LE TEMPS

OPINION ABONNÉ

Que faire quand même les premiers ministres se font pirater leur téléphone?

OPINION. Affaires Pegasus, espionnage économique… Le vrai chiffre des piratages de smartphones est immense, soutient le militant de la démocratie numérique Rufo Guerreschi, qui propose avec sa Trustless Computing Association à Genève des pistes de solutions

Image prétexte — © Karl-Josef Hildenbrand/Keystone

Rufo Gueresschi
militant, entrepreneur dans le domaine de la démocratie numérique

Publié lundi 30 janvier 2023 à 16:42
Modifié mercredi 1 février 2023 à 09:15

Novembre 2022, on apprend que le portable de l'ancienne ministre britannique des Affaires étrangères Liz Truss, a été espionné pendant des mois, lors de conversations avec des collègues, des amis et des diplomates étrangers. Quelques jours plus tard, c'est au tour du président et ministre des Affaires étrangères de la Suisse, Ignazio Cassis, dont on découvre que comme 100 autres hauts fonctionnaires, il a été victime de piratage par des gangs de pirates indiens, via des cabinets d'avocats britanniques.

Ils sont en bonne compagnie. Rien que l'année dernière, les premiers ministres en exercice d'Espagne et de Finlande, les chefs de l'opposition en Grèce et en Pologne, le fils du nouveau premier ministre d'Israël et le rédacteur en chef du Financial Times ont subi le même sort. L'ampleur de ce «Watergate européen» et des solutions possibles sont détaillées dans un rapport de 150 pages sur les logiciels espions qui choque, et qui a été présenté il y a quelques semaines par une commission spécialisée du Parlement européen.

Toujours l'année dernière, le ministre de la Défense britannique et plusieurs parlementaires européens ont été dupés par des agents étrangers se faisant passer pour l'avocat d'un leader de l'opposition russe. Même le président des États-Unis court ce genre de risques, expliquait le *New York Times* en 2018.

Comment pourrions-nous espérer que les autres premiers ministres, y compris Macron, Scholz, Meloni et Lula da Silva, leurs ministres, leurs parlementaires et/ou leurs proches collaborateurs ne soient pas eux aussi continuellement piratés sur leurs smartphones? Ont-ils accès à de meilleurs outils, une protection magique qui dépasserait celle du GCHQ britannique pour Mme Truss?

Tout aussi inquiétant, les smartphones actuels permettent à leurs utilisateurs de supprimer de manière fiable les preuves de hacking afin d'échapper à toute responsabilité pénale, comme l'ont montré les enquêtes sur les services secrets du président américain et sur des dirigeants d'une grande banque suisse, alors que les criminels peuvent avoir obtenu ces preuves avant leur suppression pour les utiliser dans le cadre d'un chantage.

Aussi terrible que cela soit pour nos démocraties, ce n'est que la partie émergée de l'iceberg, car le nombre de victimes se chiffre très probablement en centaines de milliers, comme nous allons le voir. Presque toutes les personnes qui ont du pouvoir ou de l'argent sont des cibles ou des victimes, y compris non seulement les élus et les politiciens, mais aussi un grand nombre de diplomates, hommes d'affaires, journalistes, militants, organisations, collaborateurs des organisations intergouvernementales...

Cet état de fait constitue une menace vitale pour nos démocraties et les droits de l'homme, et étouffe et fausse considérablement le dialogue diplomatique.

Nos responsables politiques sont-ils négligents? Pourquoi n'utilisent-ils pas leurs téléphones cryptés professionnels?

Bien sûr, ils pourraient et devraient être plus prudents, partant du principe que toute utilisation de leur smartphone peut entraîner un chantage, de l'extorsion ou du «public shaming», une exposition publique qui fait honte, car des morceaux de leur vie, légaux ou pas, pourraient se retrouver dans les médias, ou aux mains de procureurs.

La plupart des dirigeants sont désormais au courant des risques; pourtant ils continuent à utiliser leurs téléphones «pour les mêmes raisons que nous tous», a écrit *The Economist* après le piratage de Liz Truss. La même attaque contre un téléphone de fonction protégé aurait été plus difficile. Mais ces téléphones sont encombrants. Il faut saisir de longs mots de passe à chaque utilisation; il faut l'autorisation du service informatique pour installer les applications dont on a besoin; les applications de chat sont souvent configurées avec une fastidieuse authentification à deux facteurs. Et, surtout, les discussions de tous les jours avec les collègues politiques ne se font pas sur ce téléphone. Car «c'est pénible d'avoir deux appareils», écrit encore *The Economist*.

Les dirigeants sont obligés d'utiliser des téléphones mobiles, des magasins d'applications et les applications grand public s'ils veulent fonctionner un tant soit peu dans leur travail ou leur vie, alors que, de toute évidence, aucun outil de protection de leurs agences de sécurité n'est un tant soit peu suffisant.

Ils se contraignent donc à une importante autocensure pour minimiser les risques, avec des coûts énormes en termes d'efficacité. De plus, il est difficile d'attribuer les piratages sur les appareils d'aujourd'hui, il est souvent impossible de savoir si une fuite est due à un pirate ou à l'interlocuteur de la victime, comme on l'a vu dans l'affaire du piratage du premier ministre finlandais Sanna Marin; cela favorise la méfiance entre associés et une plus grande autocensure.

Les hackers sont-ils juste trop bons? Ne peut-on pas rendre ces téléphones plus sûrs?

Chaque année, Apple, les principaux fabricants de téléphones Android, et les fabricants de suites de protection en cybersécurité introduisent de nouvelles améliorations. Mais comme un mirage, une sécurité décente reste toujours hors d'atteinte.

Comment cela est-ce possible? Bien sûr, les pirates – qu'ils agissent ou non au nom d'un État – disposent de sommes considérables, et en hausse permanente. Mais nous savons comment créer des normes et des dispositifs informatiques à la fois fiables et sûrs contre les attaques les plus avancées, et accessibles à l'interception uniquement par des entités convenues, comme l'indique une étude de la Trustless Computing Association; cela a été prouvé dans les faits par Crypto AG, le leader suisse des communications diplomatiques et top secrètes occidentales pendant la guerre froide, dont il a été révélé en 2020 qu'elles avaient été interceptées par deux agences de renseignement.

Il existe deux causes profondes à cette insécurité chronique. D'abord, la concurrence dans les smartphones haut de gamme entraîne hyper-complexité et secrets de fabrication, de quoi assurer des fonctions de divertissement riches et performantes. Deuxièmement, il y a le besoin non avoué de s'assurer subrepticement que plusieurs nations puissantes peuvent les pirater à tout moment pour contrer les criminels ou les nations terroristes, ennemies ou adverses.

Enfin, transporter un appareil supplémentaire peut être acceptable pour les personnes les plus potentiellement ciblées, mais pas pour leurs nombreux interlocuteurs sensibles non classifiés.

Des centaines de milliers de victimes probables

Aussi critique qu'il soit, le problème est-il limité aux hauts fonctionnaires? Le nombre réel des victimes de piratage est très difficile à estimer, puisque à dessein, il est prioritaire pour les agences de renseignements de faire en sorte que les criminels et les terroristes surestiment la sécurité de l'informatique sécurisée, tandis que les entreprises informatiques sécurisées jouent le jeu, pour des raisons de rentabilité. Mais de temps en temps, des données concrètes sont publiées.

Le procès intenté par Facebook au groupe NSO a montré que plus de 1400 comptes WhatsApp avaient été piratés dans le monde en l'espace de deux semaines. En juin 2022, le groupe NSO justement a témoigné devant les 42 membres de la commission PEGA du Parlement européen, qui travaille sur les logiciels espions. Plus de 12 000 citoyens par an sont piratés via son système Pegasus, selon ses déclarations. Or ce n'est que la partie émergée de l'iceberg, car ce nombre ne prend pas en compte (1) les dizaines d'autres sociétés de logiciels espions similaires qui louent ou vendent leurs solutions à des nations et à des groupes privés; (2) les personnes directement piratées par les agences de renseignements des pays puissants et leurs mandataires; (3) les centaines ou milliers d'autres entités qui trouvent, achètent, volent ou simplement payent pour accéder illégitimement à des utilisateurs à haut profil, comme l'ont montré les scandales Shadow Brokers et Vault 7, conséquence de la manière subreptice dont les nations puissantes s'assurent de maintenir accès «backdoor».

Il faut aussi savoir aussi qu'une grande majorité de ces cybercrimes mettent des mois ou années à être identifiés (quand ils le sont) car ils ne laissent souvent aucune trace. Lorsqu'ils sont découverts, ils restent presque toujours secrets, car victimes comme agresseurs n'ont rien à gagner à les signaler. Les victimes ne sont pas tenues de divulguer un piratage. Le piratage de hauts fonctionnaires est souvent classé secret d'État.

En 2018, le *New York Times* indiquait, à propos du groupe NSO: «Les clients pouvaient payer plus pour cibler des utilisateurs supplémentaires, en bénéficiant de remises sur les gros volumes: 800 000 dollars pour 100 téléphones supplémentaires», ce qui donne un prix de 8000 euros par cible – c'est plus cher apparemment aujourd'hui.

Ainsi, le véritable nombre de personnes piratées est loin des 12 000 citées, il pourrait approcher les centaines de milliers.

Les personnes les plus ciblées sont au courant. Des enquêtes UBS et Northern Trust menées avant la crise du Covid ont montré que la cybersécurité est la préoccupation principale pour les 16 millions de personnes les plus riches du monde, et la 2e préoccupation la plus importante pour les family offices. L'argent ne suffit pas. Même les plus riches n'ont nulle part où se cacher, pour ne rien dire des journalistes et des militants: il y a une véritable urgence démocratique, et une énorme demande non satisfaite.

Certes en 2021, Apple a déclaré qu'il ne fallait pas s'inquiéter de ces hackings car les programmes pirates «coûtent des millions de dollars à développer, ont souvent une faible durée de vie et sont utilisés pour cibler des individus spécifiques». Ce n'est pas une menace «pour l'écrasante majorité de nos utilisateurs»: mais cette expression «d'écrasante majorité de nos utilisateurs» est tout à fait compatible avec des centaines de milliers d'appareils exposés, soit 0,01% du 1,5 milliard d'iPhones existants…

L'interdiction ou la réglementation des logiciels espions pourraient-elles être une solution?

Un récent rapport de 150 pages d'une commission du Parlement européen, qui suit les recommandations des principales organisations de défense des droits de l'homme basées aux États-Unis, évoque un «watergate européen». Mais un moratoire, voire une interdiction des logiciels espions, n'empêcheraient pas les pays non réglementés et les criminels d'espionner, tandis que les agences de sécurité dûment autorisées, elles, ne pourraient pas intercepter les criminels les plus dangereux.

Des réglementations appropriées seraient plus utiles et nécessaires, mais elles sont soumises à des complexités techniques et juridictionnelles largement insolubles, inhérentes à la manière dont les logiciels espions sophistiqués sont construits et déployés à l'échelle mondiale, et à la complexité et au secret des appareils mobiles sécurisés, qui rendent leur application largement inefficace.

Vers une solution plus complète et efficace

Une solution efficace doit donc inévitablement d'abord garantir que les appareils mobiles largement accessibles aux utilisateurs sensibles ne soient pas simplement plus résistants aux attaques les plus sophistiquées, mais qu'ils le soient radicalement. Nous savons comment faire, comme nous l'avons mentionné plus haut à propos de Crypto AG, et comme le prouvent aussi nos réussites dans la sécurité nucléaire et l'aviation civile.

Mais alors, qui garantit et s'assure que la meilleure ingénierie possible soit appliquée et que les plus puissantes tentatives de compromission soient bien déjouées? Et comment faire pour que ces dispositifs soient adoptés en masse sur le marché hégémonique des appareils mobiles? Comment empêcher que ce soient des criminels, des terroristes et des nations adverses qui les utilisent? Il faut que les solutions appropriées bénéficient de la confiance d'une grande majorité de personnes sensibles dans le monde entier, et qu'elles ne permettent qu'un accès légitime et légal, national et international.

Pour être adoptées à grande échelle par une grande majorité des interlocuteurs habituels de nos élus et autres personnes vulnérables, ces solutions doivent être suffisamment pratiques et bon marché. La plus sûre des applications de messagerie sécurisée à code source ouvert que tout le monde peut consulter, ne peut être aussi sûre que l'appareil sur lequel elle fonctionne.

La réponse doit être un dispositif matériel autonome supplémentaire. Mais personne n'a envie de transporter un dispositif supplémentaire. Heureusement, la même miniaturisation qui permet aujourd'hui de plier les téléphones pourrait permettre d'intégrer un dispositif ultra-mince, minimaliste mais ultra-sécurisé, à l'arrière de n'importe quel smartphone ou de le transporter à l'envers dans des étuis, voire portefeuilles en cuir personnalisés, pour ceux qui préfèrent cela.

Pour bénéficier d'une confiance globale, tous les processus et techniques critiques de la solution et de son utilisation doivent être suffisamment ouverts et contrôlables. La sécurité la plus élevée ne pouvant plus être vérifiée après coup, il faut que tous les composants techniques et humains – le codeur, l'architecte de données, le fournisseur de technologie, le fabricant de la puce et formateur des utilisateurs – soient soumis à une transparence totale et à une surveillance extrêmement fiable.

La conception et la surveillance devraient être assurées par un organisme international dont la qualité de la gouvernance serait évaluée par des citoyens relativement éduqués et informés, tout comme cela se passe pour les processus et procédures d'élections démocratiques correctement conçus. Il pourrait s'agir d'un mélange de nations diversifiées au niveau mondial, d'organisations intergouvernementales et d'organisations non gouvernementales, de citoyens du monde choisis au hasard et d'experts «éthiques» reconnus.

Permettre un accès légitime et légal au niveau national et international, tout en réduisant suffisamment le risque d'abus, ne serait pas possible, selon les articles détaillés de plusieurs militants libertaires de la vie privée et des experts en sécurité basés aux États-Unis très influents. Au contraire, il existe des précédents pratiques et des arguments scientifiques solides en faveur d'une procédure de «porte d'entrée» suffisamment sécurisée, supervisée par un tiers de confiance à l'échelle mondiale et impliquant des systèmes informatiques minimisés ultra-sécurisés.

En pratique, c'est ce qu'a montré Crypto AG, le dispositif standard occidental de cryptage basé en Suisse utilisé pour les communications diplomatiques sécurisées pendant la guerre froide, et dont il a été révélé plus tard qu'il était aux mains de la CIA et de son équivalent allemand, qui procédaient à des interceptions systématiques. En théorie, c'est ce que l'auteur de cette tribune a argumenté dans un article publié en 2018: Case for a Trustless Computing Certification Body. Ces deux exemples montrent qu'il est tout à fait possible qu'un organisme de certification international hautement fiable et résilient fonctionne. Certes l'ajout d'un accès «frontal» ajouterait inévitablement une vulnérabilité potentielle supplémentaire, mais une telle approche a de bonnes chances de réduire globalement radicalement ou au moins substantiellement le risque pour la vie privée par rapport à tout autre système informatique sécurisé disponible aujourd'hui, ou en cours de développement, qui n'offre pas une telle «porte d'entrée».

A quoi pourrait ressembler une solution globale?

Une solution plus définitive pourrait impliquer un petit groupe de nations, d'ONG et d'OIG diversifiées à l'échelle mondiale qui s'uniraient pour créer – un organisme de certification intergouvernemental ouvert pour garantir à la fois la plus haute sécurité possible et un accès légal légitime «en personne» sûr, ainsi que

– une nouvelle catégorie de produits, des appareils mobiles minimalistes, ultra-minces, conformes aux prescriptions de cet organisme, qui s'intègre à l'arrière de tout smartphone Android, Harmony et iOS, ou transportable dans des portefeuilles adaptés mais utilisables comme un portefeuille normal, pour toutes les données sensibles des premiers ministres et de tous les citoyens. Le projet s'appuierait sur un ensemble redondant de fournisseurs de technologies critiques dans les pays participants, et sur des technologies open source pour atténuer les perturbations ou les compromissions de la chaîne d'approvisionnement.

Un certain nombre de pays membres et non membres de l'UE, reconnaissant l'impossibilité «institutionnelle» pour l'UE et l'ONU de prendre une telle initiative, pourraient prendre les choses en main en élaborant de telles solutions techniques ouvertes et les institutions intergouvernementales qui seraient capables de garantir le respect de ces exigences – ouvrant ensuite la voie à l'UE, aux autres organisations intergouvernementales régionales et à l'ONU.

Des excellents précédents: le Minitel!

Outre Crypto AG, déjà mentionnée, des initiatives semblables ont déjà été lancées avec succès par l'Allemagne et les États-Unis. La définition et l'adoption conjointes par les États membres de l'UE des normes GSM ont permis à l'UE de devenir le leader du secteur de la téléphonie mobile pendant deux décennies. La France et l'Allemagne se sont associées pour créer la chaîne de télévision publique franco-allemande ARTE et, plus récemment, pour partager une plateforme de «messagerie mobile sécurisée» (basée sur Element/Matrix). Un exemple encore plus proche est le Minitel, cette plate-forme numérique créée par le gouvernement français, qui a connu un grand succès et qui, en 1988, constituait tout un écosystème numérique avec 3 millions d'utilisateurs, des terminaux (ou PC) privés et publics compatibles et conformes, des milliers de services et d'applications privés et publics. Malgré son succès, le Minitel a été remplacé en quelques années par des PC privés s'appuyant sur les systèmes d'exploitation hégémoniques américains, en raison d'une part de leurs meilleures performances et de l'expérience utilisateur, et d'autre part en raison de leurs investissements plus élevés dus à leurs plus grands marchés nationaux et mondiaux, d'un écosystème d'applications interopérables au niveau mondial et de terminaux/PC privés, et du choix du Minitel de permettre à ses services de fonctionner sur les nouveaux PC américains.

Notre initiative pourrait être comprise comme une sorte de version multigouvernementale, mobile et ultra-sécurisée du Minitel. Contrairement au Minitel, il ne serait pas, dans un premier temps, en concurrence directe avec les smartphones commerciaux américains dominants, mais les compléterait par un dispositif matériel complémentaire, sous la forme d'un appareil mobile autonome, de 2 mm d'épaisseur. Ces nouveaux appareils constitueraient un écosystème informatique parallèle offrant des niveaux uniques de confidentialité, de confiance et d'intégrité, que les smartphones américains et chinois n'offrent pas et ne peuvent pas offrir, et que les citoyens réclameront avec insistance, car les wearables, la santé en ligne et les assistants d'intelligence artificielle font de la fiabilité un élément clé des services les plus avancés.

Les grandes puissances du cyberespace se joindraient-elles au projet?

Parce qu'ils contrôlent les principales entreprises privées de sécurité informatique numérique, les États-Unis et Israël ont un avantage distinct apparent, via leur capacité à accéder à de meilleures protections, de meilleures capacités d'espionnage et de meilleures contre-mesures d'espionnage. C'est un fait.

Pourtant, le modèle actuel crée également d'énormes dommages collatéraux à leur propre sécurité nationale, à la démocratie et à leurs relations avec leurs alliés, à tel point que nous pouvons soupçonner qu'ils seraient ouverts à une solution meilleure et multilatérale si elle pouvait être conçue et réalisée.

Si presque toutes les nations seraient les bienvenues dans une telle initiative, aucune n'est nécessaire. Cela dit, il serait très avantageux que quelques nations jouant un rôle clé dans l'architecture mondiale actuelle et future de la cybersécurité - comme les États-Unis, Israël et/ou la Chine - y adhèrent tôt ou tard.

Notre vision, et les prochaines étapes

En tirant parti de niveaux de transparence uniques, ainsi que de la coopération et de la surveillance des nations participantes et des citoyens à tous les niveaux et à toutes les étapes, ces nouveaux dispositifs et les services en nuage associés créeront un cyberespace parallèle au cyberespace hégémonique américano-chinois, qui permettra le dialogue équitable, sage et efficace dont nous avons besoin pour favoriser l'émergence de vérités partagées, d'un dialogue et d'une coordination plus approfondis entre toutes les nations, et pour protéger et renforcer la démocratie, la liberté et la sécurité au sein des sociétés libérales et sociales démocratiques.

Au fil du temps, il deviendra une sorte de hub de confiance personnel qui sera essentiel pour la vie numérique privée ou sensible des citoyens – la santé en ligne, la participation politique, les réseaux sociaux, la banque en ligne, l'administration en ligne, les services avancés basés sur l'intelligence artificielle –, pour l'authentification forte des ordinateurs portables, des PC et des téléphones cellulaires, ainsi que pour le contrôle et l'interaction des citoyens avec les dispositifs portables, les casques de réalité augmentée…

Des représentants de plusieurs pays et organisations intergouvernementales discuteront de ces perspectives lors de la 9e édition de la série de conférences Free and Safe in Cyberspace, qui se tiendra pour la troisième fois à Genève, les 14 et 15 mars 2023, autour de la Trustless Computing Association.

Dans nos colonnes: Pegasus, la nécessaire indignation (2021)

> Le Temps publie des chroniques et des tribunes – ces dernières sont proposées à des personnalités ou sollicitées par elles. Qu'elles soient écrites par des membres de sa rédaction s'exprimant en leur nom propre ou par des personnes extérieures, ces opinions reflètent le point de vue de leurs autrices et auteurs. Elles ne représentent nullement la position du titre.