Le piratage gouvernemental

De quoi s'agit-il et quand devrait-il être utilisé?

Août 2022

Le cryptage est un élément crucial de notre vie quotidienne. Presque partout dans le monde, des aspects fondamentaux de notre vie reposent sur le cryptage. Les réseaux électriques, les transports, les marchés financiers, mais aussi les babyphones[1] sont plus fiables grâce au cryptage. Le cryptage protège nos données les plus vulnérables contre les criminels et les terroristes, mais peut également permettre de dissimuler des données criminelles aux autorités.

Le piratage gouvernemental est l'une des techniques utilisées par les agences de sécurité nationale et les forces de l'ordre afin d'accéder à des informations cryptées (par ex.: le FBI a fait appel à une entreprise de piratage pour déverrouiller l'iPhone au cœur de l'affaire de San Bernardino[2]). Cette technique vient s'ajouter à d'autres stratégies visant à obtenir un accès exceptionnel[3] en demandant, ou en imposant, aux entreprises technologiques de disposer des moyens techniques de décrypter les données des utilisateurs lorsque cela est nécessaire à des fins légales.

L'Internet Society considère que la robustesse du cryptage est vitale pour Internet, et est vivement préoccupée par toute politique ou action susceptible de nuire au cryptage, quel que soit le motif invoqué. Le piratage gouvernemental entraîne un risque de dommages collatéraux, à la fois pour Internet et pour ses utilisateurs, et ne devrait donc être envisagé qu'en tant qu'outil de dernier recours, à déployer dans des conditions strictes avec des garanties vérifiables.

Définition du piratage gouvernemental

Nous définissons le « piratage gouvernemental » comme l'exploitation par des entités gouvernementales (ex.: agences de sécurité nationale, forces de l'ordre ou acteurs privés agissant en leur nom) de vulnérabilités dans des systèmes, des logiciels ou du matériel, afin de pouvoir accéder à des informations qui seraient sans cela cryptées ou inaccessibles.

1 Les babyphones et caméras de sécurité bien conçus devraient sécuriser leurs données pour assurer leur confidentialité sur Internet. Ce n'est pas toujours le cas.

2 https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute#Apple_ordered_to_assist_the_FBI

3 https://www.internetsociety.org/wp-content/uploads/2019/05/FactSheet-EncryptionVsLawfulAccess-FR.pdf

Les dangers du piratage gouvernemental

L'exploitation de vulnérabilités de quelque nature que ce soit, à des fins de maintien de l'ordre, de tests de sécurité ou pour tout autre objectif, ne doit pas être prise à la légère. D'un point de vue technique, le piratage d'une ressource technologique, d'information ou de communication (TIC) sans l'accord de son utilisateur ou de son propriétaire est toujours une attaque, quel que soit le motif. Les attaques peuvent endommager un appareil, un système ou un flux de communication actif, ou les laisser dans un état moins sécurisé. Cela augmente significativement le risque de violations ultérieures et met potentiellement en danger l'ensemble des utilisateurs du système.[4]

Les risques sont encore plus importants lorsque les gouvernements exploitent des vulnérabilités « zero-day », des vulnérabilités matérielles ou logicielles dont le fournisseur n'a pas connaissance ou qui n'ont pas encore été atténuées (par ex. : aucun correctif n'a été publié). Cette approche est particulièrement dangereuse, car elle expose Internet et ses utilisateurs à de nouveaux risques, contre lesquels il n'existe aucun moyen de se protéger. Pour cette raison, des processus clairs doivent être mis en place pour la divulgation responsable et l'atténuation coordonnée des vulnérabilités de sécurité découvertes dès que possible afin qu'elles puissent être traitées.[5]

Les exploitations de vulnérabilités peuvent être volées, fuiter ou être répliquées. Même des entités gouvernementales disposant des meilleurs niveaux de sécurité ont été compromises. Ainsi, le groupe ShadowBrokers a piraté la National Security Agency américaine (la NSA) et a rendu public EternalBlue, l'exploitation de vulnérabilité zero-day de l'agence[6]; Hacking Team, une entreprise italienne de sécurité, a été piratée en 2015[7]; et Vault 7, un ensemble d'outils de piratage de la Central Intelligence Agency, a fuité en 2017.[8]

Toute exploitation de vulnérabilité, quelle que soit son origine, peut être adaptée par des criminels ou des États-nations pour attaquer des utilisateurs innocents. Le rançongiciel Petya/NotPetya (basé sur EternalBlue) a entraîné des conséquences tangibles, notamment des retards pour des traitements médicaux, la suspension d'opérations bancaires et la perturbation de services portuaires.[9] Ces incidents mettent en évidence les risques que font courir toutes les entités (y

4 Le piratage technique peut également nuire à l'intégrité des preuves numériques, compromettant ainsi l'application efficace de la loi et le processus judiciaire.

5 Cela va bien au-delà d'un appel à créer des procédures d'évaluation et de gestion des vulnérabilités (comme https://cyberstability.org/norms/#toggle-id-5) car cela appelle à divulguer toutes les vulnérabilités.

6 https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html

7 https://www.vice.com/en_us/article/3k9zzk/hacking-team-hacker-phineas-fisher-has-gotten-away-with-it

8 https://fr.wikipedia.org/wiki/Vault_7

9 https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how

compris les gouvernements) qui collectionnent des vulnérabilités zero-day et créent ou conservent des exploitations de ces vulnérabilités.

Les équipes de piratage commercial ne vendent pas uniquement leurs services aux « gentils ». En 2019, des chercheurs dans le domaine de la sécurité ont découvert que les logiciels de NSO Group, une société israélienne de renseignement informatique, utilisés par de nombreuses agences gouvernementales, avaient servi à pirater secrètement les comptes WhatsApp de journalistes et d'activistes afin de surveiller leurs communications. D'autres reportages similaires révèlent qu'il ne s'agissait en aucun cas de la seule utilisation de la technologie.[10] [11] [12] [13]

Une cible peut se transformer en plusieurs cibles. Le piratage gouvernemental peut être conçu pour être ciblé et chirurgical, mais une technique de piratage ou une exploitation de vulnérabilités qui fonctionne sur une seule cible peut être utilisée contre d'autres appareils du même type, et souvent aussi d'autres logiciels et systèmes. Des vulnérabilités et des outils peuvent également être découverts ou divulgués de manière inappropriée, ou utilisés à d'autres fins, par exemple pour s'engager dans des cyberattaques ou une cyberguerre par des acteurs de la menace persistante avancée (en anglais, Advanced Persistent Threat ou APT)[14], qui poursuivent souvent les objectifs d'un État. L'exemple le plus célèbre d'APT est le virus Stuxnet, qui aurait été créé par les gouvernements américain et israélien pour détruire les centrifugeuses nucléaires iraniennes, puis s'est répandu à travers le monde (bien au-delà de sa cible initiale) en affectant des millions d'autres systèmes.[15]

Les auteurs d'attaques découvrent continuellement de nouveaux points faibles dans les systèmes informatiques. Le fait de dissimuler un point faible (afin de l'exploiter par la suite) n'empêchera pas que celui-ci soit découvert par d'autres acteurs. Par exemple, pour le système d'exploitation Android, le taux de redécouverte des points faibles de gravité élevée ou critique a atteint 23% en un an.[16] Étant donné l'existence de ces points faibles, les acteurs les plus motivés, comme les criminels, les terroristes et les gouvernements hostiles, tenteront plus que quiconque de les trouver

10 https://www.nytimes.com/2019/05/13/technology/nso-group-whatsapp-spying.html
11 https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html
12 https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/
13 https://www.wired.com/story/nso-group-pegasus-el-salvador/
14 https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html
15 https://www.cybereason.com/blog/advanced-persistent-threat-apt
16 Herr & Schneier: "What You See Is What You Get: Revisions to Our Paper on Estimating Vulnerability Rediscovery" (Lawfare 2017) https://www.belfercenter.org/sites/default/files/files/publication/Vulnerability%20Rediscovery%20%28belfer-revision%29.pdf

et de les exploiter. Les prix et la demande pour ces points faibles sur le marché noir et le marché gris illustrent bien leur importance.[17] Le fait de disposer d'exploitations de vulnérabilités pouvant servir de base pour la rétro-ingénierie rendra cette tâche encore plus facile.

Le franchissement des juridictions. Ces techniques induisent également le risque d'infiltrer ou d'altérer par inadvertance les réseaux ou systèmes d'un autre État, ce qui pourrait être considéré comme une attaque contre cet État, ses intérêts ou ses citoyens, et engendrer des conséquences politiques et économiques et potentiellement des cyberattaques. Cela pourrait également inciter certains pays à adopter une approche de souveraineté pour Internet.

La position de l'Internet Society sur le cryptage et le piratage gouvernemental

En tant qu'élément technique à la base de la confiance sur Internet, le cryptage facilite la liberté d'expression, le commerce, la confidentialité et la confiance des utilisateurs. Il contribue à protéger les données et les communications contre les dommages accidentels et malveillants. L'Internet Society estime que le cryptage devrait être la norme pour le trafic Internet et le stockage des données, et elle n'est pas la seule à le penser. Par exemple, le rapporteur spécial de l'ONU pour les Droits de l'homme et l'OCDE ont très clairement déclaré leur soutien aux outils de cryptage.[18]

Les tentatives légales et techniques visant à limiter le recours au cryptage, même si elles partent d'une bonne intention, auront un impact négatif sur la sécurité des citoyens respectueux de la loi et sur Internet dans son ensemble.

Le piratage gouvernemental visant à contourner le cryptage nuit également à la sécurité d'utilisateurs innocents, de systèmes critiques (notamment des réseaux et services gouvernementaux) et d'Internet.

Nous ne soutenons pas le piratage gouvernemental, qui engendre un risque pour la sécurité d'Internet et des internautes. À cause de ce risque de dommages collatéraux, cette solution ne devrait jamais devenir une technique normale utilisée par les forces de l'ordre ou les gouvernements afin d'obtenir l'accès à des données cryptées. Nous nous opposons également aux lois, ainsi qu'aux autres règlements, qui exigent des entreprises de technologies qu'elles créent des failles de sécurité

17 Voir par ex. https://en.wikipedia.org/wiki/Cyber-arms_industry#Notable_markets pour quelques exemples cités de ces marchés

18 Voir https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx et http://www.oecd.org/sti/ieconomy/cryptography.htm respectivement.

dans leurs produits et services. Il existe de nombreuses preuves que de telles vulnérabilités sont inévitablement divulguées ou découvertes et utilisées à des fins nuisibles.

Le risque est particulièrement élevé pour les piratages gouvernementaux basés sur des vulnérabilités zero-day et leur exploitation (comme expliqué ci-dessus). Cependant, il existe également un risque lorsque les vulnérabilités sont connues mais non corrigées - peut-être parce que les systèmes sont trop anciens, parce que les gens ne peuvent pas se permettre des appareils plus sécurisés ou en raison de procédures de correction inadéquates.

En règle générale, l'exploitation des failles de tout système crée un risque inhérent. Même dans le scénario le plus optimiste, selon lequel une entité gouvernementale animée des meilleures intentions exploite une vulnérabilité avec les autorisations adéquates et avec un résultat positif, le risque que cette exploitation de vulnérabilité ne reste pas limitée à ce gouvernement est élevé. Le système dans son ensemble devient moins sûr simplement du fait de l'exploitation de cette vulnérabilité, quelle que soit l'intention.

Étant donné les risques inhérents, les gouvernements ne devraient pas récupérer, acheter, créer, conserver ou exploiter des vulnérabilités afin d'obtenir l'accès à des informations à des fins de sécurité nationale ou d'application de la loi si les conditions suivantes ne sont pas respectées:

- Sérieux: il peut être démontré que cela est nécessaire pour protéger des vies humaines, contrer des risques imminents et significatifs pour la sécurité publique ou empêcher des crimes d'une extrême gravité.
- Dernier recours: il n'existe aucune alternative viable.
- Judiciaire: cela est fait dans le cadre d'un mandat judiciaire exécuté correctement.
- Proportionnel: une opération peut être objectivement considérée comme une mission ciblée et proportionnelle, définie de la manière la plus restrictive possible.
- Limitation des risques: il n'existe pas de risque de dommage ou de préjudice à la sécurité d'autrui.
- Procédural: une évaluation de l'impact, basée sur des critères établis, doit être effectuée et prise en compte en avance. Les critères doivent être transparents et définis par les parties prenantes concernées, et régulièrement revus. Ce processus devrait notamment inclure des organismes de maintien de l'ordre, des juges, des spécialistes techniques et la société civile.
- Limité: chaque cas de piratage gouvernemental doit être autorisé sur la base de critères préapprouvés et avec une date de fin claire. Les autorisations « continues » (renouvelées par défaut toutes les quelques semaines ou tous les mois) ne doivent pas être utilisées pour contourner cette exigence.

Jamais dans l'histoire de l'humanité autant de données n'ont été mises à la disposition des gouvernements et de leurs organismes chargés de l'application de la loi: en effet, dans certains cas, l'application a échoué non pas à cause d'un manque de données, mais à cause d'un excès de données.[19] [20]

L'Internet Society exhorte les gouvernements à donner la priorité à d'autres voies pour la collecte, l'analyse et l'utilisation d'informations et de preuves, afin de ne pas compromettre la sécurité des appareils, des logiciels et des services Internet. Cela comprend l'analyse d'une vaste quantité de renseignements en open source, des données accessibles dont disposent les fournisseurs de service, des métadonnées des communications concernées, et la collecte de preuves non numériques, telles que les informations de témoins et les documents.

19 https://www.theguardian.com/uk/2006/may/11/july7.uksecurity [2006]

20 https://www.techdirt.com/2013/09/10/problem-with-too-much-data-mistaking-signal-noise/ [2013]