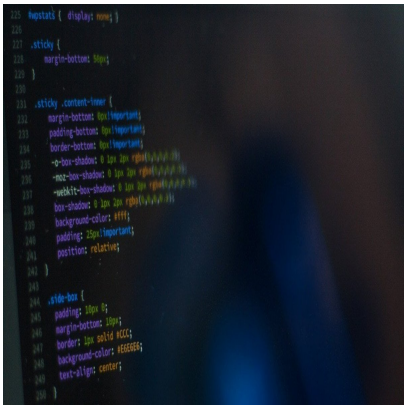
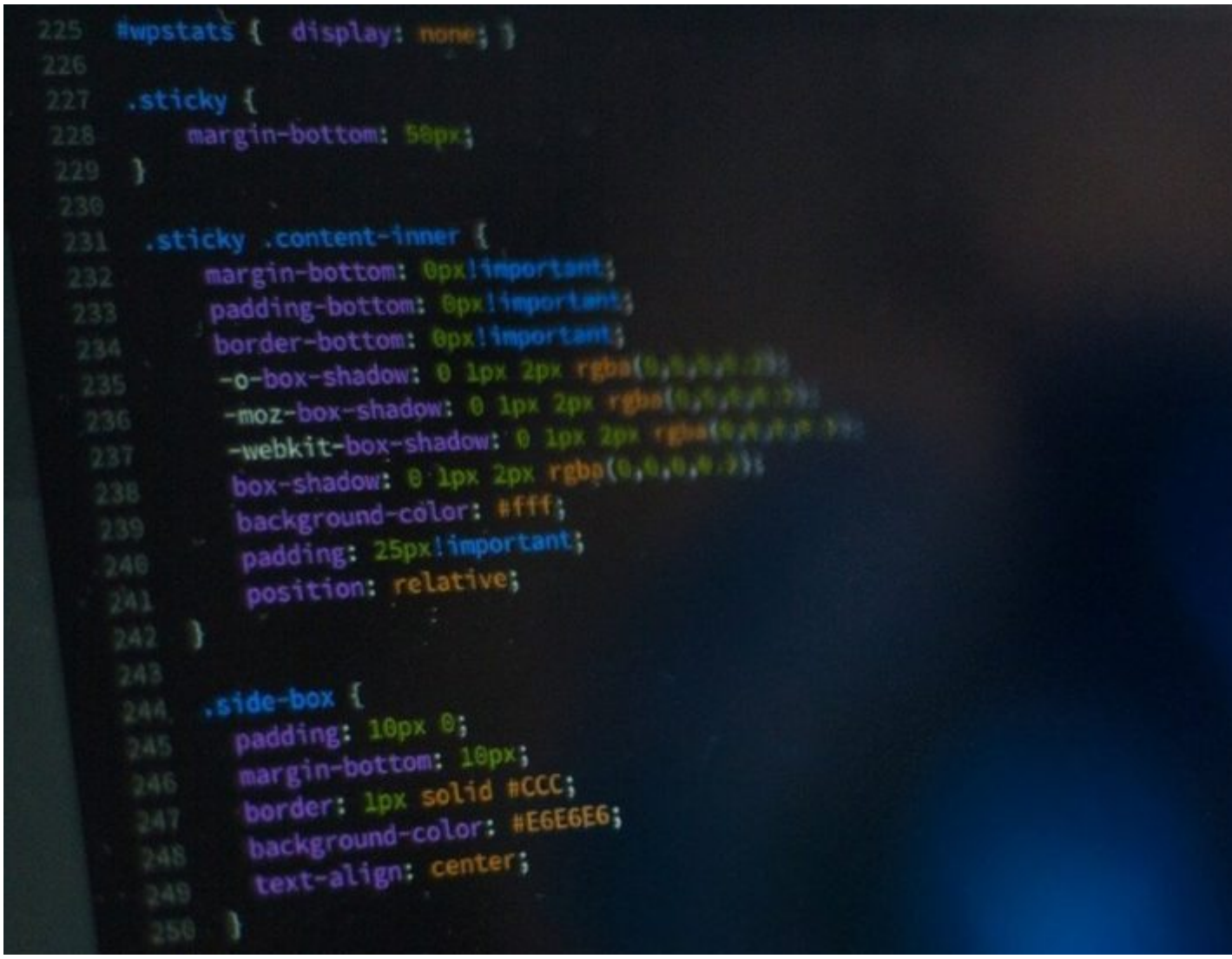


Â« Cyber Mercenaires Â» : lâ??industrie israÃ©lienne des logiciels espions est critiquÃ©e dans le monde entier

Description

Le 21 dÃ©cembre, par Sagi Cohen pour le Haaretz

La mise sur liste noire des Ã?tats-Unis et les rapports cinglants de Google et de Meta, propriÃ©taire de Facebook, ne sont que quelques-unes des mesures prises Ã lâ??encontre des entreprises israÃ©liennes qui ne sont pas correctement supervisÃ©es par les agences nationales.



Ã? premiÃ¨re vue, la startup israÃ©lienne Cobwebs Technologies semble Ãªtre une cyberentreprise comme les autres. Sur son site Web, la firme dÃ©clare fiÃ¨rement quâ??elle est Â« un leader mondial de lâ??intelligence web. Â» En 2019, lorsquâ??elle a annoncÃ© avoir levÃ© 10 millions de dollars, lâ??entreprise a affirmÃ© avoir dÃ©veloppÃ© un moteur de recherche pour les informations de renseignement et a dÃ©clarÃ© vouloir Ãªtre le Â« Google du renseignement. Â»

Au dÃ©but de la crise du coronavirus, Cobwebs a annoncÃ© quâ??elle avait dÃ©veloppÃ© un produit permettant de prÃ©dire la propagation de la pandÃ©mie, et sâ??est mÃªme vantÃ©e de travailler avec lâ??Administration pour le dÃ©veloppement des armes et des infrastructures technologiques du ministÃ¨re de la DÃ©fense.

Mais le rapport publiÃ© jeudi par Meta, la sociÃ©tÃ© mÃ¨re de Facebook, expose un Ã©lÃ©ment plus secret des activitÃ©s de lâ??entreprise. Le rapport dÃ©crit Cobwebs, trois autres sociÃ©tÃ©s israÃ©liennes et trois entitÃ©s dâ??Inde, de Chine et de MacÃ©doine du Nord comme des Â« cyber mercenaires Â».

Selon Meta, Cobwebs active pour ses clients des comptes contrefaits qui effectuent une surveillance en ligne, notamment sur des rÃ©seaux sociaux tels que Facebook, Instagram, WhatsApp et Twitter.

Par exemple, les clients peuvent collecter des informations sur des activistes, des politiciens et des reprÃ©sentants gouvernementaux dans le monde entier.

Les comptes contrefaits rejoignent Ã©galement des communautÃ©s et des forums, incitant les gens Ã rÃ©vÃ©ler des donnÃ©es personnelles et piratant ensuite les tÃ©lÃ©phones ou les ordinateurs des cibles. Cobwebs a des clients aux Ã?tats-Unis, mais aussi au Bangladesh, en Arabie saoudite et ailleurs.

Le rapport de Meta Ã©tait tout sauf circonspect. Il nomme les sociÃ©tÃ©s israÃ©liennes Cobwebs, Cognyte, Bluehawk et Black Cube, ainsi que la sociÃ©tÃ© Cytrox de MacÃ©doine du Nord (qui appartient apparemment Ã IsraÃ«l), la sociÃ©tÃ© BellTroX basÃ©e en Inde et Â« une entitÃ© inconnue en Chine Â». Ils sont dÃ©crits comme appartenant Ã une Â« industrie mondiale de surveillance pour le compte de tiers Â» dont les mÃ©thodes sont similaires Ã celles de la sociÃ©tÃ© israÃ©lienne NSO Group Technologies.

Â« Compte tenu de la gravitÃ© de leurs violations, nous les avons bannis de nos services Â», Ã©crit Meta. Â« Nous avons Ã©galement alertÃ© environ 50 000 personnes qui, selon nous, Ã©taient visÃ©es par ces activitÃ©s malveillantes dans le monde entier, en utilisant le systÃ¨me dâ??alerte que nous avons lancÃ© en 2015. Nous lâ??avons rÃ©cemment mis Ã jour pour fournir aux gens des dÃ©tails plus granulaires sur les types de ciblage et lâ??acteur derriÃ¨re eux, afin quâ??ils puissent prendre des mesures pour protÃ©ger leurs comptes, en fonction de la phase de la chaÃ®ne dâ??attaque de surveillance que nous dÃ©tectons dans chaque cas. Â»

Dans la plupart des cas, lâ??industrie de la cybersÃ©curitÃ© opÃ¨re sous le radar. Bien que la plupart des entreprises ne soient pas spÃ©cialisÃ©es dans les outils de piratage sophistiquÃ©s comme le NSO, les cibles et les mÃ©thodes sont similaires. Ces entreprises veillent Ã opÃ©rer dans une zone juridiquement grise et se considÃ¨rent comme des sociÃ©tÃ©s lÃ©gitimes de collecte de renseignements.

En effet, la collecte de renseignements par les pays et les entreprises est une pratique courante. Bien que certaines de ces entreprises affirment que leurs outils permettent de lutter contre le terrorisme ou la criminalitÃ©, Facebook met en lumiÃ¨re, par exemple, le piratage des appareils de journalistes, de militants des droits de lâ??homme et dâ??opposants au rÃ©gime dans une centaine de pays, y compris des pays non dÃ©mocratiques.

Dans le rapport, Meta ne discute pas des motifs des clients, mais il pourrait sâ??agir dâ??entreprises qui collectent des renseignements sur leurs concurrents, de rÃ©gimes qui surveillent leurs opposants et de personnes ou dâ??organisations qui recueillent des renseignements Ã des fins dâ??extorsion ou de rÃ©clamation juridique. Les PDG et les hommes politiques du monde entier peuvent demander Ã leurs collaborateurs de Â« trouver des saletÃ©s sur lui Â», qui contactent ensuite les fournisseurs israÃ©liens de logiciels espions.

Le rapport de Meta est rare ; lâ??entreprise ne descend pratiquement jamais Ã ce niveau de dÃ©tail. Les entreprises de cybersÃ©curitÃ© recueillent des renseignements en exploitant les plateformes dÃ©tenues par Meta â?? WhatsApp, Facebook et Instagram. Les enquÃªteurs de Meta peuvent ainsi identifier les cibles, les clients et le mode opÃ©ratoire.

Dans un premier temps, le faux compte prend contact avec la cible et la persuade dâ??engager une conversation et de fournir des informations telles que des coordonnÃ©es ou des mots de passe.

Dans un deuxiÃ¨me temps, un logiciel de surveillance est implantÃ© dans le tÃ©lÃ©phone ou lâ??ordinateur de la cible ; il peut sâ??agir dâ??un outil de cyberguerre sophistiquÃ© ou dâ??un simple produit du commerce. Dans tous les cas, il permet une surveillance totale de la vie numÃ©rique dâ??une personne. Les entreprises israÃ©liennes citÃ©es par Meta ont rÃ©alisÃ© lâ??une ou lâ??autre de ces Ã©tapes, voire les deux.

IngÃ©nierie sociale

Outre Cobwebs, Meta a Ã©galement nommÃ© Cognyte, lâ??entreprise dirigÃ©e par Elad Sharon qui a Ã©tÃ© sÃ©parÃ©e de la sociÃ©tÃ© israÃ©lienne Verint en 2019. Selon le rapport, Cognyte vend des outils permettant de gÃ©rer des comptes contrefaits sur les sites de mÃ©dias sociaux, de Facebook Ã YouTube en passant par le site russe Vkontakte. Ces outils, selon Meta, permettent aux clients Â« de faire de lâ??ingÃ©nierie sociale et de collecter des donnÃ©es. Â»

En dâ??autres termes, ils amÃ¨nent la victime, par exemple, Ã rÃ©vÃ©ler des informations sensibles ou Ã cliquer sur un lien malveillant. Les clients de Cognyte sont situÃ©s dans des pays tels quâ??IsraÃ«l, la Colombie, le Kenya, le Maroc, la Jordanie et lâ??IndonÃ©sie. Parmi les cibles : des journalistes et des hommes politiques.

Black Cube, une sociÃ©tÃ© dâ??intelligence Ã©conomique dirigÃ©e par Dan Zorella, connaÃ®t dÃ©jÃ la controverse. Selon Meta, la sociÃ©tÃ© permet Ã ses clients de se faire passer pour dâ??autres personnes et dâ??obtenir lâ??adresse Ã©lectronique dâ??une personne Ã des fins dâ??hameÃ§onnage.

Des cibles ont Ã©tÃ© identifiÃ©es dans lâ??industrie mÃ©dicale, lâ??exploitation miniÃ¨re, lâ??Ã©nergie et parmi les groupes Ã but non lucratif. Parmi les autres cibles figurent des activistes palestiniens, des personnes travaillant dans les mÃ©dias russes, ainsi que des experts dans le monde universitaire, la haute technologie et la finance.

Bluehawk, dirigÃ© par Guy Klisman, un ancien de la division de recherche du renseignement militaire israÃ©lien, propose des options dâ??espionnage comprenant la collecte dâ??informations lÃ©gales et la gestion de faux comptes destinÃ©s Ã persuader les gens dâ??installer des logiciels malveillants. Une pratique courante consiste Ã se faire passer pour un journaliste. Parmi les victimes figurent des hommes politiques et des hommes dâ??affaires Ã©miratis et qataris.

Une autre entreprise mentionnÃ©e par Meta est Cytrox, basÃ©e en MacÃ©doine du Nord, qui dÃ©veloppe des outils de piratage similaires Ã ceux de NSO. Selon un rapport de Citizen Lab, un groupe de recherche de lâ??UniversitÃ© de Toronto qui se concentre sur les abus des technologies de surveillance, Cytrox a des liens Ã©troits avec des organisations et des hommes dâ??affaires en IsraÃ«l. Selon un article de 2019 de Forbes, Cytrox a Ã©tÃ© rachetÃ© par lâ??IsraÃ©lien Tal Dillian, ancien commandant dâ??une unitÃ© technologique du renseignement militaire et dÃ©sormais entrepreneur en cyberguerre.

Meta sâ??attaque Ã IsraÃ«l ?

La collecte dâ??informations sur les utilisateurs, bien sÃ»r, est au cÅ?ur du modÃ¨le Ã©conomique de Meta, et la sociÃ©tÃ© contrÃ´lÃ©e par Mark Zuckerberg a Ã©tÃ© impliquÃ©e dans ses propres scandales de surveillance et de collecte dâ??informations, comme lâ??affaire Cambridge Analytica. Facebook a Ã©galement achetÃ© lâ??application israÃ©lienne Onavo qui permettait Ã Facebook de collecter des donnÃ©es sur les actions de ses utilisateurs.

Des sources proches de lâ??attaque de Cobwebs Meta . Â« Facebook a dâ??abord choisi de sâ??adresser aux mÃ©dias et nâ??a informÃ© les entreprises que plus tard. Sâ??ils Ã©taient vraiment prÃ©occupÃ©s par le bien-Ãªtre de leurs utilisateurs, ils auraient dâ??abord approchÃ© les entreprises et non les mÃ©dias, comme il est dâ??usage Â», a dÃ©clarÃ© une source.

Â« Cobwebs est une entreprise standard ; il y en a des dizaines comme elle dans le monde. Pas un seul de ses nombreux concurrents aux Ã?tats-Unis ou en Europe nâ??est mentionnÃ© dans le rapport, ce qui vous amÃ¨ne Ã la conclusion quâ??il sâ??agit dâ??une attaque bien orchestrÃ©e contre les entreprises israÃ©liennes dans le but de montrer que Meta protÃ¨ge ses utilisateurs. Â»

Entre-temps, les outils de surveillance numÃ©rique et les logiciels espions sont devenus un secteur dâ??exportation extrÃªmement populaire pour IsraÃ«l. Ces entreprises exploitent lâ??abondance dâ??informations amassÃ©es au fil des ans par les FDI dans les domaines de la cybernÃ©tique et du renseignement et les combinent avec des prouesses dans lâ??analyse de lâ??information et la publicitÃ© numÃ©rique. Elles sont donc fortes sur le plan technique, mais parfois moins sur le plan Ã©thique.

Il nâ??y a rien de nouveau dans le fait que des entreprises israÃ©liennes de haute technologie opÃ¨rent dans des zones grises lorsquâ??il sâ??agit de violer la vie privÃ©e et dâ??acquÃ©rir des donnÃ©es. Par exemple, la sociÃ©tÃ© de logiciels Glassbox a eu des problÃ¨mes avec Apple aprÃ¨s quâ??il a Ã©tÃ© rÃ©vÃ©lÃ© quâ??elle permettait Ã des applications dâ??enregistrer secrÃ¨tement les actions des utilisateurs dâ??iPhone.

De mÃªme, un module complÃ©mentaire de la sociÃ©tÃ© israÃ©lienne Similarweb a Ã©tÃ© bloquÃ© par le navigateur Chrome de Google parce quâ??il suivait la navigation des utilisateurs sur le web, tandis quâ??un module complÃ©mentaire VPN de la sociÃ©tÃ© israÃ©lienne Hola (de lâ??entitÃ© connue aujourdâ??hui sous le nom de Bright Data) a Ã©tÃ© accusÃ© Ã plusieurs reprises de violations de la vie privÃ©e et de la sÃ©curitÃ© des donnÃ©es â?? jusquâ??Ã ce quâ??il soit rÃ©cemment bloquÃ© et supprimÃ© par Chrome.

Mais les entreprises citÃ©es par Meta font de lâ??espionnage Ã un tout autre niveau. Il est trÃ¨s possible que ces entreprises ne tiennent pas compte du fait que les rÃ¨gles du jeu commencent Ã changer.

Le rapport de Meta sâ??inscrit dans une vague dâ??Ã©vÃ©nements montrant que la patience du secteur technologique Ã lâ??Ã©gard des sociÃ©tÃ©s dâ??espionnage est Ã bout. Les gÃ©ants de la technologie sont peut-Ãªtre eux-mÃªmes des empires de la collecte de renseignements, mais ils sont moins conciliants lorsquâ??il sâ??agit dâ??entreprises tierces israÃ©liennes qui exploitent leurs plates-formes pour effectuer de la surveillance et collecter des donnÃ©es sur leurs utilisateurs.

IsraÃ«l manque de supervision

De mÃªme, les gouvernements et les organismes de rÃ©glementation aux Ã?tats-Unis et en Europe commencent Ã se rendre compte quâ??il faut sâ??attaquer Ã ce phÃ©nomÃ¨ne. Â« Câ??est significatif, car cela montre que ce nâ??est pas le problÃ¨me dâ??une seule entreprise ou dâ??une poignÃ©e dâ??entreprises. Câ??est un problÃ¨me qui touche lâ??ensemble du secteur Â», a dÃ©clarÃ© Ã Bloomberg John Scott-Railton, chercheur principal au Citizen Lab.

La preuve en est ce qui est arrivÃ© ces derniers mois Ã NSO. Bien quâ??elle prÃ©tende travailler contre le terrorisme et la criminalitÃ©, elle a Ã©tÃ© poursuivie par Facebook et Apple, et lâ??administration amÃ©ricaine lui a infligÃ© des sanctions (ainsi quâ??Ã une autre sociÃ©tÃ© israÃ©lienne de cyberguerre, Candiru).

La semaine derniÃ¨re, Google a publiÃ© un rapport contenant des dÃ©tails sans prÃ©cÃ©dent sur les mÃ©thodes de Pegasus, lâ??outil de piratage dÃ©veloppÃ© par NSO. Selon les mÃ©dias Ã©trangers, tout cela a amenÃ© NSO Ã envisager de fermer ou de vendre ses opÃ©rations de cyberguerre.

Si ce processus devait sâ??aggraver, les industries israÃ©liennes de la cyberguerre et des logiciels espions, qui jouissent toujours dâ??une libertÃ© dâ??action, devront faire preuve dâ??une plus grande responsabilitÃ©, changer leur mode de fonctionnement, devenir plus transparentes, modifier leurs modÃ¨les commerciaux ou peut-Ãªtre mÃªme fermer leurs portes. Ce ne serait pas la premiÃ¨re fois ; la pression des gÃ©ants de la technologie a dÃ©jÃ dÃ©truit une industrie entiÃ¨re qui sâ??Ã©tait dÃ©veloppÃ©e en IsraÃ«l : des barres dâ??outils invasives qui prenaient le contrÃ´le des navigateurs et des ordinateurs des gens. De nombreuses entreprises israÃ©liennes ont dÃ» fermer leurs portes ou changer de direction.

Pourtant, dâ??une maniÃ¨re ou dâ??une autre, toutes les pressions exercÃ©es sur les entreprises israÃ©liennes proviennent de gouvernements et de sociÃ©tÃ©s Ã©trangers. Mis Ã part les mÃ©dias et quelques groupes de la sociÃ©tÃ© civile, aucun ministÃ¨re, aucune agence ou aucun organisme de rÃ©glementation â?? ni les dÃ©partements qui supervisent les exportations au sein des ministÃ¨res de lâ??Ã©conomie et de la dÃ©fense, ni lâ??autoritÃ© de protection de la vie privÃ©e, ni la direction nationale du cyberespace â?? nâ??a manifestÃ© dâ??intÃ©rÃªt particulier pour la supervision ou la restriction de lâ??utilisation des pratiques douteuses des sociÃ©tÃ©s israÃ©liennes de logiciels espions.

Ces entreprises offrent leurs services Ã des rÃ©gimes non dÃ©mocratiques, et cela se produit mÃªme si la plupart de ces entreprises dÃ©pendent de lâ??expertise des vÃ©tÃ©rans des FDI.

Black Cube a dÃ©clarÃ© dans un communiquÃ© : Â« Black Cube ne se livre Ã aucun hameÃ§onnage ou piratage et nâ??opÃ¨re pas dans le cybermonde. Black Cube est une sociÃ©tÃ© de soutien aux litiges qui utilise des mÃ©thodes dâ??enquÃªte de renseignement humain lÃ©gal pour obtenir des informations pour les litiges et les arbitrages. Black Cube travaille avec les plus grands cabinets dâ??avocats du monde pour prouver la corruption, dÃ©couvrir des faits de corruption et rÃ©cupÃ©rer des centaines de millions dâ??actifs volÃ©s. Black Cube obtient des conseils juridiques dans chaque juridiction dans laquelle nous opÃ©rons afin de sâ??assurer que les activitÃ©s de nos agents sont entiÃ¨rement conformes aux lois locales. Â»

Cobweb a dÃ©clarÃ© : Â« Nos produits sont basÃ©s sur des donnÃ©es open source et nous opÃ©rons uniquement dans le respect de la loi et des normes les plus strictes en matiÃ¨re de protection de la vie privÃ©e. Â»

Bluehawk a dÃ©clarÃ© : Â« La sociÃ©tÃ© Bluehawk rejette les affirmations de Meta, dont les reprÃ©sentants nâ??ont jamais pris contact avec la sociÃ©tÃ© pour clarifier les choses. La sociÃ©tÃ© opÃ¨re dans la recherche dâ??informations commerciales et le soutien aux procÃ©dures de litige, et ne sâ??engage en aucune faÃ§on dans lâ??espionnage ou le phishing, et nâ??est pas proche dans ses opÃ©rations des sociÃ©tÃ©s listÃ©es par Meta, car la recherche et la collecte sont effectuÃ©es uniquement Ã partir de sources ouvertes. Â»

Cognyte nâ??a pas fait de commentaire dans lâ??immÃ©diat.

Traduction : AFPS

Source : Haaretz

date crÃ©Ã©e
2021/12/22