Surveillance de masse par l'armée américaine

Le 21 septembre 2022 par Joseph Cox https://www.vice.com/en/article/y3pnkw/us-military-bought-mass-monitoring-augury-team-cymru-browsing-email-data

Augury (Image Smederevac)

L'armée américaine a acquis un outil de surveillance de masse qui concerne des données relatives à la navigation sur Internet et aux courriels. La plateforme "Augury" compte des données de réseau très sensibles que Team Cymru, une entreprise privée, vend à l'armée. «Tout est là. Rien d'autre à capturer si ce n'est l'odeur de l'électricité», a déclaré un expert en cybersécurité.

Plusieurs branches de l'armée américaine ont acheté l'accès à un puissant outil de surveillance d'Internet qui prétend couvrir plus de 90 % du trafic Internet mondial et qui, dans certains cas, permet d'accéder aux données de messagerie, à l'historique de navigation et à d'autres informations telles que les cookies Internet des individus, selon des données contractuelles et d'autres documents examinés par *Motherboard*.

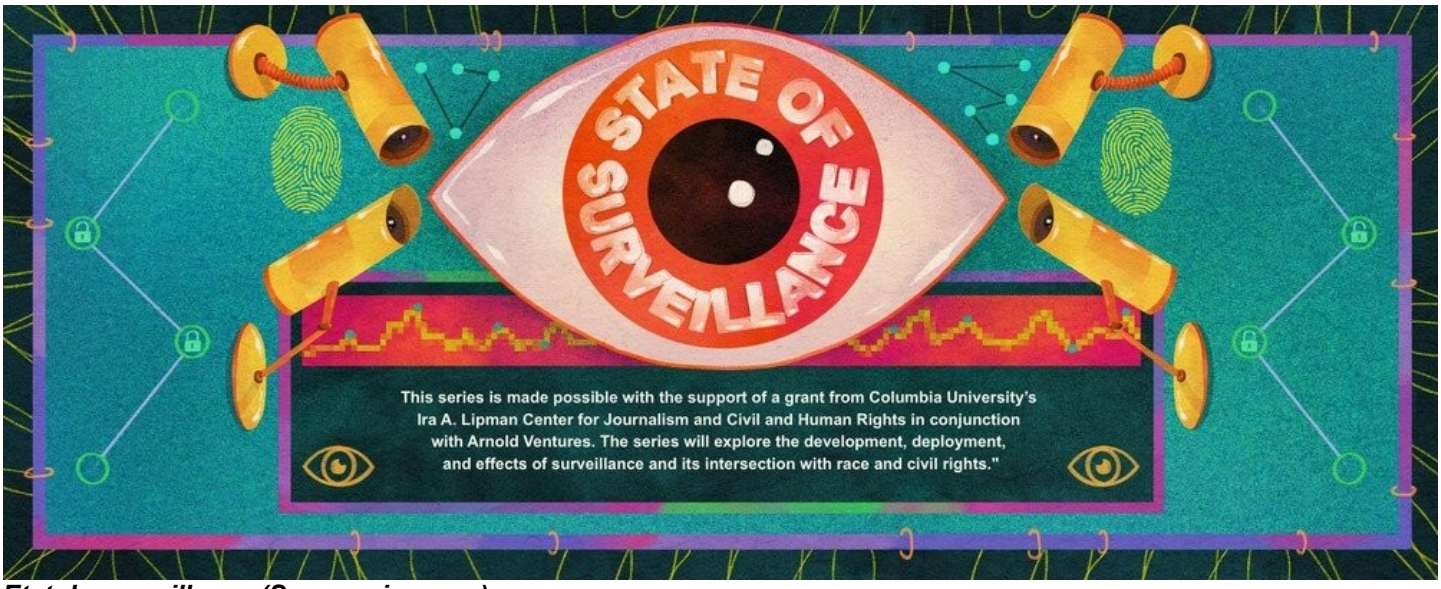
En outre, le sénateur Ron Wyden indique qu'un lanceur d'alerte a contacté son bureau concernant des allégations d'utilisation et d'achat sans mandat de ces données par le NCIS, (https://www.documentcloud.org/documents/22670252-1763_001) selon la copie de la lettre partagée par le bureau de Wyden avec *Motherboard*, agence civile chargée de l'application de la loi qui fait partie de la marine, et qui a déposé, auprès du ministère de la Défense, une plainte par le biais de la procédure officielle de signalement.

Ces documents révèlent la vente et l'utilisation d'une capacité de surveillance jusqu'alors peu connue, alimentée par des achats de données auprès du secteur privé. L'outil, appelé Augury, est développé par la société de cybersécurité Team Cymru et regroupe une quantité massive de données qu'elle met à la disposition des gouvernements et des entreprises en tant que service payant.

Dans le secteur privé, les analystes en cybersécurité l'utilisent pour suivre l'activité des pirates ou trouver la source de cyberattaques. Dans les agences gouvernementales, les analystes peuvent en faire de même, mais celles qui sont en charge des enquêtes criminelles ont également acheté cette fonctionnalité. Les agences militaires n'ont pas renseigné leurs cas d'utilisation de l'outil. Cependant, la vente de l'outil met en évidence la façon dont Team Cymru obtient ces données controversées et les revend ensuite comme une entreprise, ce qui a alarmé de multiples sources dans le secteur de la cybersécurité.

«Les informations du réseau comprennent des données provenant de plus de 550 points de collecte dans le monde entier, dont certains en Europe, au Moyen-Orient, en Amérique du Nord/Sud, en Afrique et en Asie, et sont mises à jour au moyen de pas moins de 100 milliards de nouveaux enregistrements chaque jour», peut-on lire dans une description de la plateforme Augury dans un dossier d'achat du gouvernement américain examiné par *Motherboard* (https://sam.gov/opp/96b4874e76af45be90bb5a0b8b2bdb6b/view). Elle ajoute qu'Augury donne accès à des

«pétaoctets» de données actuelles et passées.



Etat de surveillance (Source vice.com)

Motherboard a découvert que la marine et l'armée américaines, le Cyber Command et la Defense Counterintelligence and Security Agency ont collectivement payé au moins 3,5 millions de dollars pour avoir accès à Augury. Cela permet aux militaires de suivre l'utilisation d'Internet en utilisant une quantité incroyable d'informations sensibles.

Motherboard a largement couvert (https://www.vice.com/en/article/n7wakg/cbp-dhs-location-data-venntel-apps) la manière dont les agences américaines accèdent à des données qui, dans certains cas, nécessiteraient un mandat ou un autre mécanisme légal, et cela, simplement en achetant auprès de sociétés privées des données disponibles dans le commerce.

Le plus souvent, les ventes portent sur les données de localisation récoltées sur les smartphones. Les achats d'Augury montrent que cette approche consistant à acheter l'accès aux données s'étend également aux informations plus directement liées à l'utilisation d'Internet.

Team Cymru affirme sur son site web que sa méthode (https://www.team-cymru.com/post/what-we-re-seeing-with-x-509-certificates-and-why-you-should-worry) donne «accès à une écrasante majorité de toutes les activités sur Internet».

Travaillez-vous dans une entreprise qui traite des données de flux net? Travaillez-vous chez un FAI [Fournisseur d'Accès Internet, NdT] qui distribue ces données? Ou savez-vous autre chose sur le commerce ou l'utilisation des données de flux net? Nous serions ravis de vous entendre.

En utilisant un téléphone ou un ordinateur non professionnel, vous pouvez contacter Joseph Cox en toute sécurité sur Signal au +44 20 8133 5190, Wickr sur josephcox, ou par e-mail joseph.cox@vice.com.

«Augury donne une visibilité à 93% du trafic internet», peut-on lire sur un autre site web décrivant l'outil. (https://www.cosive.com/augury). Certains clients ont accès à la plateforme sous la marque différente de Pure Signal RECON, selon le site web de Team Cymru(https://www.team-cymru.com/post/what-we-re-seeing-with-x-509-certificates-and-why-you-should-worry).

Selon les dossiers d'achat en ligne, la plateforme Augury met à la disposition de ses utilisateurs un large éventail de différents types de données Internet. Elles comprennent les données de capture de paquets (PCAP "pour «*packet capture*») liées aux protocoles de messagerie, de bureau à distance et de partage de fichiers. Le PCAP fait généralement référence à une capture complète des données et englobe des informations très détaillées sur l'activité du réseau. Ses données comprennent la requête envoyée d'un serveur à un autre, ainsi que la réponse de ce serveur.

Les données PCAP sont «tout ce qui existe», a déclaré Zach Edwards, un chercheur en cybersécurité qui a suivi de près le commerce des données, lors d'un entretien en ligne avec *Motherboard*. «Tout est là. Rien d'autre à capturer si ce n'est l'odeur de l'électricité». (Team Cymru a déclaré à *Motherboard* qu'il limitait effectivement les données renvoyées aux utilisateurs, mais n'a pas précisé quelles données étaient effectivement fournies à un utilisateur de la plateforme).

Une source dans le secteur de la cybersécurité a déclaré «c'est de la folie» lorsqu'on lui a montré que des informations sensibles comme les données PCAP étaient disponibles sur Augury. Certains utilisateurs de l'industrie privée semblent avoir moins accès à certains types de données dans Augury que ceux répertoriés dans les dossiers de marchés publics. *Motherboard* a accepté que plusieurs sources de cet article s'exprime sous couvert d'anonymat parce qu'elles n'étaient pas autorisées par leurs employeurs à aborder cette question.

Reconnaissance vidéo (IMAGE: SHUTTERSTOCK REMIX: JASON KOEBLER)

Selon les dossiers de passation de marchés, les données d'Augury peuvent également inclure l'activité d'un navigateur web, comme les URL visitées et l'utilisation des cookies. Les cookies sont des fichiers sensibles que les sites web déposent sur les ordinateurs lorsque les internautes les visitent. Étant donné leur caractère unique, les cookies peuvent être efficaces pour le suivi. Facebook et Google, par exemple, utilisent les cookies pour suivre un utilisateur particulier d'un site Web à l'autre et suivre son activité.

La NSA s'est ensuite appuyée sur ces cookies (https://www.washingtonpost.com/news/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/) pour identifier des cibles à pirater. Des captures d'écran obtenues par *Motherboard* semblent montrer des résultats contenant des cookies, des URL visitées et des données de messagerie. *Motherboard* a montré une partie de l'une des captures d'écran à plusieurs sources connaissant l'outil, et ces dernières ont confirmé qu'il s'agissait bien du panneau Augury.

Augury contient également ce que l'on appelle des données de flux net, qui créent une image du flux et du volume du trafic sur un réseau. Ces données peuvent indiquer quel serveur a communiqué avec quel autre, ce qui est une information qui n'est normalement disponible que pour le propriétaire du serveur lui-même ou pour le fournisseur d'accès Internet qui achemine le trafic.

Ces données de flux net peuvent être utilisées pour suivre le trafic à travers les réseaux privés virtuels et montrer le serveur à partir duquel ils se connectent finalement. De multiples sources dans le secteur de la cybersécurité ont déclaré à *Motherboard* que les données netflow peuvent être utiles pour identifier l'infrastructure utilisée par les pirates.

Team Cymru obtient ces données de flux net auprès des FAI; en retour, la compagnie fournit aux FAI des renseignements sur les menaces. Ce transfert de données se fait probablement sans le consentement éclairé des utilisateurs des FAI. Une source familière avec les données netflow a précédemment déclaré à *Motherboard* que «les utilisateurs ne [savent] certainement pas» que leurs données sont fournies à Team Cymru, qui en vend ensuite l'accès.

On ne sait pas exactement comment Team Cymru obtient le PCAP et d'autres informations plus sensibles, que ce soit auprès des FAI ou par une autre méthode. *Motherboard* a demandé à plusieurs reprises à Team Cymru si Augury contenait des cookies, des URL visitées et des données PCAP, comme le montrent les dossiers d'achat.

Team Cymru n'a pas répondu directement à la question, et à la place, a répondu dans un courriel que «la plateforme Augury n'est pas conçue pour cibler des utilisateurs spécifiques ou l'activité des utilisateurs. La plateforme ne possède pas sur les abonnés les informations spécifiques qui seraient nécessaires pour relier les enregistrements à un quelconque utilisateur».

«Notre plateforme ne fournit pas d'informations sur les utilisateurs ou les abonnés, et elle ne fournit pas de résultats qui montrerait un quelconque mode de vie, ce qui empêche sa capacité à être utilisée pour cibler des individus. Notre plateforme ne capture qu'un échantillon limité des données disponibles, et est encore plus restreinte en n'autorisant que

des requêtes sur des données limitées et à échantillon restreint, qui proviennent toutes de logiciels malveillants, d'activités malveillantes, de pots de miel [Type de piège employé par les spécialistes de la sécurité pour détecter les attaques ou prélever des échantillons de malwares, NdT], de scans et de tiers qui fournissent des flux de ces mêmes données. Les résultats sont alors encore plus limités quant à la portée et au volume de ce qui est renvoyé», a déclaré Team Cymru dans un autre courriel.

Une capture d'écran d'Augury obtenue par Motherboard (Image: Motherboard)

Cependant, il est arrivé que les données de Team Cymru soient utilisées dans le cadre d'enquêtes visant à identifier des ordinateurs spécifiques pour ensuite contacter la personne qui les utilise. En juillet 2021, des chercheurs du Citizen Lab ont publié un rapport (https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/) sur le fournisseur israélien de logiciels espions Candiru. Dans ce rapport, les chercheurs ont expliqué qu'ils avaient utilisé les données de Team Cymru pour identifier un ordinateur qui, selon eux, avait été infecté par le logiciel malveillant de Candiru, et qu'ils avaient ensuite contacté le propriétaire de cet ordinateur. Citizen Lab n'a pas répondu à une demande de commentaire.

Le dossier d'achat qui indique qu'Augury a accès aux données PCAP, aux URL visitées et aux cookies concerne la maintenance d'un achat de l'outil par le ministère de la Marine. D'autres données d'approvisionnement consultées par *Motherboard* montrent que le ministère de la Marine a payé pour une licence Augury "Platinum".

Au-delà de cela, il n'est pas clair quels clients du gouvernement américain de Team Cymru ont accès aux données plus sensibles telles que les cookies. Les dossiers de l'armée, du Cyber Command et de la Defense Counterintelligence and Security Agency ne mentionnent pas explicitement le niveau "platine", mais dans certains cas, le montant payé par les agences est le même que celui payé par la Navy pour une licence platine.

VIDEO (https://youtu.be/vEFpAlSaCv4)

Ces ventes au gouvernement américain ont été réalisées par l'intermédiaire d'une société appelée Argonne Ridge Group, dont *Motherboard* a découvert qu'elle partageait une adresse avec Team Cymru. Team Cymru a déclaré dans un courriel que Argonne Ridge Group est une filiale de Team Cymru qui a historiquement géré des contrats avec des agences gouvernementales.

Bien qu'ils ne mentionnent pas explicitement Augury, *Motherboard* a trouvé de multiples contrats entre Argonne Ridge Group et le FBI et les services secrets. L'un des contrats du FBI stipule qu'«il obtiendra l'approbation du financement pour acheter le flux net d'un fournisseur commercial et l'intégrer dans les sources existantes de flux net disponibles pour les analystes du cyber-renseignement afin de les analyser comme une preuve de concept». Les services secrets n'ont pas répondu aux multiples demandes de commentaires. Le FBI n'a pas fourni de réponse à temps pour pouvoir être publiée ici.

L'armée n'a pas été en mesure de fournir une déclaration sur les achats de la plate-forme Augury à temps pour la publication. Après avoir initialement accusé réception de la demande de commentaire de *Motherboard*, la Defense Counterintelligence and Security Agency s'en est remise au ministère de la Défense.

Cibles (IMAGE: CATHRYN VIRGINIA)

Charles E. Spirtos, du bureau d'information de la Marine, a déclaré à *Motherboard* dans un courriel que le NCIS «mène des enquêtes et conduit des opérations conformément à toutes les lois et réglementations applicables. L'utilisation des données de flux net par le NCIS ne nécessite pas de mandat». Spirtos a ajouté que le NCIS n'a pas utilisé les données de flux net au cours d'une enquête criminelle, mais que «le NCIS utilise les données de flux net pour divers objectifs de contre-espionnage».

En ce qui concerne le lanceur d'alerte, lequel a, selon le sénateur Wyden, contacté son bureau, sa plainte concerne, selon *Motherboard,* spécifiquement le contrat d' Argonne Ridge Group avec le NCIS. «Le NCIS déjouera les menaces provenant de l'ensemble du spectre du renseignement étranger, du terrorisme et de la criminalité en menant des opérations et des enquêtes sur terre, sur mer et dans le cyberespace, afin de protéger et de préserver la supériorité des combattants de la Marine et du Corps des Marines», peut-on lire sur le site Web du NCIS.

Dans sa lettre adressée aux départements de surveillance du DHS, du DoJ et du DoD, le sénateur Wyden écrit que «mon bureau a récemment été contacté par un lanceur d'alerte qui a décrit une série de plaintes officielles qu'il a déposées en amont et en aval de sa chaîne de commandement, ainsi qu'auprès de l'inspecteur général du DoD et de la Defense Intelligence Agency, concernant l'achat et l'utilisation sans mandat de données de flux net par le Naval Criminal Investigative Service (NCIS)».

« Tout comme les utilisateurs de Tor, les développeurs, les chercheurs et les fondateurs qui ont rendu Tor possible constituent un groupe diversifié de personnes. Mais toutes les personnes qui se sont engagées dans ce projet sont unies par une conviction commune: les utilisateurs d'Internet devraient avoir un accès privé à un web non censuré », peut-on lire sur le site du projet Tor.(https://www.torproject.org/about/history/)

Interrogée par *Motherboard* en avril sur la position de Thomas au sein du conseil d'administration du Projet Tor tout en étant également le PDG d'une entreprise qui vend une capacité d'attribution de l'activité sur Internet, Isabela Bagueros, directrice exécutive du Projet Tor, a déclaré dans un courriel que «les conflits d'intérêts potentiels de Rabbi Rob ont été examinés conformément au processus standard de divulgation des conflits d'intérêts requis de tous les membres du conseil d'administration. Sur la base de la connaissance de son travail avec Team Cymru, le conseil n'a pas identifié de conflits d'intérêts».

Le lanceur d'alerte allègue que le NCIS achète des données de Team Cymru qui comprennent à la fois «des enregistrements de flux de réseau et certains contenus de communication», poursuit la lettre. «Le lanceur d'alerte a informé mon bureau que sa plainte avait été transmise par l'inspecteur général du ministère de la Défense à l'inspecteur général de la Marine».

Faisant référence aux divers contrats du gouvernement américain pour l'accès à Augury, que son bureau a également examinés, le sénateur Wyden demande dans sa lettre aux branches de surveillance du DHS, du DoJ et du DoD d'

«enquêter sur l'achat et l'utilisation sans mandat des enregistrements de navigation Internet des Américains par les agences sous vos juridictions. Votre surveillance indépendante doit garantir que les activités de surveillance du gouvernement soient conformes à la décision de la Cour suprême dans l'affaire Carpenter et qu'elles protègent les droits des Américains selon le quatrième amendement».

Le secrétaire à la Défense Lloyd Austin repartant après avoir pris la parole lors d'un point presse au Pentagone, mercredi 20 juillet 2022, à Washington (Photo: Alex Brandon (AP))

Le bureau de l'inspecteur général du ministère de la défense, qui, selon le lanceur d'alerte, a transmis la plainte à la marine, a déclaré à *Motherboard* qu'il avait reçu la lettre de M. Wyden et que celle-ci était en cours d'examen. Le bureau de l'inspecteur général de la marine a refusé de commenter et a renvoyé *Motherboard* à son homologue du ministère de la défense.

En plus de son travail quotidien en tant que PDG de Team Cymru, le rabbin Rob Thomas siège également au conseil d'administration du projet Tor, une ONG de protection de la vie privée qui gère le logiciel Tor. Ce logiciel est le pilier du système d'anonymat Tor, un ensemble de milliers de serveurs (https://metrics.torproject.org/networksize.html) gérés par des bénévoles qui permettent à tout le monde de naviguer anonymement sur Internet.

Motherboard a précédemment révélé d'autres achats de données par l'armée américaine. En 2020, on a découvert qu'une application de prière musulmane (https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x) téléchargée plus de 98 millions de fois vendait ses données de localisation à un courtier appelé X-Mode. X-Mode, à son tour, comptait des entrepreneurs de l'armée américaine parmi ses clients.

Dans le cadre de cette enquête, *Motherboard* a également découvert que le Commandement des opérations spéciales des États-Unis avait acheté Locate X, un outil de surveillance basé sur les données de localisation recueillies auprès d'applications courantes. En mars dernier, *Motherboard* a rapporté qu'une unité militaire qui effectue des frappes de drones avait également acheté Locate X (https://www.vice.com/en/article/y3g97x/location-data-apps-drone-strikes-iowa-national-guard).

Après la publication de certains de ces résultats par *Motherboard*, le sénateur Wyden a demandé au ministère de la défense de lui fournir davantage d'informations sur ses achats de données. Certaines des réponses de l'agence ont été données sous une forme qui ne permettait pas au bureau de Wyden de publier légalement des détails sur la surveillance ; une réponse en particulier était classifiée.

C'est la raison pour laquelle Wyden a écrit dans une deuxième lettre en mai 2021 à l'agence (https://www.vice.com/en/article/88ng8x/pentagon-americans-surveillance-without-warrant-internet-browsing): «Je vous écris pour vous demander instamment de rendre publiques les informations relatives à la surveillance sans mandat des Américains par le ministère de la défense (DoD)», suggérant que le Pentagone est engagé dans une telle surveillance. À l'époque, le bureau de M. Wyden a refusé de fournir à *Motherboard* des détails sur la réponse confidentielle. Mais un assistant de M. Wyden a déclaré que la question portait sur l'achat de métadonnées Internet par le ministère de la Défense.

En août, la Chambre des représentants a approuvé des modifications au budget militaire de l'année prochaine qui obligeraient le ministère de la Défense à commencer à divulguer tout achat de données relatives à la navigation sur Internet ou aux smartphones qui nécessiterait normalement un mandat, a rapporté *Gizmodo* à l'époque (https://gizmodo.com/pentagon-budget-force-data-purchase-disclosure-ndaa-1849432085). Cette proposition doit encore être approuvée par le Sénat.

D'autres entreprises de cybersécurité rassemblent également des ensembles de données controversés. En 2020, *Motherboard* a rapporté que HYAS, une société de renseignement sur les menaces, s'est procuré des données de localisation afin de suivre les gens jusque sur le «pas de leur porte».