Le marché lucratif des vulnérabilités informatiques

written by Jacques-André Fines Schlumberger | 3 mai 2022

2,5 millions de dollars : c'est la somme que s'engage à payer Zerodium à celui qui trouvera une vulnérabilité dite *« zero-day »* et *« zero-click »* sur les téléphones Android, c'est-à-dire une faille de sécurité, inconnue de tous, qui permet de prendre le contrôle de l'appareil de manière invisible. Qu'il soit noir, gris ou blanc, le marché des vulnérabilités informatiques se professionnalise.

Les vulnérabilités informatiques dites *« zero-day »* sont des failles de sécurité dans des logiciels qui n'ont pas encore été portées à la connaissance de l'éditeur et n'ont donc pas encore fait l'objet de correctifs. Par conséquent, elles peuvent être exploitées pendant un certain laps de temps avant que leur découverte ne soit rendue publique (voir *La rem* n°59, p.30). Ces vulnérabilités informatiques sont vendues de plus en plus cher par des entreprises de sécurité, un marché dont Zerodium est le leader mondial. Les acheteurs peuvent ainsi opérer des attaques informatiques sophistiquées comme le vol ou la destruction de données ou encore la prise de contrôle à distance d'une machine, voire d'installations informatiques plus complexes. Comme l'explique en toute transparence le site web de Zerodium, *« nos clients sont des institutions gouvernementales (principalement d'Europe et d'Amérique du Nord) qui ont besoin d'exploits* zero-day *avancés et de capacités de cybersécurité »*.

Selon Hervé Debar, chercheur en cybersécurité à Télécom Sud Paris, *« ces offensives peuvent être un moyen de récupérer des informations secrètes sur des projets industriels, économiques ou politiques. Elles permettent au responsable de se dissimuler et de rendre difficile l'identification de l'origine de l'attaque, ce qui les rend particulièrement dangereuses »*. En 2010, un ver informatique, appelé Stuxnet, a été développé à partir de plusieurs vulnérabilités *zero-day* par la National Security Agency (NSA) américaine, en collaboration avec une agence de sécurité israélienne, pour s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium. Les États-Unis entretiennent une législation relativement floue concernant cette pratique de vente de vulnérabilités informatiques, probablement parce qu'ils en sont les premiers clients, mais sans présager de ce qu'en feraient d'autres acquéreurs.

Zerodium, leader mondial en la matière, a commencé sous le nom de Vupen Security. Fondée en 2004 à Montpellier par Chaouki Bekrar, alors âgé de 24 ans, Vupen Security avait pour objet de traquer l'existence de vulnérabilités informatiques dans les logiciels des plus grands éditeurs

mondiaux. En 2012, l'entreprise fait parler d'elle en exploitant une faille sur le navigateur Google Chrome, et refuse l'offre de Google qui propose de racheter l'information 60 000 dollars. *« Nous ne partagerions pas cette faille avec Google, même pour un million de dollars,* déclare alors Chaouki Bekrar au magazine Forbes en mars 2012*. Nous ne voulons pas leur transmettre de quoi les aider à corriger cet exploit ou d'autres exploits similaires. Nous voulons garder cela pour nos clients. »* Le ton est donné.

En 2014, Vupen Security décide de cesser son activité en France, notamment parce que l'étau législatif se resserre en Europe. En décembre 2014, l'entrée en vigueur d'un amendement durcit les modalités de contrôle à l'exportation de telles vulnérabilités informatiques, modalités inscrites dans l'Arrangement de Wassenaar. Ce régime multilatéral de contrôle des exportations a été mis en place en 1996 par trente-trois États (aujourd'hui au nombre de quarante-deux) afin de coordonner leurs politiques respectives en matière d'exportations d'armements conventionnels, ainsi que de biens et technologies à double usage. Fin 2013, Vupen Security avait déjà un bureau à Annapolis, aux États-Unis, situé à quelques kilomètres du siège de la NSA. Deux ans plus tard, Chaouki Bekrar a lancé, avec quelques associés, Zerodium, dont le siège est aujourd'hui à Washington. Cette plateforme achète, auprès d'une communauté forte de 1 500 hackers, des vulnérabilités informatiques critiques, revendues par la suite à des tiers. Elle compte parmi ses clients les services de sécurité des États-Unis, de l'Angleterre ou d'Allemagne, mais aussi d'autres entreprises de « sécurité informatique » comme la société israélienne NSO Group, éditrice du logiciel d'espionnage Pegasus qu'elle a vendu à des États peu scrupuleux et à des dictatures (voir *La rem* n°59, p.30).

Selon plusieurs bases de données, dont celle tenue par une équipe de chercheurs en sécurité de Google, connue depuis 2014 sous le nom « Project Zero », *« au moins 66 vulnérabilités zero-day ont été découvertes en 2021, soit près du double de celles découvertes en 2020 et plus que pour toute autre année enregistrée »*. Cette recrudescence de failles *zero-day* peut s'expliquer par le fait que *« tous les groupes* [malveillants] *dépensent un tas d'argent dans des failles* zero-day *qu'ils utilisent pour eux-mêmes et ils en récoltent les fruits »*, précise le Massachusetts Institute of Technology (MIT), lors de propos rapportés par le lemondeinformatique.fr.

Ce marché des vulnérabilités *zero-day* est à distinguer des programmes de *bug bounty*, « chasses aux bugs » ou « prime à la faille », proposés par de nombreux éditeurs de logiciels et organisations parmi lesquels Facebook, Google, Microsoft ou encore le département américain de la Défense. Il s'agit dans ce cas de rémunérer quelques centaines ou milliers de dollars les personnes qui identifient et signalent des vulnérabilités informatiques. Certains programmes sont organisés de

manière confidentielle par une entreprise qui souhaite faire appel à des hackers et des chercheurs en sécurité. D'autres se déroulent publiquement, par l'intermédiaire de plateformes comme la française Yogosha, le leader européen YesWeHack, la néerlandaise Zerocopter, ou encore les américaines HackerOne, Bugcrowd et Zero Day Initiative (ZDI).

Créé en 2013, YesWeHack propose à des entreprises de soumettre leurs logiciels ou applications à une communauté de hackers qui seront rémunérés selon les failles de sécurité qu'ils repèrent. *« Nos hackers, tous indépendants, ne travaillent que pour le compte des clients dont ils ont découvert les vulnérabilités »*, explique Romain Lecoeuvre, directeur technique de YesWeHack. En mai 2020, l'application de traçage de contacts StopCovid (voir *La rem* n°54, p.31) a ainsi fait l'objet d'un tel programme, organisé par la start-up française à la demande de l'Institut national de recherche en informatique et en automatique (Inria) et de l'Agence nationale de la sécurité des systèmes d'information (Anssi). Ce qui a permis d'identifier environ une dizaine de problèmes plus ou moins graves. Un marché foncièrement différent de celui des vulnérabilités *zero-day* dont les principaux clients sont les services de renseignement des pays industrialisés.

Lorsqu'un hacker découvre une faille de sécurité *zero-day*, trois options s'offrent à lui. La première est celle de la vendre sur le marché noir, secrètement, comme cela a toujours été possible. À moins qu'il ne la cède sur le marché gris, « officiellement » *via* une plateforme telle que Zerodium ou à des entreprises de sécurité, Netragard, par exemple, fondée en 2006 aux États-Unis. Ces canaux de distribution sont légaux dans certains pays, mais ils reposent sur une législation floue et permissive comme aux États-Unis, sachant que l'éditeur du logiciel interdit par principe ce type de commerce. En France et en Europe, la vente de telles failles de sécurité est interdite. La troisième option du hacker qui souhaite vendre une faille de sécurité sera de contacter l'éditeur du logiciel concerné afin que ce dernier le dédommage éventuellement pour sa découverte, à moins de la soumettre à une plateforme de *bug bounty.*

Selon le rapport annuel de la plateforme américaine HackerOne pour l'année 2020, *« les pirates ont signalé plus de 181 000 vulnérabilités valides et la valeur commerciale de chaque vulnérabilité découverte est, en moyenne, de 979 dollars »*. Si l'appât du gain constitue la principale motivation du pirate chercheur de faille de sécurité, les sommes colossales offertes par le marché gris ont de quoi ébranler l'éthique du métier.

Sources :

- The Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies, wassenaar.org.

- « Meet the hackers who sell spies the tools to crack your PC (and get paid six-figure fees) », Andy Greenberg, forbes.com, March 21, 2012.
- « Prism : le révélateur du lucratif (et très discret) business de la vente de failles » Reynald Fléchaux, silicon.fr, 6 septembre 2013.
- « Vente de failles et d'exploits : le français Vupen a bien fourni la NSA », Reynald Fléchaux, silicon.fr, 18 septembre 2013.
- « Dans l'ombre de Vupen, Zerodium programme les chasseurs de failles zero-day », Ariane Beky, silicon.fr, 27 juillet 2015.
- « Hacking the Army », Kate Conger, techcrunch.com, January 19, 2017.
- « Zero-day : de quoi parle-t-on ? », Orange Cyber Défense, orangecyberdefense.com, 11 avril 2019.
- « Il est désormais plus compliqué de pirater un smartphone sous Android qu'un iPhone », Gilbert Kallenborn, 01net.com, 4 septembre 2019.
- « Coronavirus : les hackers font passer un sale quart d'heure à l'appli StopCovid », SudOuest.fr avec AFP, sudouest.fr, 28 mai 2020.
- « Piratage : Zerodium, la discrète place de trading des failles informatiques fondée par un Français », Delphine Dechaux, challenges.fr, 29 juillet 2021.
- « Record des failles zero-day en 2021 », Dominique Filippone, lemondeinformatique.fr, 24 septembre 2021.
- « Attaques zero-click : l'espionnage à l'ère des smartphones », Rémy Fauvel, imtech.wp.imt.fr, Institut Mines-Télécom, 12 octobre 2021.
- « Recherche de faille de sécurité chez un tiers, chantage à l'image de marque ? », Arthur Sicard, École de guerre économique, ege.fr, 8 novembre 2021.
- « How hackers can strengthen cloud security for applications », HackerOne, hackerone.com, November 11th, 2021.