Trend Micro ausculte la cybercriminalité underground en France

Un chercheur de Trend Micro s'est livré à un exercice délicat : plonger dans l'univers de la cybercriminalité souterraine en France. Connu sous le vocable « underground », cette partie du web accueille des places de marchés, des forums où s'achètent contre monnaie virtuelle des armes, de la drogue, des faux documents, mais aussi des malwares.

Dans son étude, l'éditeur japonais précise que le tréfonds du web français reste relativement modeste par rapport à d'autres pays comme la Chine ou la Russie. Néanmoins, il recense 40 000 cybercriminels sur l'underground hexagonal ayant des compétences hétérogènes (expert à novice). Ce foyer génère entre 5 à 10 millions d'euros par mois.

Une prudence de sioux

Un des leitmotiv des cybercriminels français est la prudence. Pour approcher ce monde souterrain, il faut montrer patte blanche. L'objectif est d'éviter de se faire coincer par les forces de l'ordre. Le climat de méfiance règne donc allant jusqu'à la délation (signalement des actes malhonnêtes et frauduleux) et jusqu'à l'affrontement (les places de marché se piratent mutuellement pour se piquer des clients).

L'acceptation sur les forums fait par cooptation, par évaluation de la réputation. Mais ce qui distingue le Dark Net Français, c'est le recours à des tiers de confiance (*escrow* en anglais). Ils jouent un rôle d'intermédiaire dans la transaction entre les deux parties pour s'assurer que chacun récupère son dû. Ces intermédiaires prennent une commission (entre 5 et 7%) sur la transaction. Certaines places de marché ont même créé leurs propres plateformes de tiers de confiance (mais faut-il encore avoir confiance ?).

La disparition des forums est aussi un grand classique, comme le précise le chercheur de Trend Micro. « *Un des forums les plus en vue du French Dark Net qui recensait 40 000 utilisateurs avec la possibilité de gérer leurs transactions a fermé du jour au lendemain et les administrateurs se sont enfuis avec la caisse*. *Le préjudice est estimé à 180 000 euros.* » Et d'ajouter que les mêmes administrateurs ont créé une nouvelle structure dans les jours suivant. Rien ne se perd, tout se crée.

Chiffrement et bitcoin de rigueur

Parmi les autres enseignements, l'underground français n'échappe pas à la vague du chiffrement des communications. Logique, avec un degré de méfiance qui frise la paranoïa, les conversations sont chiffrées et plutôt fortement, assure Trend Micro. « *On est principalement sur du PGP.* » De même, l'usage de Tor s'est banalisé. Pour trouver les forums ou les places de marché, il est quasiment impossible de les repérer sur le web normal. Les sites se terminent par .onion indiquant son appartenance au réseau anonymisé Tor.

Le Bitcoin et les cartes prépayées sont les moyens de paiement préférés sur l'underground

français. La crypto-monnaie est traditionnellement utilisée dans ce genre de secteur. Mais la carte prépayée PCS est une spécificité française. « *Elles sont devenues si populaires que certains cybercriminels vendent ce type de cartes avec de faux papiers d'identité et des fausses informations personnelles comme adresse physique, e-mail et carte SIM. L'objectif est de déverrouiller le plafond de paiement pour atteindre jusqu'à 3000 euros. L'opération coûte à peu près 60 euros* », souligne Trend Micro.

Le royaume des faux documents officiels et Pass PTT

Héritage du système jacobin et du régime napoléonien, la France est la partie des papiers administratifs. On ne s'étonnera donc pas que les propositions commerciales sur le Dark Net hexagonal concernent la fraude aux documents administratifs. Fausse carte d'identité, carte grise (500 euros), carte PMR (mobilité réduite pour 40 euros), justificatif de domicile (utile pour certaines démarches), vente de points pour le permis de conduire, ouverture d'un compte bancaire (700 euros).

Autre élément typiquement français, le pass PTT. Il s'agit d'une clé dont dispose les livreurs pour ouvrir l'ensemble des boîtes aux lettres d'un immeuble. Les personnes peuvent ainsi chercher des plis contenant de l'argent, des chéquiers ou des clés de maison. Ces pass PTT sont disponibles sur les forums underground à des tarifs abordables. Un vendeur proposait 25 clés pour 220 euros, un autre vendait à l'unité au tarif de 15 euros et un troisième livrait un fichier d'impression 3D de la dite clé, rapporte l'éditeur de sécurité.

Du ransomware et du binder made in France

Enfin pour terminer, le marché noir de la cybersécurité comprend tout l'attirail pour mener à bien des attaques, des intrusions, etc. Ainsi, le ransomware qui est la menace la plus développée aujourd'hui dans le cyberespace, trouve sa place sur l'underground français. Trend Micro a détecté deux cybercriminels qui ont développé des rançongiciels conçus pour des victimes françaises.

Autre spécificité, l'éditeur de sécurité a découvert un binder (outil d'obfuscation de malware qui mixe le code du malware avec un logiciel légitime et ainsi éviter d'être détecté), réalisé par un développeur français. Mais ce binder n'est ni promu, ni vendu. Habituellement, les cybercriminels français utilisent des logiciels et des outils malveillants achetés sur d'autres marchés underground.

A lire aussi :

Johanne Ulloa, Trend Micro : « La v2 du ransomware est déjà là »

Sécurité réseau : Trend Micro récupère TippingPoint auprès de HP

crédit photo © GlebStock – Shutterstock