Facebook bannit de ses plateformes sept compagnies Â« cyber-mercenaires Â»

Description

Le 16 dÃ©cembre 2021, par Stephanie Kirchgaessner et Michael Safi

La compagnie va aussi envoyer des avertissements Ã 48 000 personnes qui, aprÃ¨s enquÃªte, pourraient avoir Ã©tÃ© visÃ©es par une activitÃ© malveillante en ligne

Lâ??enquÃªte menÃ©e par Facebook arrive alors que la compagnie doit elle-mÃªme faire face Ã un examen intense Ã Washington et dans le monde. Photographe : Olivier Douliery/AFP/Getty Images

AprÃ¨s une investigation de plusieurs mois dans lâ??industrie Â« cyber-mercenaire Â», Facebook a banni sept compagnies de Â« surveillance pour le compte dâ??autrui Â» de ses plateformes et enverra des avertissements Ã 48 000 personnes dont la compagnie pense quâ??elles ont Ã©tÃ© visÃ©es par une activitÃ© malveillante en ligne.

La compagnie de rÃ©seau social a dit jeudi [16 dÃ©cembre] que son enquÃªte a rÃ©vÃ©lÃ© de nouveaux dÃ©tails sur la maniÃ¨re dont les compagnies de surveillance permettent Ã leurs clients de cibler des personnes Â« de maniÃ¨re indiscriminÃ©e Â» sur tout internet, afin de rassembler des renseignements sur elles, de les manipuler â?? et finalement de compromettre leurs Ã©quipements.

Parmi les compagnies de surveillance que Facebook a nommÃ©es dans son enquÃªte et bannies de ses plateformes figurent :

- Black Cube, une compagnie israÃ©lienne qui est devenu fameuse lorsquâ??il est apparu quâ??Harvey Weinstein, magnat des mÃ©dias maintenant en disgrÃ¢ce et dÃ©linquant sexuel condamnÃ©, les avait engagÃ©s pour cibler des femmes qui lâ??avaient accusÃ© dâ??agression. Black Cube a rejetÃ© les affirmations de Facebook sur ses activitÃ©s.
- Cobwebs, une autre compagnie israÃ©lienne dont Facebook a dit quâ??elle permettait Ã ses clients dâ??utiliser des sites web publics et des sites du dark web pour tromper leurs cibles et leur faire rÃ©vÃ©ler des informations personnelles. La compagnie aurait aussi travaillÃ© pour des clients aux Ã?tats-Unis, dont un dÃ©partement de la police locale Ã Hartford, dans le Connecticut.
- Cytrox, une entreprise de la MacÃ©doine du Nord dont Facebook a dit quâ??elle permettait Ã ses clients dâ??infecter des cibles avec des logiciels malveillants aprÃ¨s des campagnes de phishing.

Lâ??enquÃªte menÃ©e par Facebook arrive alors que la compagnie doit elle-mÃªme faire face Ã un examen intense Ã Washington et dans le monde, aprÃ¨s les accusations dâ??une lanceuse dâ??alerte, Frances Haugen, selon lesquelles la compagnie faciliterait les discours de haine et la dÃ©sinformation.

Lâ??enquÃªte de Facebook est nÃ©anmoins importante parce quâ??elle rÃ©vÃ¨le de nouveaux dÃ©tails sur la maniÃ¨re dont des parties de lâ??industrie de surveillance utilisent les rÃ©seaux sociaux â?? de Facebook Ã Instagram â?? pour crÃ©er de faux comptes afin de tromper leurs cibles et de cacher leurs propres activitÃ©s.

Alors que beaucoup de compagnies affirment quâ??elles sont employÃ©es pour viser des criminels et des terroristes, Facebook a dit que lâ??industrie permet Â« rÃ©guliÃ¨rement Â» Ã ses clients de cibler des journalistes, des dissidents, des critiques des rÃ©gimes autoritaires et des militants pour la dÃ©fense des droits humains ainsi que leurs familles.

Â« Notre espoir est de contribuer Ã une comprÃ©hension plus large des maux que cette industrie reprÃ©sente dans le monde entier et dâ??appeler les gouvernements dÃ©mocratiques Ã prendre dâ??autres mesures pour aider Ã la protection des personnes et pour imposer un contrÃ´le sur les vendeurs de logiciels espions rÃ©pandus Â», a dit la compagnie. Elle a ajoutÃ© quâ??elle nâ??avait pas seulement Ã©liminÃ© de ses plateformes les faux comptes des compagnies, mais quâ??elle avait aussi Ã©mis des ordonnances de cesser et de sâ??abstenir et quâ??elle travaillerait Ã garantir que les compagnies ne cherchent pas Ã se rÃ©inscrire sur ses plateformes.

Facebook a dit que les 48 000 personnes qui recevront des avertissements nâ??ont pas toutes Ã©tÃ© piratÃ©es, mÃªme si la compagnie croit effectivement quâ??ils ont Ã©tÃ© sujets Ã une Â« activitÃ© malveillante Â».

Elle a aussi soulignÃ© lâ??attention intense portÃ©e rÃ©cemment par les mÃ©dias, lors dâ??investigations par le *Guardian* et dâ??autres organes de presse, sur le groupe NSO, le fabricant israÃ©lien de logiciels espions qui Ã©tait au cÅ?ur du Projet Pegasus et a Ã©tÃ© rÃ©cemment mis sur liste noire par lâ??administration Biden. WhatsApp, qui appartient Ã la compagnie mÃ¨re de Facebook, Meta, a intentÃ© un procÃ¨s contre NSO en 2019 et a Ã©tÃ© un critique majeur de la compagnie. NSO ne fait pas partie des compagnies bannies jeudi.

Â« Il est important de comprendre que NSO nâ??est quâ??une piÃ¨ce dans un Ã©cosystÃ¨me cyber-mercenaire mondial plus large Â», a dit Facebook.

Alors que Facebook annonÃ§ait son enquÃªte, des chercheurs de pointe au Citizen Lab de lâ??UniversitÃ© de Toronto ont publiÃ© un nouveau rapport qui se concentrait sur une entitÃ© â?? Cytrox â?? dont le logiciel espion, appelÃ© Predator, aurait Ã©tÃ© utilisÃ© par un client inconnu pour pirater les Ã©quipements de deux individus.

Lâ??un dâ??eux, Ayman Nour, est un politicien Ã©gyptien en exil qui, selon Citizen Lab, sâ??est trouvÃ© avoir Ã©tÃ© simultanÃ©ment piratÃ© par deux Ã?tats nationaux clients distincts, lâ??un utilisant Predator et lâ??autre utilisant Pegasus. Nour, qui est basÃ© en Turquie, est le prÃ©sident dâ??un groupe dâ??opposition politique Ã©gyptien appelÃ© lâ??Union des forces nationales Ã©gyptiennes et il a Ã©tÃ© candidat Ã une Ã©lection prÃ©sidentielle contre lâ??ancien prÃ©sident Hosni Mubarak.

Ayman Nour parle aux mÃ©dias Ã Istanbul, en Turquie, de la disparition de Jamal Khashoggi en 2018. Photographe : Anadolu Agency/Getty Images

AprÃ¨s sa campagne, il a Ã©tÃ© emprisonnÃ© pendant quatre ans sur des allÃ©gations â?? considÃ©rÃ©es comme Ã©tant politiquement motivÃ©es â?? de falsification de signatures pour des pÃ©titions. Il a Ã©tÃ© libÃ©rÃ© aprÃ¨s des pressions internationales. Il Ã©tait aussi un collaborateur de Jamal Khashoggi, le journaliste du *Washington Post* qui a Ã©tÃ© assassinÃ© par des agents saoudiens au consulat saoudien en 2018.

Dans un interview avec le *Guardian*, Nour a dit que câ??Ã©tait douloureux dâ??apprendre quâ??il avait Ã©tÃ© piratÃ©.

Â« Cela a eu un impact psychologique nÃ©gatif sur moi. Mes gosses vivent au Royaume-Uni et aux Ã?tats-Unis et je vis dans un troisiÃ¨me pays, la Turquie, donc Ã©tant sÃ»r que jâ??Ã©tais espionnÃ©, jâ??ai cessÃ© de communiquer avec mes fils, parce que jâ??ai peur pour eux Â», a-t-il dit.

Nour a dit quâ??il avait participÃ© Ã un meeting par zoom avec des Egyptiens, des Saoudiens et des Emiratis dans le cadre dâ??une discussion sur lâ??utilisation de la peine de mort dans les pays arabes le jour oÃ¹ les chercheurs ont appris ultÃ©rieurement quâ??il avait Ã©tÃ© piratÃ©.

Une deuxiÃ¨me cible, qui est restÃ©e anonyme, a Ã©tÃ© dÃ©crite par Citizen Lab comme un journaliste en exil, ouvertement critique du rÃ©gime dâ??Abdel Fatah al-Sisi.

Cytrox nâ??a pas immÃ©diatement rÃ©pondu Ã notre demande de commentaire.

Des analyses internes de Citizen Lab ont dÃ©couvert des clients probables de Predator en ArmÃ©nie, en Egypte, en GrÃ¨ce, en IndonÃ©sie, Ã Madagascar, Ã Oman, en Arabie saoudite et en Serbie.

Cytrox ferait partie dâ??Intellexa, Â« lâ??Alliance star Â» des logiciels espions qui a Ã©tÃ© formÃ©e pour concurrencer NSO et se dÃ©crit sur son site web comme Ã©tant basÃ©e et rÃ©glementÃ©e aux

Ã?tats-Unis. Intellexa nâ??a pas rÃ©pondu Ã notre demande de commentaire.

Un porte-parole de NSO a dit quâ??il nâ??avait pas vu le rapport de Citizen Lab mais que les affirmations Ã©taient Â« technologiquement et contractuellement illogiques Â» parce que lâ??Egypte est sur une liste de Â« non-vente Â» pour NSO, nâ??Ã©tait pas un client et Â« nâ??en serait jamais un Â».

Â« Lâ??utilisation dâ??outils Ã©lectroniques pour surveiller des dissidents, des activistes et des journalistes est une mauvaise utilisation grave de toute technologie et va contre lâ??usage souhaitÃ© de tels outils critiques. La communautÃ© internationale devrait avoir une politique de tolÃ©rance zÃ©ro envers de tels actes, donc une rÃ©gulation globale est nÃ©cessaire. La compagnie NSO a prouvÃ© dans le passÃ© quâ??elle avait une tolÃ©rance zÃ©ro pour ces types de mauvais usages, en mettant fin Ã des contrats Â», a dit le porte-parole.

Des rapports prÃ©cÃ©dents du Projet Pegasus ont montrÃ© que NSO avait prÃ©cÃ©demment conservÃ© certains clients, dont les Emirats arabes unis, malgrÃ© des allÃ©gations dâ??abus. La compagnie a quant Ã elle indiquÃ© avoir coupÃ© les liens avec certains clients, dont lâ??Arabie saoudite et les Emirats arabes unis, aprÃ¨s des allÃ©gations dâ??abus.

Citizen Lab a dit que Cytrox aurait commencÃ© comme une startup en MacÃ©doine du Nord et que lâ??entreprise est prÃ©sente en IsraÃ«l et en Hongrie.

Dans son rapport, Facebook a dit Ã©liminer 300 comptes sur Facebook et Instagram liÃ©s Ã Cytrox. La compagnie a dit que les enquÃªtes avec Citizen Lab avaient dÃ©couvert une Â« vaste infrastructure de domaines Â» quâ??elle pensait utilisÃ©s par Cytrox pour usurper des entitÃ©s dâ??informations authentiques dans les pays qui les intÃ©ressaient.

Dans son rapport sur les menaces, Facebook a dÃ©crit trois Ã©tapes que les clients de la plupart des compagnies sous investigation utilisent pour viser des individus. Dâ??abord, lâ??Ã©tape de la reconnaissance, qui inclut Â« la surveillance Ã distance Â» pour discerner les intÃ©rÃªts individuels. Suit ce que Facebook appelle une Â« Ã©tape dâ??engagement Â», dans lequel les clients des compagnies Ã©tablissent alors le contact avec les cibles et essaient de bÃ¢tir de la confiance, de solliciter de lâ??information et de les Â« tromper Â» pour quâ??ils cliquent sur des liens et tÃ©lÃ©chargent des documents.

Enfin, Facebook a dit que lâ??Ã©tape finale implique Â« le piratage pour le compte dâ??autrui Â» dans lequel des individus sont piratÃ©s ou ciblÃ©s par des programmes malveillants. La compagnie a dit quâ??il Ã©tait important de se concentrer sur les deux premiÃ¨res Ã©tapes de la surveillance invasive (qui ont reÃ§u moins dâ??attention dans les rapports des mÃ©dias) et de les interrompre.

Dans le cas de Black Cube, Facebook a dit avoir Ã©liminÃ© 300 comptes Facebook et Instagram liÃ©s Ã la compagnie.

Â« Black Cube a exploitÃ© des personnages fictifs taillÃ©s pour ses cibles : certains dâ??entre eux se sont fait passer pour des Ã©tudiants diplÃ´mÃ©s, des travailleurs dâ??ONG et de dÃ©fense des droits humains et des producteurs de film ou de tÃ©lÃ©vision Â», a dit Facebook.

Dans une dÃ©claration, Black Cube â?? qui sâ??est excusÃ© publiquement pour son travail pour Weinstein â?? a dÃ©clarÃ© : Â« Black Cube ne rÃ©alise aucun phishing ou piratage et nâ??opÃ¨re pas dans le cybermonde. Black Cube est une sociÃ©tÃ© de soutien pour des recours en justice, qui utilise des mÃ©thodes dâ??investigation lÃ©gales Humint afin dâ??obtenir de lâ??information pour des contentieux et des arbitrages. Black Cube travaille avec des firmes juridiques de premier plan dans le monde pour prouver des pots-de-vin, dÃ©voiler la corruption et rÃ©cupÃ©rer des centaines de millions dâ??actifs volÃ©s. Black Cube demande des conseils juridiques dans toute juridiction dans laquelle nous opÃ©rons afin de garantir que toutes les activitÃ©s de nos agents sont totalement conformes aux lois locales. Â»

Dâ??autres entitÃ©s bannies par Facebook incluent : Cognyte, Bluehawk CI, BellTroX et ce qui a Ã©tÃ© dÃ©crit comme une Â« entitÃ© inconnue Â» en Chine qui, dit Facebook, Ã©tait responsable de ciblage malveillant et semble avoir Ã©tÃ© utilisÃ©e pour lâ??application des lois intÃ©rieures en Chine. Le logiciel malveillant dÃ©ployÃ© par le groupe Ã©tait utilisÃ© contre des groupes des minoritÃ©s dans le Xinjiang, au Myanmar et Ã Hong Kong.

BellTroX nâ??a pas pu Ãªtre atteint pour commenter. Un porte-parole de Cobwebs a dit Ã Reuters que la compagnie sâ??appuyait sur des sources ouvertes et que ses produits Â« ne sont en aucune faÃ§on intrusifs Â». Les autres entitÃ©s nommÃ©es par Facebook nâ??ont pas rÃ©pondu Ã nos demandes de commentaires.

Traduction CG pour lâ??Agence MÃ©dia Palestine

Source : The Guardian

date crÃ©Ã©e
2021/12/28