CYBERCRIMINALITÉ

Chez les pirates informatiq il n'y a plus de place pour l'

Les groupes de cybercriminalité sont-ils plus rentables que les jeunes pousses les plus prometteuses de la tech ? On n'en est pas loin. A grands coups d'attaques aux ransomwares, les pirates se portent bien. Très bien même.

THOMAS CASAVECCHIA
ENVOYÉ SPÉCIAL À HELSINKI

Dans le milieu des nouvelles technologies, on parle de « licornes » : des start-up valorisées à plus d'un milliard de dollars. Eh bien, ces licornes existent aussi dans le secteur, plus confidentiel, des pirates informatiques. « C'est assez surprenant que ce soit le cas », avoue Mikko Hyppönen, directeur de la recherche chez WithSecure, une des plus grosses sociétés de sécurité informatique européennes, et théoricien des licornes cybercriminelles, que nous avons rencontré à Helsinki. « Je n'étais pas sûr que ça puisse arriver quand j'ai évoqué le concept pour la première fois, mais aujourd'hui, c'est une réalité. Ces groupes criminels gagnent énormément d'argent. Bien sûr, le nombre d'attaques DDoS ou au *ransomware* a explosé en quelques années, multipliant les rentrées d'argent. Mais c'est surtout l'évolution des cours des cryptomonnaies qui a permis à ces groupes de se retrouver assis sur des montagnes d'argent. »

Une augmentation de capital qui leur a permis de beaucoup se professionnaliser en quelques années. « Certains, aujourd'hui, ressemblent à de véritables multinationales », surenchérit Laurent Mathy, professeur de systèmes informatiques et sécurité à l'ULiège. « Ces groupes disposent d'avocats, de négociateurs chargés des contacts avec les entreprises victimes de leurs attaques, d'armées de techniciens, voire carrément de services de ressources humaines. Certains ont même des bureaux physiques ! » C'est notamment le cas de groupes aux noms célèbres tels que REvil ou Conti.

« Ils disposent carrément de véritables SAV », s'étrangle Mikko Hyppönen. Des professionnels qui négocient individuellement avec les entreprises afin de convenir du prix de la rançon et qui « aident », le cas échéant, leurs victimes à récupérer leurs données une fois l'extorsion réussie : comble du cynisme ? Pas forcément.

« Une certaine forme d'honnêteté »

« Leur *business model* tient notamment grâce à une certaine forme d'honnêteté », concède Laurent Mathy. « C'est pour créer de la confiance avec leurs victimes, leurs "clients", que ces groupes engagent des négociateurs, et même des agents de service après-vente. Il faut pouvoir montrer aux victimes que si elles paient, elles pourront récupérer leurs données et qu'elles ne seront pas ensuite revendues sur le dark web. S'ils avaient la réputation de ne pas tenir leurs engagements, personne ne leur verserait le moindre centième de BitCoin. » Quand on se lance dans la piraterie, il faudrait presque pouvoir revendiquer un score de cinq étoiles sur Yelp.

Encore faut-il trouver des cibles qui paieront à coup sûr. « Il y a quelques années, on voyait beaucoup d'attaques à l'aveuglette, par phishing », explique Christine Bejerasco, CTO chez WithSecure. « Mais peu avant 2020, les groupes cybercriminels ont changé de tactique et ont réorienté leurs efforts sur les entreprises les plus susceptibles de payer des rançons élevées plutôt que sur des particuliers, aux moyens plus limités. »

C'est pour cette raison que l'on a vu les attaques contre les PME ou les hôpitaux se multiplier ces dernières années. Ces services, encore moins que d'autres, ne peuvent se permettre de s'arrêter. Et les données médicales dont ils disposent sont particulièrement sensibles et ne peuvent pas fuiter. « Comme les entreprises sont de plus en plus averties des risques d'une attaque, elles se montrent plus prudentes et effectuent des sauvegardes de leurs données afin que le blocage des serveurs ne soit pas un trop gros problème », poursuit la responsable.

Pour contrer cela, une nouvelle stratégie a donc été mise en place par les pirates : en plus d'exiger une rançon pour décrypter les fichiers bloqués, ils menacent de diffuser ces données sur le dark web. Evidemment, le paiement de la rançon n'offre pas vraiment de garantie contre une fuite des données en bonne et due forme puisque sur les réseaux du « web profond », ces données s'échangent pour de très belles sommes. Cette assise financière rend les pirates plus dangereux que jamais.

« Beaucoup de chercheurs travaillant pour les cybercriminels traquent activement les failles de sécurité *zero-days* », poursuit Mikko Hyppönen. « Avant cela, la recherche de telles failles était réservée aux gouvernements ou aux chercheurs. Désormais, certains groupes pirates ont les ressources pour s'y atteler. Aujourd'hui, ces escrocs peuvent se permettre d'investir des sommes colossales dans leurs attaques afin que celles-ci soient encore plus dévastatrices. Je crains qu'ils ne parviennent même à débaucher des experts en intelligence artificielle et en *machine learning* alors que ces profils sont particulièrement recherchés sur le marché traditionnel de l'emploi. Avec ces talents, il y a fort à parier que l'on assiste dans les prochaines années à des attaques automatisées comme jamais. Avec des mails destinés au phishing qui détectent leurs signalements comme "potentiellement dangereux" et se réécrivent seuls pour échapper à la détection. Ou des *malwares* qui, pour rester sous les radars, réécrivent leur code en permanence. Le tout sans la moindre intervention humaine. »

Certains, comme le professeur de cybersécurité à l'UCLouvain Axel Legay, estiment que ce type d'attaque existe déjà même si c'est extrêmement compliqué de les détecter. Pour l'expert finnois, en revanche, cela ne fait pas un pli : ces attaques devraient se généraliser dans les prochaines années.

Automatisation des attaques ou pas, ces groupes se professionnalisent à la vitesse grande V. « Depuis quelques années, ils jouent même les mercenaires et proposent leurs services aux plus offrants sur les forums les plus obscurs », assure Michaël Dantinne, professeur de criminologie à l'ULiège. « On parle de "DDoS as a service" ou de "Ransomware as a service", des attaques clés en main rendues accessibles à ceux dont les connaissances techniques sont limitées et qui souhaitent s'en prendre à une cible. Aujourd'hui, avec ces prestataires de service d'un nouveau genre, pirater le poste de travail d'un collègue ou espionner un proche est accessible en deux clics, ou presque. »

en Ukraine Des cybe

TH. CA

Fin février, le célèbre groupe de hackers Conti a annoncé dans un communiqué qu'il prêtait allégeance à la Russie et lancera des représailles envers toute structure qui viserait le pays d'une cyberattaque. Dans la foulée, un ou plusieurs membres du groupe, mécontents de cette prise de position, ont fait fuiter quelques milliers de messages internes à Conti. Des documents critiques, s'étalant sur plusieurs années, qui révèlent de nombreux détails sur l'organisation criminelle et l'identité de ses membres. « Ces documents ont permis de constater que Conti fonctionne sur de nombreux points comme une entreprise traditionnelle qui vend ses services aux plus offrants sur le *dark web* », relève Mikko Hyppönen. « Ils ont même instauré un système d'"employé du mois". »

Mais après ces révélations, au lieu d'être démantelé, le groupe a continué à agir : « Cela montre bien les accointances entre ces pirates et les autorités russes », conclut le directeur de la recherche chez WithSecure. « Jusqu'ici, on constatait une forme de laisser-faire de la part de la Russie. Désormais, on peut parler de protection puisque de nombreux membres de l'organisation