Les États, (cyber)criminels en série ?

Les groupes français Thales et israélien Verint ont publié lundi un annuaire mondial des groupes de pirates informatiques les plus menaçants, où se distinguent particulièrement les groupes étatiques ou para-étatiques.

Temps de lecture : minute

7 octobre 2019

Sur les 66 groupes d'attaquants de haut niveau figurant dans ce Who's who du cybercrime, 49% sont considérés d'origine étatique ou soutenus par un Etat. Ces groupes agissent généralement à des fins de cyberespionnage, de déstabilisation politique, ou de sabotage. Dans le reste des groupes, 26% sont des "hacktivistes", des militants motivés par des idéologies communautaires, religieuses, politiques. 20% sont des cybercriminels, motivés par l'appât du gain, 5% des cyberterroristes.

Parmi les groupes les plus dangereux en terme de sophistication de leurs outils, les groupes russes dominent (4 dans les 10 premiers), suivis par les groupes chinois (3 sur 10). Certains groupes comme les groupes russes ou chinois semblent parfois "*faire exprès de se faire connaître, pour afficher leur niveau de compétence*", a expliqué à des journalistes Ivan Fonterensky, l'un de l'équipe à l'origine
du rapport.

"*Il y a quelque temps, des bateaux ont été compromis au large de l'Indonésie*", a-t-il indiqué. Les investigations ont montré qu'un groupe chinois avait fait exprès de pousser du logiciel malveillant sur les navires, "*pour se faire détecter et que l'on sache qu'ils étaient présents*", a-t-il ajouté.

Discrétion des groupes américains

A l'inverse, les groupes américains restent extrêmement discrets, et très peu d'informations ont pu être collectées. Dans les 10 premiers groupes du classement, on trouve aussi un groupe vietnamien, un groupe iranien... et un groupe français, baptisé Animal Farm ou ATK 08, dont le rapport laisse entendre qu'il est sans doute lié à l'Etat français.

Ce groupe "actif depuis au moins 2009" utilise des "*techniques avancées mais ne semble pas motivé par des gains financiers*". Il est connu pour ses logiciels malveillants "de haute qualité", dont les outils ont été utilisés contre des organisations diverses "*notamment en Syrie, en Iran et en Malaisie*".

Les cibles privilégiées des 66 groupes répertoriés sur les dix dernières années sont le gouvernement et la défense (près de la moitié des attaques), la finance (plus du tiers), l'énergie (10% environ). Les attaques contre les médias et le secteur médical (hôpitaux) et pharmaceutique ont connu une augmentation "*particulièrement significative*" ces derniers mois.

Côté Thales, le rapport a été produit par l'équipe d'analyse technique de la menace, une cellule de renseignement cyber. La mission de cette cellule d'une douzaine de personnes est notamment d'alimenter en informations les outils de protection informatique vendus par Thales.

Article écrit par Maddyness avec AFP