Microsoft combat les hackers russes de Fancy Bear avec… ses avocats

C'est sur un terrain un peu inattendu que Microsoft a choisi de déplacer le combat contre Fancy Bear, ce groupe de hackers que les autorités américaines accusent de n'être qu'un faux nez des services secrets russes. Selon *The Daily Beast*, les avocats du premier éditeur mondial harcèlent Fancy Bear devant la justice américaine, accusant les hackers d'intrusions sur des systèmes, de cybersquatting et d'atteinte aux marques Microsoft. Si ces actions ne visent évidemment pas à amener les hackers de Fancy Bear devant un tribunal américain, elles ciblent ce que Microsoft voit comme le point faible de cette organisation : les serveurs de commande et de contrôle que les assaillants utilisent pour distribuer et piloter leurs malwares ou encore recueillir des données une fois leurs cibles infectées.

Entre août 2016 et mars 2017, au travers de plusieurs requêtes devant la justice, Microsoft a ainsi mis la main sur 70 domaines utilisés par Fancy Bear dans ses campagnes infectieuses, affirment nos confrères. Plutôt que de tenter de faire saisir ces machines, que Fancy Bear loue à des prestataires partout dans le monde, Redmond choisit une stratégie indirecte consistant à réclamer la propriété de domaines exploités par les hackers, mais renvoyant à ses marques. Des domaines comme livemicrosoft.net or rsshotmail.com. Une fois que Microsoft en récupère le contrôle, l'entreprise peut couper le lien qui relie les Fancy Bear à leurs victimes en redirigeant le trafic vers ses propres serveurs. Au passage, l'éditeur de Windows récupère une foule de données sur les activités et les cibles du célèbre groupe de pirates, aussi connu sous les pseudos APT28, Sofacy ou Pawn Storm.

Microsoft vs Fancy Bear : le chat et la souris

Rappelons que cette organisation, que les Etats-Unis présentent comme proche du GRU (les services secrets militaires russes), voire comme une émanation pure et simple de ces derniers, est soupçonnée des piratages de l'Otan, de la Maison Blanche (sous Obama), de TV5 Monde, de l'agence mondiale anti-dopage, du camp démocrate lors de la dernière campagne présidentielle américaine ou encore des équipes d'En Marche, en amont de l'élection d'Emmanuel Macron à la présidence de la République. Liste évidemment non exhaustive, loin s'en faut.

Si la technique qu'emploie Microsoft a déjà été utilisée, notamment par les autorités contre des cybercriminels, l'offensive de Microsoft est la première d'un industriel contre une opération de renseignement émanant apparemment d'un gouvernement étranger. En 2015, l'éditeur russe Kaspersky avait certes réussi à mettre la main sur une douzaine de domaines cachant des serveurs de commande et contrôle de la NSA américaine, mais seulement après que cette dernière ait négligé ou décidé de ne pas renouveler l'enregistrement de ces URL. Notons que l'offensive de Microsoft contre Fancy Bear tient largement du jeu du chat et de la souris ; les hachers enregistrant de nouveaux domaines à mesure que l'éditeur parvient à mettre la main sur certaines URL.

A lire aussi :

Pour la NSA, la Russie a bien tenté de hacker l’élection américaine

En Marche est la cible d’attaques de phishing des services russes

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

Photo via Activedia via Visualhunt.com