Une app Android pour traquer l'ennemi : comment le cyber s'invite dans la guerre

Après s'être penché sur le rôle des Fancy Bear, un groupe de hackers réputé lié au renseignement militaire russe (GRU), dans les opérations visant à révéler les secrets du camp démocrate lors de la campagne présidentielle américaine, Crowdstrike s'intéresse à ses activités sur un autre front, l'Ukraine. Et les découvertes de la société américaine s'apparentent à un cas d'école de la manière dont le cyber peut venir s'intégrer dans des conflits armés traditionnels.

En suivant les traces de X-Agent (ou Sofacy), le kit préféré des Fancy Bear, Crowdstrike est remonté, à la fin de l'été dernier, à « *un curieux package Android* ». Un fichier APK contenant des références à des systèmes d'arme, dont la pièce d'artillerie d'origine russe D-30, mais qui, après rétro-ingénierie, s'est avéré dissimuler une variante de X-Agent. Les analystes de la firme américaine affirment que cette souche infectieuse est un kit d'accès à distance, repéré depuis près d'une décennie par les chercheurs en sécurité et opéré exclusivement par les Fancy Bear. Elle essaime sur de multiples plates-formes : Windows, iOS, probablement MacOS et donc Android.

Localiser les D-30 pour les détruire

En réalité, le nom du package Android, piégé avec X-Agent, renvoie à une application des plus légitimes, développée par un officier de l'armée ukrainienne et permettant de réduire le temps de mise à feu d'une pièce D-30, en accélérant le calcul des données de ciblage. Selon ledit officier, cette application est employée par environ 9 000 utilisateurs. C'est cet édifice qu'est venu pervertir les Fancy Bear, en déployant une version de l'app infectée. Une version pirate distribuée sur les très officiels forums de l'armée ukrainienne dès la fin de 2014, selon Crowdstrike.

Avec des conséquences dévastatrices pour l'armée de ce pays, engagé dans un conflit avec Moscou. « *La capacité de ce malware à récupérer les communications et les données de localisation brutes depuis un terminal infecté l'a transformé en un moyen attractif pour localiser l'artillerie ukrainienne et engager le combat avec elle* », écrit la société Crowdstrike. Or, selon cette dernière, des données librement disponibles montrent que l'artillerie ukrainienne a perdu 50 % de ses pièces en deux ans de conflit. Et même 80 % de ses D-30, le pourcentage le plus élevé de pertes que déplore Kiev sur ce terrain.

« *On ne parle pas ici d'attaque ou de piratage d'équipements militaires mais de ciblage des usages*

'personnels' des militaires, relève Gérôme Billois, senior manager en cybersécurité du cabinet de conseil Wavestone. *Ce qui en lumière un risque particulier, lié à la pénétration des technologies grand public dans la sphère militaire. Certaines armées ont édicté des règles strictes sur ces usages, en particulier aux Etats-Unis. Cette affaire montre aussi que les groupes cybercriminels n'hésitent pas à cibler la sphère personnelle (téléphone, email…) des individus présents dans les organisations qu'ils veulent attaquer. On a déjà vu des cybercriminels recherchant, contre rémunération, sur des forums underground des infos pour accéder aux comptes personnels de dirigeants ou d'administrateurs du SI* ». Une façon de se ménager un accès aux données professionnelles que de nombreux professionnels transfèrent sur leur boite personnelle pour travailler le week-end, mais aussi d'exploiter le potentiel qu'offrent les terminaux mobiles de ces cibles (localisation, installation d'applications espion, etc…).

A lire aussi :

Hacking des élections : les partis politiques français sont-ils prêts ?

Fuite Shadow Brokers : la preuve d'une nouvelle taupe à la NSA ?