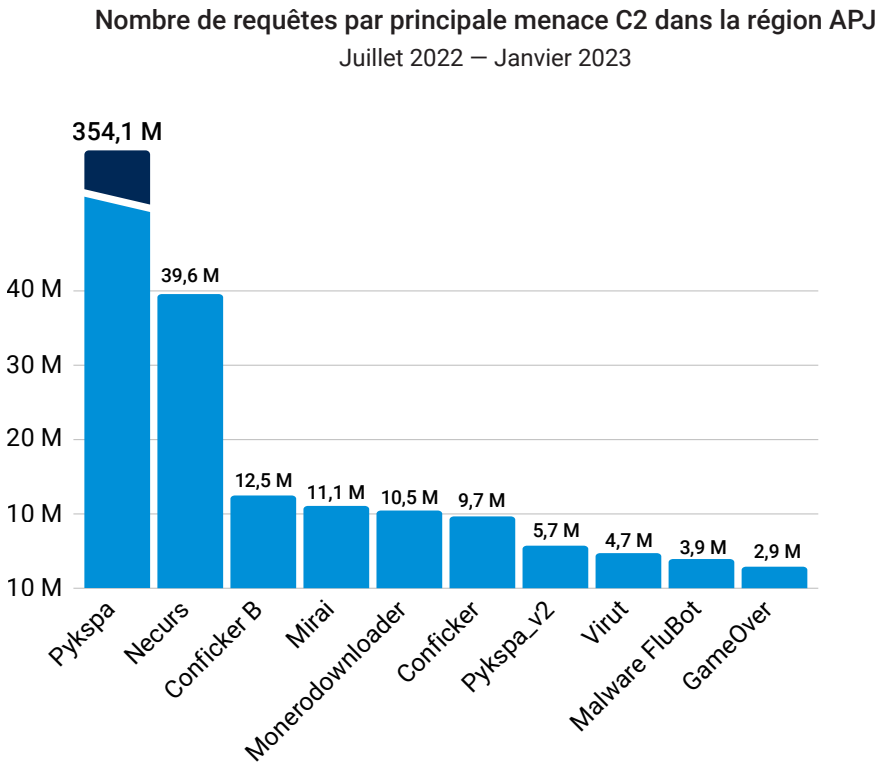


Figure 18 : les menaces dominantes dans la région APJ sont Pykspa et Necurs

Plus de 350 millions de demandes relatives à Pykspa ont été observées dans la région APJ (figure 18). Dans un article publié en 2019 sur le blog, nous avons expliqué que Pykspa utilisait un algorithme DGA sélectif pour rester indétectable le plus longtemps possible. Les domaines mentionnés dans ce rapport se trouvaient principalement en Asie de l'Est. Nous avons également observé des requêtes associées à des botnets comme Necurs, ce qui indique qu'il est très probable que les systèmes soient infectés par d'autres programmes malveillants.

Vue d'ensemble de l'écosystème du hameçonnage

Dans la dernière partie de notre analyse du trafic DNS, nous avons examiné les kits d'hameçonnage et leur rôle crucial dans le succès des campagnes d'hameçonnage. L'hameçonnage reste plus que jamais d'actualité en raison des tactiques en constante évolution utilisées par les pirates et du nombre croissant d'informations personnelles disponibles en ligne. Les cybercriminels utilisent l'ingénierie sociale pour que leurs tentatives d'hameçonnage soient perçues comme légitimes, et des preuves indiquent que le taux de réussite de ces attaques reste élevé. Les recherches d'Akamai sur les escroqueries par hameçonnage pendant les fêtes ont révélé l'utilisation de nouvelles techniques et tactiques par les pirates pour continuer à rester indétectables. Ces dernières incluent notamment l'utilisation de témoignages de faux utilisateurs et la technique récemment découverte d'ancrage HTML, qui vise à s'assurer que seuls des utilisateurs valides arrivent sur les sites Web de l'escroquerie.

L'augmentation du télétravail due à la pandémie de COVID-19 a également compliqué la détection et la prévention des attaques d'hameçonnage, ce qui rappelle l'importance pour les particuliers et les entreprises de rester vigilants et de prendre des mesures pour se protéger. En outre, l'essor des réseaux sociaux et le nombre croissant de terminaux connectés à Internet ont multiplié les opportunités pour les cybercriminels.

Les campagnes d'hameçonnage affectent les services financiers

Il existe plusieurs modes de collecte des données pour déterminer quelles marques ont tendance à être exploitées et imitées dans des escroqueries par hameçonnage. Nous avons comparé le nombre total de campagnes au nombre de victimes. Cela nous permet d'évaluer le taux de réussite d'une campagne donnée et de connaître le pourcentage ciblé dans chaque secteur.

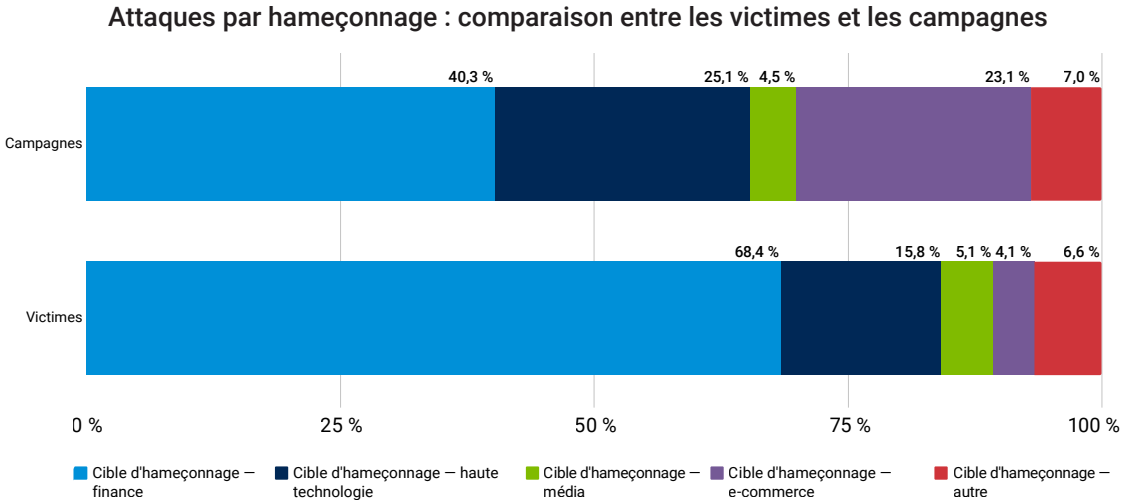


Figure 19 : la majorité des campagnes d'hameçonnage ont visé le secteur des services financiers au 4e trimestre 2022

Nos recherches ont révélé que les secteurs de la haute technologie et des services financiers arrivaient en tête du nombre de campagnes et de victimes (figure 19). Nous avons constaté que 40,3 % des campagnes visant les clients des services financiers avaient été activées, ce qui a entraîné 68,4 % de victimes. Cela indique que les attaques contre les services financiers ont été très efficaces au quatrième trimestre 2022. Dans notre rapport sur les services financiers, Ennemi en vue : analyse des attaques visant les services financiers, nous avons souligné que les attaques par hameçonnage étaient motivées par l'argent et ciblaient principalement les services financiers et leurs clients. Les impacts potentiels de telles attaques incluent des atteintes à la marque et à la réputation, ainsi que la perte de confiance des clients. L'hameçonnage peut également coûter des ressources à l'entreprise pour résoudre le problème.

Nous avons constaté que l'e-commerce concernait 23 % des campagnes d'hameçonnage activées au quatrième trimestre 2022. Bien que nous ayons observé plus de campagnes que de véritables victimes, il est intéressant de noter que les pirates ciblent ce secteur. Les utilisateurs doivent donc rester vigilants, car les cybercriminels peuvent s'en prendre à leurs informations personnelles ou bancaires.

Kits d'outils d'hameçonnage : des aides indispensables aux escroqueries par hameçonnage

L'extrême ampleur de l'écosystème d'hameçonnage est due aux kits d'outils d'hameçonnage. Les outils d'hameçonnage permettent le déploiement et la maintenance de sites Web d'hameçonnage, ce qui pousse même les escrocs non-techniciens à rejoindre l'écosystème de l'hameçonnage et à lancer des escroqueries de ce type.

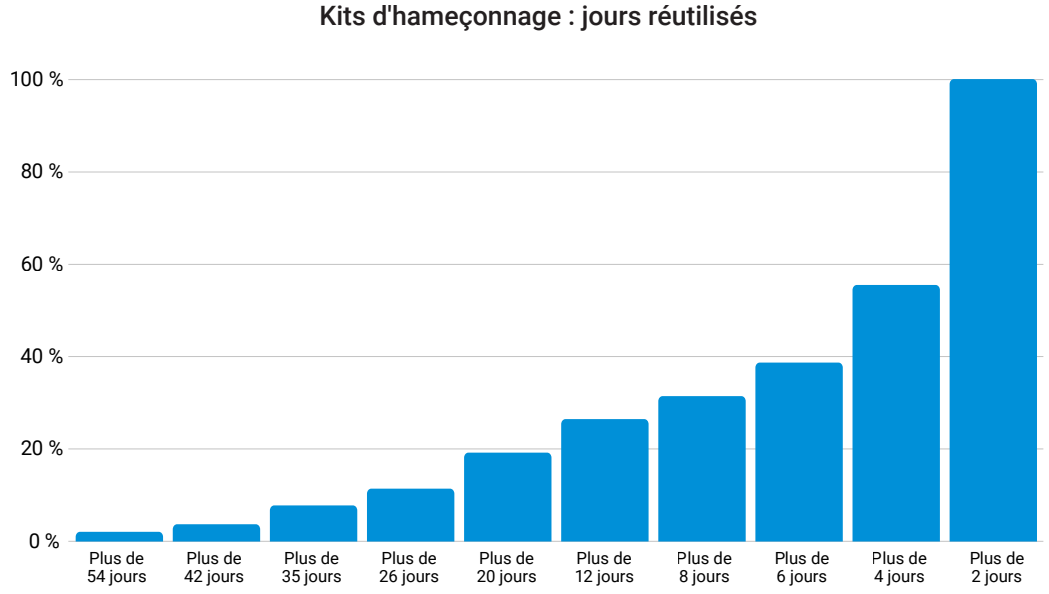


Figure 20 : kits d'outils d'hameçonnage par nombre de jours réutilisés au 4e trimestre 2022

Selon nos études, qui ont suivi plus de 300 kits d'outils d'hameçonnage différents utilisés pour lancer de nouvelles campagnes d'attaques, 2,04 % des kits suivis ont été réutilisés pendant au moins 54 jours au cours du quatrième trimestre 2022 (figure 20). En outre, 55,5 % des kits ont été réutilisés pour lancer une nouvelle campagne d'attaque pendant au moins quatre jours, et 100 % des kits suivis ont été réutilisés pendant au moins deux jours au quatrième trimestre 2022.

Conclusion et recommandations : combattre les attaques actuelles en mettant en place des mesures proactives

Maintenant que nous avons passé en revue les groupes de menaces et les méthodes des pirates, voyons comment exploiter toutes ces informations. Nous commencerons par nous demander s'il vaut mieux gérer le DNS en interne ou sous-traiter sa gestion à un tiers. Si vous êtes une grande entreprise ou une organisation complexe, il peut être judicieux de demander à un fournisseur spécialisé dans la gestion du DNS de s'occuper de cette activité pour vous. Dans tous les cas, pensez à surveiller les performances et les protections de votre DNS. Ensuite, réfléchissez aux différents contrôles dont vous aurez besoin. Les attaques DDoS, les attaques de logiciels malveillants et l'extraction, les mouvements latéraux et l'exfiltration sont les principales menaces contre lesquelles vous devez vous protéger. Un modèle de cybersécurité appelé chaîne d'attaque suit ce parcours de données et recherche toutes les vulnérabilités critiques que vous pouvez corriger à chaque étape de la chaîne.

Envisagez de mettre en place des stratégies pour les techniques d'attaque décrites dans ce rapport. Consultez votre équipe de test de pénétration ou votre équipe rouge pour savoir si elles utilisent les mêmes outils et techniques que les IAB comme Qakbot et Emotet, les bots comme QSnatch, les ransomwares comme LockBit (en laboratoire), et des outils comme Cobalt Strike. Il est important de s'assurer de l'efficacité de vos contrôles de sécurité quant à l'alerte et au blocage de ces types d'attaques, et que vos équipes sont formées pour y répondre.

Si Cobalt Strike est détecté dans votre réseau, générez immédiatement un rapport d'incident et menez l'enquête. Bien que cet outil puisse être utilisé par votre équipe rouge (auquel cas, il doit tout de même être examiné et signalé), la présence d'un tel trafic doit déclencher l'alarme, car sa présence peut indiquer une intrusion par d'autres groupes d'attaque RaaS ou cybercriminels, et signaler une attaque en cours qu'il est encore temps de déjouer.

Réfléchissez au fonctionnement de votre centre d'opérations de sécurité et déterminez comment vous surveillez les processus (bits, wget, curl, etc.) indiquant la probabilité qu'une menace liée à un IAB effectue une reconnaissance dans votre réseau. Les composants essentiels cherchent ce qui a été téléchargé et interrompent le téléchargement s'il est toujours en cours. Étudiez ensuite ce qui a déclenché l'IAB (fichier LNK, macro, VScript ?) et découvrez à partir de là comment la violation a commencé.

Tenez-vous au courant de nos dernières recherches en consultant notre centre de recherche sur la sécurité.

Méthodologies

Trafic des attaques par commande et contrôle

Les données de ce rapport proviennent de notre solution Secure Internet Access (SIA) et décrivent le trafic des attaques par commande et contrôle (C2). SIA est une passerelle Web sécurisée dans le cloud, conçue pour aider les utilisateurs à connecter facilement leurs terminaux à Internet en toute sécurité. Les deux ensembles de données utilisés dans ce rapport reflètent respectivement les données d'alertes de sécurité provenant d'entreprises comptant de nombreux utilisateurs, et de fournisseurs d'accès Internet grand public. Ces données ont été mesurées par le nombre de terminaux affectés et le nombre de requêtes, respectivement. Un terminal affecté est défini comme un terminal qui a communiqué au moins une fois avec un domaine de C2 connu et identifié. De même, une requête C2 est définie comme une requête qui a communiqué avec un domaine de C2 connu et identifié. Nos équipes de sécurité utilisent ces données en interne pour étudier les attaques, signaler des comportements malveillants afin d'avertir les clients et fournir des renseignements supplémentaires aux solutions de sécurité d'Akamai.

Crédits

Édition et rédaction

Or Katz

Eliad Kimhy

Badette Tribbey

Révision et expertise

Tanya Belousov

Shiran Guez

Ophir Harpaz

Stiv Kupchik

Grace Wang

Steve Winterfeld

Analyse des données

Ronan Ballantine

Gal Kochner

Chelsea Tuttle

Marketing et publication

Georgina Morales Hampe

Shivangi Sahu

D'autres rapports État des lieux d'Internet / Sécurité

Lisez les numéros précédents et surveillez les prochaines parutions du célèbre rapport État des lieux d'Internet / Sécurité d'Akamai. akamai.com/soti

D'autres recherches d'Akamai sur les menaces

Tenez-vous au courant des dernières analyses d'informations sur les menaces, des rapports de sécurité et des recherches sur la cybersécurité. akamai.com/security-research

Accéder aux données de ce rapport

Consultez des versions de haute qualité des graphiques et des tableaux référencés dans ce rapport. Ces images sont libres d'utilisation et de référence, à condition qu'Akamai soit dûment crédité en tant que source et que le logo Akamai soit conservé. akamai.com/sotidata

En savoir plus sur les solutions Akamai

Pour en savoir plus sur les solutions Akamai de lutte contre les menaces ciblant les entreprises, consultez notre page Secure Internet Access Enterprise. Les fournisseurs de services qui ciblent le marché grand public et celui des PME peuvent consulter nos services Secure Internet Access pour les FAI.

Akamai soutient et protège la vie en ligne. Les entreprises leaders du monde entier choisissent Akamai pour concevoir, diffuser et sécuriser leurs expériences digitales, et aident des milliards de personnes à vivre, travailler et jouer chaque jour. Akamai Connected Cloud, plateforme cloud massivement distribuée en bordure de l'Internet, rapproche les expériences et les applications des utilisateurs tout en éloignant les menaces. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu d'Akamai, rendez-vous sur akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur Twitter et LinkedIn. Publication : 03/23