Une cyberentreprise israÃ©lienne secrÃ¨te vend des technologies dâ??espionnage Ã lâ??Arabie saoudite

Description

Par Gur Megiddo, le 8 juin 2021

Quadream, dirigÃ©e par un ancien responsable du renseignement militaire israÃ©lien, et la technologie de piratage tÃ©lÃ©phonique ont Ã©tÃ© vendues Ã lâ??Arabie saoudite. Elle permet aux clients de pirater lâ??iPhone dâ??une cible en un seul clic.

Il nâ??y a pas de panneau sur la porte, pas de logo indiquant que ce bureau abrite une cybersociÃ©tÃ© qui mÃ¨ne des offensives en ligne. Mais si vous Ãªtes parvenu au 19e Ã©tage de cet immeuble de bureaux anodin de Ramat Gan, soit vous savez oÃ¹ vous allez, soit vous Ãªtes au mauvais endroit et vous nâ??Ãªtes pas le bienvenu. MÃªme les coursiers ne sont pas autorisÃ©s Ã entrer et il y a une boÃ®te spÃ©ciale oÃ¹ la nourriture commandÃ©e par les travailleurs peut Ãªtre dÃ©posÃ©e et rÃ©cupÃ©rÃ©e par ceux qui sont autorisÃ©s Ã entrer.

Bienvenue dans les bureaux de Quadream. Une recherche en ligne sur le nom de la cyberentreprise israÃ©lienne ne donne que peu ou pas de rÃ©sultats. Quelques rapports payants associent son nom Ã dâ??autres rapports du Ghana, mais pas grand-chose dâ??autre.

Quadream est une entreprise de cybercriminalitÃ© offensive spÃ©cialisÃ©e dans lâ??intrusion et le piratage de tÃ©lÃ©phones portables. Elle fournit des solutions technologiques Ã ceux qui veulent extraire des donnÃ©es des smartphones et permet mÃªme Ã ses clients de transformer ces tÃ©lÃ©phones en dispositifs dâ??espionnage tÃ©lÃ©commandÃ©s qui suivent leurs propriÃ©taires involontaires.

IsraÃ«l est le leader mondial de ces technologies et le principal exportateur de ces services, dont la clientÃ¨le ne provient pas toujours des pays les plus dÃ©mocratiques.

Parmi les clients de Quadream figurent des organismes chargÃ©s de faire respecter la loi dans un certain nombre de pays lÃ©gitimes, indique une source, Â«mais il y en a aussi dâ??autres.Â» Haaretz a dÃ©couvert que la firme fournissait ses services Ã lâ??un des rÃ©gimes les plus oppressifs et les

moins dÃ©mocratiques du Moyen-Orient: lâ??Arabie Saoudite.

Selon des rapports Ã©trangers, Quadream nâ??est pas la seule sociÃ©tÃ© israÃ©lienne active en Arabie saoudite. NSO, la sociÃ©tÃ© controversÃ©e de piratage informatique, aurait Ã©galement fait des affaires avec les Saoudiens et semble fournir un service similaire. Pourquoi les Saoudiens auraient-ils besoin des deux?

Quadream a Ã©tÃ© crÃ©Ã©e en 2016 par trois IsraÃ©liens. Deux fondateurs assurent le cÃ´tÃ© technologique: Guy Geva et Nimrod Reznik. Les deux hommes ont travaillÃ© dans lâ??industrie cybernÃ©tique avant de crÃ©er Quadream. Le troisiÃ¨me fondateur a un parcours diffÃ©rent: Ilan Dabelstien, qui a Ã©tÃ© pendant des annÃ©es un haut fonctionnaire des services de renseignements militaires israÃ©liens. Le PDG de la sociÃ©tÃ© sâ??appelle Avi Rabinovtich.

Un dossier de vente destinÃ© Ã des clients potentiels et obtenu par Haaretz rÃ©vÃ¨le que Quadream utilise une sociÃ©tÃ© basÃ©e Ã Chypre appelÃ©e InReach pour vendre ses services Ã lâ??Ã©tranger. InReach est un actionnaire de Quadrum. Selon le deck, le principal outil de piratage â?? le virus qui infecte rÃ©ellement les tÃ©lÃ©phones cibles, appelÃ© Reign â?? appartient Ã InReach elle-mÃªme.

Reign, selon le jeu de cartes dâ??InReach, a des capacitÃ©s de clics nuls pour les iPhones. Cela signifie quâ??il peut infecter un tÃ©lÃ©phone sans que son propriÃ©taire ait Ã cliquer sur un seul lien, comme lâ??exigent gÃ©nÃ©ralement les logiciels malveillants. La plupart des appareils mobiles fonctionnant sous Android peuvent Ã©galement Ãªtre piratÃ©s par Reign, poursuit le jeu de cartes, mais ils nÃ©cessitent que le propriÃ©taire clique sur un lien quelconque.

Selon la plate-forme, une fois infectÃ© par Reign, le logiciel peut extraire toute forme de donnÃ©es du tÃ©lÃ©phone. Par exemple, selon la prÃ©sentation commerciale dâ??InReach, Reign peut soulever tout document ou toute donnÃ©e stockÃ©e sur le tÃ©lÃ©phone, y compris les photos, les vidÃ©os, les e-mails, les messages WhatsApp ou ceux appartenant Ã dâ??autres applications de messagerie comme Telegram. Mais ce nâ??est pas tout: il peut Ã©galement faire fonctionner lâ??appareil photo Ã distance, ainsi quâ??Ã©couter Ã travers le microphone du tÃ©lÃ©phone ou activer son systÃ¨me GPS pour suivre son propriÃ©taire.

Lâ??utilisation dâ??une sociÃ©tÃ© chypriote comme bureau de vente frontal peut avoir des consÃ©quences rÃ©glementaires. Les cyber-entreprises israÃ©liennes sont soumises Ã la surveillance de lâ??organisme israÃ©lien de rÃ©glementation des exportations de dÃ©fense. Mais cela ne sâ??applique pas Ã une entitÃ© chypriote. Le ministÃ¨re de la DÃ©fense nâ??a pas rÃ©pondu aux questions de Haaretz concernant la surveillance de Quadream et InReach. Quadream nâ??a pas non plus rÃ©pondu.

La surveillance exercÃ©e par les experts de la dÃ©fense israÃ©lienne a pour but dâ??empÃªcher que les technologies israÃ©liennes ne tombent entre de mauvaises mains, notamment celles impliquÃ©es dans le terrorisme. Il est Ã©galement censÃ© sâ??assurer que la technologie israÃ©lienne nâ??est pas utilisÃ©e Ã des fins illÃ©gales et quâ??elle est limitÃ©e aux efforts lÃ©gaux de lutte contre le terrorisme et la criminalitÃ©, et non Ã des fins de persÃ©cution politique, par exemple.

Entre MBS et NSO

Jamal Khashoggi a Ã©tÃ© assassinÃ© Ã lâ??intÃ©rieur de lâ??ambassade saoudienne Ã Istanbul en 2018. Son assassinat a Ã©tÃ© le point culminant dâ??un processus qui a commencÃ© deux ans auparavant lorsque Mohammed bin Salman a Ã©tÃ© nommÃ© prince hÃ©ritier dâ??Arabie saoudite et a commencÃ© Ã sÃ©vir contre ceux qui sâ??opposaient Ã son pouvoir croissant au sein du royaume, enfermant de maniÃ¨re cÃ©lÃ¨bre dâ??autres membres de la famille royale au Ritz Ã Riyad.

Selon Citizen Lab, NSO a travaillÃ© avec les Saoudiens et sa technologie pourrait mÃªme avoir jouÃ© un rÃ´le dans la localisation de Khashoggi. NSO a dÃ©menti avec vÃ©hÃ©mence ce rapport.

Quadream, a appris Haaretz, a travaillÃ© avec le rÃ©gime saoudien depuis 2019 et donc leur technologie nâ??a, semble-t-il, rien Ã voir avec lâ??affaire Khashoggi. Cependant, cela pose la question de savoir pourquoi MBS aurait besoin dâ??un service aussi similaire et Ã quelle fin.

Quadream, a appris Haaretz, a travaillÃ© avec le rÃ©gime saoudien depuis 2019 et donc leur technologie nâ??a rien Ã voir avec lâ??affaire Khashoggi. Dâ??autre part, Quadream a commencÃ© Ã fournir des capacitÃ©s de piratage Ã lâ??Arabie saoudite de MBS aprÃ¨s que la nature impitoyable de son rÃ©gime envers ses rivaux politiques Ã©tait bien connue. La question demeure: pourquoi les Saoudiens auraient-ils besoin de ce qui semble Ãªtre un service trÃ¨s similaire fourni par deux fournisseurs diffÃ©rents?

Une source bien informÃ©e sur Quadream affirme que contrairement Ã NSO, qui fait lâ??objet dâ??une surveillance, la technologie dâ??InReach ne peut Ãªtre dÃ©sactivÃ©e Ã distance. NSO, comme beaucoup dâ??autres, a la possibilitÃ© dâ??arrÃªter son logiciel en cas dâ??abus et de violation de ses conditions dâ??utilisation. Quadream nâ??a pas cette possibilitÃ©. Cette diffÃ©rence peut Ãªtre la clÃ© pour expliquer pourquoi le rÃ©gime de MBS a Ã©galement voulu utiliser Quadream.

Le dossier de vente, qui a rÃ©cemment Ã©tÃ© prÃ©sentÃ© Ã un gouvernement Ã©tranger, ne mentionne pas quâ??InReach peut Ãªtre dÃ©sactivÃ© Ã distance. Il convient toutefois de noter que la prÃ©sentation souligne Ã plusieurs reprises que la technologie ne doit Ãªtre utilisÃ©e quâ??Ã des fins lÃ©gales et par les forces de lâ??ordre.

Une autre explication, selon des sources du secteur, est quâ??Ã cÃ´tÃ© de certaines diffÃ©rences dans leurs capacitÃ©s, les services de Quadream sont gÃ©nÃ©ralement moins chers que ceux fournis par NSO.

Â«Le problÃ¨me du piratage des tÃ©lÃ©phones portables, câ??est quâ??Ã tout moment, les services peuvent se dÃ©connecter. Personne nâ??est en mesure de fournir un service Ã 100% et la plupart des produits actuels sont loin dâ??atteindre ce chiffreÂ», a dÃ©clarÃ© une source dans le secteur de la cybernÃ©tique.

Â« Il suffit que la cible mette Ã jour le systÃ¨me dâ??exploitation de son tÃ©lÃ©phone pour que [le hack] soit dÃ©connectÃ©. Il faut donc des personnes disponibles 24 heures sur 24, capables de passer Ã lâ??action et de pirater Ã nouveau le tÃ©lÃ©phone quelques heures aprÃ¨s le lancement du nouveau systÃ¨me dâ??exploitation.

Â«Ceux qui achÃ¨tent des services coÃ»teux savent quâ??ils bÃ©nÃ©ficient dâ??une assistance 24 heures sur 24 de la part des travailleurs les plus chers du marchÃ©, de sorte quâ??il ne sâ??Ã©coule quâ??un minimum de temps entre la dÃ©connexion et la nouvelle connexion. Si vous ciblez des

personnes qui ne sont pas aussi sensibles et que vous pouvez vous permettre de les perdre de vue pendant quelques heures, voire quelques jours, alors dans ce cas, vous pouvez prÃ©fÃ©rer un service moins cher.Â»

14 hommes au Ghana

En septembre 2020, des rapports en provenance du Ghana ont indiquÃ© que 14 IsraÃ©liens de lâ??industrie cybernÃ©tique sont arrivÃ©s dans le pays. Certains dâ??entre eux Ã©taient de Quadream et, selon les rapports, ils Ã©taient lÃ Ã lâ??invitation du prÃ©sident du pays, Nana Akufo-Addo, qui aurait un projet pour eux.

Le dirigeant se dirigeait vers une rÃ©Ã©lection prÃ©vue en dÃ©cembre 2020 quâ??il a finalement remportÃ©e.

Haaretz a confirmÃ© deux aspects clÃ©s du rapport: premiÃ¨rement, le personnel de Quadream est bien arrivÃ© au Ghana Ã ce moment-lÃ et deuxiÃ¨mement, Quadream a travaillÃ© pour le gouvernement ghanÃ©en. Cependant, Haaretz nâ??a pas confirmÃ© la raison de leur prÃ©sence dans le pays ni le projet dans lequel ils Ã©taient impliquÃ©s.

Haaretz a Ã©galement confirmÃ© que Quadream a proposÃ© ses services Ã une agence officielle en IndonÃ©sie.

Quadream a refusÃ© de commenter ce rapport.

Source : Haaretz

Traduction TD pour lâ??Agence mÃ©dia Palestine

Tags

1. arabie saoudite
2. cyberentreprise
3. espionnage

date crÃ©Ã©e
2021/06/10