Rançongiciels : 7 hackers proches du groupe REvil arrêtés

Chaque vendredi, dans sa revue de presse, Maddyness vous propose une sélection d'articles sur un sujet qui a retenu l'attention de la rédaction. Cette semaine, l'arrestation de 7 hackers proches du groupe REvil aux Etats-Unis et en Europe.

Temps de lecture : minute

12 novembre 2021

7 hackers du groupe REvil arrêtés

L'actu

Opération "Golddust", poussière d'or. Un nom à la James Bond pour un coup de filet d'envergure mondiale, impliquant 17 pays et visant un groupe de cybercriminels considéré comme le plus redoutable en matière de rançongiciels. Sept personnes ont été arrêtées dans le cadre de cette opération destinée à porter un coup d'arrêt au groupe de hackers russophones REvil, parfois appelé Sodinokibi, a détaillé Europol dans un communiqué rendu public lundi soir.

Lire l'article complet sur Libération.

Une opération collaborative

L'enquête

Ces arrestations et ces saisies de fonds sont les fruits des efforts considérables déployés ces derniers mois par plusieurs pays, dont les Etats-Unis et la France, pour déjouer l'industrie criminelle des rançongiciels, qui a causé des dégâts incommensurables dans le monde entier. REvil faisait figure de cible numéro un : aux Etats-Unis, les autorités ont été particulièrement échaudées par deux attaques de ce groupe. Outre Kaseya, le fonctionnement de l'entreprise de l'agroalimentaire JBS avait été gravement perturbé par les pirates en juin. *Lire l'article complet sur le Monde.*

Un système bien rodé

Le réseau

Les suspects sont ce que l'on appelle des " affiliés " à REvil ou GandCrab. L'écosystème des rançongiciels s'est structuré ses dernières années. Une forme de sous-traitance s'est installée entre les développeurs des virus, ceux qui pénètrent un système informatique cible et ceux qui négocient la rançon. Les affiliés de REvil auraient mis la main sur près de 200 millions de dollars au total.

Le département du Trésor a également sanctionné Chatex, bourse d'échange de cryptomonnaies et trois autres entreprises liées, accusées de faciliter le blanchiment de l'argent des rançons. *Lire l'article complet sur Siècle digital.*

Les investigations continuent

La traque

Les autorités américaines sont également aux trousses d’un autre pirate d’envergure, à savoir Yevgeniy Polyanin. Cet homme de 28 ans aurait réalisé plus de 3000 attaques avec REvil et récolté plus de 31 millions de dollars de rançon. Il court toujours, mais les autorités américaines ont réussi à récupérer l’équivalent de 6,1 millions de dollars en cryptoactifs. Ces derniers étaient stockés sur un compte de la place de marché FTX. *Lire l'article complet sur 01Net.*

Article écrit par Anne Taffin