Des rebelles syriens piratés grâce à de faux profils Skype et Facebook

Des rebelles syriens piratés grâce à de faux profils Skype et Facebook

Victimes de «femmes fatales» sur les réseaux, ils se sont fait dérober des informations militaires ou personnelles.
La recette est vieille comme l'espionnage, mais elle fonctionne toujours à l'ère numérique : pour soutirer des informations à la rébellion syrienne, un groupe de pirates informatiques encore non identifié a utilisé de faux profils féminins sur les réseaux Skype et Facebook. C'est ce qu'a découvert une équipe de chercheurs travaillant pour la société américaine de sécurité informatique FireEye, dont le rapport, intitulé «Derrière les lignes de front numérique du conflit syrien», a été publié ce 2 février.

«MATA HARI NUMÉRIQUES»
La récolte est considérable. En remontant le fil de documents PDF contenant des logiciels malveillants (ou malwares), les chercheurs ont découvert un ensemble de 7,7 GB de données «révélant la stratégie de l'opposition syrienne, des plans de bataille, des besoins d'approvisionnement, et une foule d'informations personnelles et de sessions de messagerie instantanée appartenant aux hommes qui combattent les forces du président syrien Bachar al-Assad». Le piratage, qui se serait déroulé a minima de novembre 2013 à janvier 2014, a visé aussi bien des rebelles liés à l'Armée syrienne libre que des membres de groupes islamistes armés et des personnes sans affiliation précise. Parmi la soixantaine de cibles directes identifiées – un chiffre minimal, qui correspond au nombre de comptes Skype compromis –, l'équipe a notamment repéré un chef d'unité combattante, un ex-officier de haut rang ayant déserté les services de sécurité d'Assad, un coordinateur local d'une ONG turque, ou encore un membre d'un centre de presse basé en Syrie.
Lors de leurs échanges avec les «femmes fatales», les opposants au régime syrien se voyaient demander s'ils utilisaient Skype «sur un ordinateur ou sur [leur] téléphone», avant de recevoir une photo abritant le malware adéquat, grâce auquel les attaquants pouvaient ensuite accéder à l'ordinateur de leur cible. Les profils Facebook correspondants étaient, eux, truffés de liens malveillants, cachés derrière des discours favorables à l'opposition et des invitations à utiliser des outils de sécurisation des communications, tels que des réseaux privés virtuels ou le réseau d'anonymisation Tor.
Une stratégie de «Mata Hari numérique», comme l'a noté Martin Gropp, journaliste à la Frankfurter Allgemeine Zeitung :

DES OUTILS «SUR MESURE»
L'utilisation de faux profils féminins sur les réseaux sociaux à des fins d'espionnage n'est pas une nouveauté. Nicolas Arpagian, directeur scientifique à l'Institut national des hautes études de la sécurité et de la justice, fait notamment état d'une opération du même genre attribuée au Hezbollah : d'après un article du Spiegel paru en mai 2010, un faux profil Facebook aurait permis de soutirer des informations à quelque 200 soldats ou réservistes de l'armée israélienne. Il y a deux ans, une étude du département de la Défense australien a accusé les talibans d'user de la même méthode pour espionner ses soldats.

Dans le cadre du conflit syrien, en revanche, le déploiement à cette échelle de la méthode est inédit. «C'est la première fois que nous constatons un tel degré de sophistication dans l'utilisation de faux profils, et dans cet objectif», explique John Scott-Railton, chercheur associé au Citizen Lab de l'université de Toronto et l'un des auteurs du rapport de FireEye. Le mode opératoire – qui repose en grande partie sur «l'ingénierie sociale», autrement dit l'exploitation des failles humaines – n'est pas la seule différence avec ce qu'il a pu examiner jusqu'à présent (1). «Ces acteurs ont utilisé une boîte à outils plus diversifiée que ce que nous avions observé de la part de hackers pro-gouvernement ou dans l'attaque liée à l'EI, poursuit Scott-Railton. Ils ont des outils « sur mesure ». Et ils ont clairement ciblé des informations de nature militaire.» Au final, souligne le rapport, la moisson d'informations récoltées avait de quoi offrir «un avantage immédiat sur le champ de bataille».
L'attaque reste néanmoins assez peu technique, estime Raphaël Vinot, chercheur en sécurité au CERT (2) national du Luxembourg. La plupart des logiciels utilisés reprennent du code qui circulait déjà sur Internet. Le logiciel de prise de contrôle des ordinateurs à distance, dénommé «Darkcomet», existe depuis 2008 – son créateur, un programmeur français, a même cessé de le développer face aux utilisations malveillantes qui en étaient faites. «C'est un outil lourd, vraiment pas discret, estime le Luxembourgeois. Mais les antivirus ne le détectent pas, donc cela fonctionne dans la majorité des cas.»

Pour lui, l'outil le plus évolué pourrait être le malware ciblant le système d'exploitation pour smartphones Android. Ce qui est également, selon les chercheurs de FireEye, une nouveauté dans le contexte syrien. Or les smartphones sont une mine d'informations, en particulier dans une zone où, explique le rapport, «les pannes de courant régulières peuvent pousser les gens à se fier encore plus aux mobiles pour communiquer».

LA PISTE LIBANAISE
Quant à savoir qui se cache derrière cette opération, mystère. Les auteurs de l'étude avancent prudemment avoir «des indications selon lesquelles le groupe pourrait être financé et/ou situé en dehors de la Syrie». Ils font néanmoins état de multiples références au Liban, que ce soit dans les faux profils ou sur le site web mis en ligne par le même groupe, présenté comme émanant de l'opposition syrienne et lui aussi truffé de logiciels malveillants. Par ailleurs, deux versions de test des malwares utilisés ont été mises en ligne depuis le Liban. Vraie ou fausse piste ? «Avec Internet, tout est possible, rappelle John Scott-Railton. Mais si ce groupe a fait preuve d'une certaine sophistication dans l'attaque, peut-être qu'en matière de sécurité opérationnelle, il n'était pas en capacité de mettre en place une énorme « fausse bannière ».»

«C'est à juste titre que le rapport reste prudent, juge Eva Galperin, analyste à l'Electronic Frontier Foundation, qui a travaillé sur une précédente étude de cyberattaques en Syrie. Attribuer une attaque informatique est très difficile, et je ne vois rien, pour l'instant, qui indique de manière définitive un acteur originaire du Liban.» A ce stade donc, difficile d'aller plus loin que les conjectures. D'autant qu'à la différence de l'Armée électronique syrienne, qui s'illustre depuis près de trois ans par des coups d'éclat prioritairement orientés vers les médias – et dont Le Monde a été la plus récente victime –, ce groupe-ci a agi dans la plus grande discrétion.

Avant de rendre public leur rapport, les chercheurs ont contacté quelques-unes des victimes du piratage. Lesquelles ont eu une réaction assez fataliste : «Les groupes syriens ont tellement l'habitude que leurs communications soient espionnées, conclut Scott-Railton, qu'ils ne sont pas vraiment surpris d'avoir été piratés. En général, ils estiment qu'ils ont d'autres problèmes plus urgents.» Non seulement le cyberespionnage se démocratise très manifestement, mais il a en prime de beaux jours devant lui.

(1) Voir notamment les deux précédentes études auxquelles il a participé : l'une sur les attaques menées par des pirates informatiques pro-gouvernement («Quantum of Surveillance», rapport conjoint du Citizen Lab et de l'Electronic Frontier Foundation), l'autre consacrée à une attaque par malwareliée à l'État islamique.

(2) Computer Emergency Response Team, le centre d'alerte et de réaction aux attaques informatiques.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.liberation.fr/monde/2015/02/04/des-rebelles-syriens-pirates-grace-a-de-faux-profils-skype-et-facebook_1194718