Le Matin Dimanche
Dimanche 28 novembre 2021

Chaque catégorie de hacker vise un objectif précis

INFORMATIQUE Les récentes cyberattaques en Suisse lèvent le voile sur un monde inconnu du grand public mais qui constitue la grande délinquance d'aujourd'hui.

LUCIE MONNAT
lucie.monnat@lematindimanche.ch

Le SECO, des EMS, le site Comparis, l'organisateur de Baselworld et Art Basel MCH Group, ou encore des communes comme Rolle (VD): depuis quelques mois, la Suisse, comme le reste du monde, est frappée par une épidémie d'attaques en ligne. Les données volées sont bloquées, sujettes à rançon ou à la revente sur la face cachée d'Internet, le «dark web».

Les attaques augmentent car le business est extrêmement fructueux: la cybercriminalité rapporterait plus d'argent que le trafic de drogue et la prostitution. Rien d'étonnant, donc, que la scène du hacking se professionnalise et devienne toujours plus sophistiquée. Elle regroupe des profils divers qui, bien que motivés par l'appât du gain pour la plupart, poursuivent des buts différents. Tour d'horizon.

1. Objectif: appât du gain

Entrer dans le darknet n'est pas bien compliqué, même pour ceux qui ne sont pas des as de l'informatique. Mais y pénétrer revient à ouvrir la boîte de Pandore. On y découvre un monde fascinant, où tout s'achète en quelques clics: de l'héroïne pure, des ordonnances médicales, des «followers» ou des «likes» sur Instagram ou YouTube, des données de cartes bancaires... la liste est infinie, et les denrées se paient pour la plupart en cryptomonnaie, souvent des bitcoins.

Certains hackers offrent leurs services pour réaliser des missions précises, à caractère plus personnel. Vous souhaitez vérifier la fidélité de votre âme sœur? Un pirate entrera dans son téléphone et mettra à votre disposition les messages reçus et émis - même ceux qui ont été supprimés. Vous voulez modifier vos résultats universitaires afin de faire briller votre CV? Il ira falsifier votre bulletin de notes directement sur le site de l'école. Vous êtes patron d'une entreprise et enviez le savoir-faire d'un concurrent? Vous connaissez la suite.

Derrière ce marché se cachent tant des individus isolés que des petites bandes, plus ou moins organisées et motivées par l'appât du gain. Des groupes ciblent des «petits poissons», tels que des privés, des communes ou des petites à moyennes entreprises. D'autres visent des plus grosses prises, comme des institutions gouvernementales ou des multinationales. «On parle d'une véritable mafia, explique Steven Meyer, directeur de la société de sécurité ZENData. Elle se compose autant de petits cambrioleurs qui entrent dans votre maison que de types à la «Ocean's Eleven» qui braquent un casino.»

Les groupes rançonnent généralement leurs victimes et publient leurs informations sensibles sur le darknet en cas de refus de payer. C'est exactement ce qui est arrivé à Rolle, dont les données sensibles sont depuis accessibles sur le darknet. Le système est si bien organisé que les pirates proposent souvent des hotlines, disponibles 24 heures sur 24 et dans de nombreuses langues, à leurs victimes. «Si vous êtes une grand-mère, ils vont vous expliquer avec une infinie patience comment acheter des bitcoins pour les payer», raconte Steven Meyer

2. Objectif: déstabiliser

Les groupes qui se concentrent sur des attaques plus ciblées arrivent à des résultats effrayants. Nos recherches nous ont permis de trouver chez un groupe de hackers les coordonnées personnelles de juges américains et de militaires, des dossiers criminels ou des rapports destinés aux tribunaux. «L'argent reste la principale motivation mais pas que. L'objectif peut être de déstabiliser, de créer un dégât d'image ou d'obtenir une information», explique Paul Such, expert en sécurité informatique et fondateur de la société Hacknowledge.

Des États possèdent eux aussi leurs propres hackers. Il s'agit souvent d'obtenir des informations dans un contexte d'espionnage classique ou industriel. Lors de tensions politiques accrues ou de crises, les attaques peuvent porter sur des infrastructures critiques ou consister en des opérations de désinformation ciblées. Selon le site CFR.org, qui recense toutes les attaques détectées sponsorisées par des États, les principaux adeptes de la pratique sont la Chine, la Russie et la Corée du Nord. Les hackers étatiques sont donc des espions des plus modernes, ultra-efficaces et disposant de moyens et d'un temps illimité. «Avec de telles ressources, si l'un de ces hackers vous a dans sa ligne de mire, il finira tôt ou tard par vous avoir», souligne Steven Meyer. L'entreprise du spécialiste s'est occupée récemment de clients impliqués dans la vaccination contre le Covid. «Mes clients étaient attaqués par les Russes. C'est le jeu: les États espionnent les autres pour savoir comment ils gèrent une situation.»

Vous voulez vérifier la fidélité de votre âme sœur ou modifier vos résultats universitaires pour valoriser votre CV? Moyennant finance, un hacker le fera pour vous.
Getty Images

3. Objectif: militer

«À l'origine, la scène était surtout occupée par des activistes, rappelle Paul Such. Ils agissaient par idéologie, parce qu'ils avaient message à passer, mais aussi par goût du challenge technique. Ils plantaient leur drapeau en se réjouissant d'avoir pu entrer dans un système.»

Les «hacktivistes» utilisent leur savoir-faire pour véhiculer leurs opinions politiques ou religieuses. Leur militantisme se cristallise par des attaques contre des institutions ou des entreprises antagonistes à leur idéologie. Le groupe le plus connu est sans conteste les «Anonymous», qui regroupaient des individus prônant toutes sortes d'idées politiques. Ils sont, depuis quelques années, peu actifs.

«Les hacktivistes sont dangereux, car leur but est de détruire ce qui ne correspond pas à leurs idéaux, souligne Steven Meyer. Mais ils sont de moins en moins nombreux car avec ces capacités-là, on peut faire beaucoup d'argent au lieu de simplement nuire. Et ça en tente plus d'un.»

Comment faire face?

Paul Such, expert en sécurité informatique, recommande de ne jamais payer de rançon. «Je peux comprendre qu'une entreprise acculée le fasse. Mais ça revient à encourager ce système. Et on a affaire à des criminels: rien n'assure qu'ils effacent les données une fois payés.» Selon le Centre national pour la cybersécurité, les entreprises qui s'acquittent de la rançon demandée seront à nouveau appelées à passer à la caisse dans 80% des cas. Le spécialiste conseille de prévenir plutôt que de guérir. «Il faut que la mentalité change et que les entreprises et institutions acceptent de payer pour se protéger. Car une fois l'attaque commise, on ne peut plus faire grand-chose.»

Identifier les cybercriminels est très compliqué. «Certains adoptent un système pyramidal: un groupe met à disposition son «rançongiciel» *(ndlr: le cheval de Troie permettant de pénétrer dans un système)* et touche un pourcentage sur les attaques, précise Paul Such. Ils aiment aussi laisser de fausses pistes sur les auteurs des attaques, ce qui complique encore leur identification.»

Le système a énormément évolué en très peu de temps. Les attaques sont plus aisées car le système s'est segmenté. Un hacker va travailler à entrer dans un ordinateur d'une entreprise, mettons d'un employé. Un deuxième hacker s'occupera ensuite du passage dans l'ordi du CEO, car cela demande d'autres compétences. «Un autre va s'occuper de blanchir l'argent récolté grâce aux données volées, poursuit Steven Meyer, directeur de ZENData. Au final, si vous en attrapez un, ce ne sera qu'un petit maillon de la chaîne facilement remplaçable. Pour les gens qui possèdent ces compétences-là, ces réseaux sont extrêmement attrayants: un ingénieur russe gagne 600 euros par mois. Avec ses capacités, il a la possibilité de faire des millions en quelques semaines. Le calcul est vite fait.»