Cybersécurité : Erato, l'anti-Pegasus

Un expert français a mis au point un logiciel pour contrecarrer le mouchard israélien utilisé par des gouvernements et des entreprises du monde entier.

Le logiciel Erato est une défense contre le mouchard Pegasus.© KHANH RENAUD POUR « LE POINT »

Par Aziz Zemouri pour LE POINT

Publié le 12/04/2022 à 20h00

Si les forêts de Sologne sont réputées pour la chasse, l'ex-hackeur Patrice Guichard, 56 ans, docteur en sécurité des systèmes informatiques de l'université Paris-8, voisins des sangliers et autres cerfs solognots, se livre, lui, à un autre genre de traque. Son gibier : virus, ransomwares, malwares, spywares et autres stalkerwares, le traqueur des maris trompés. Et ce, pour le compte de Cristal Group International, la PME d'intelligence économique qui emploie d'anciens cadres de la DGSE, notamment le général Yves Mathian, longtemps patron de la technique au sein du service de contre-espionnage. Expert en cybersécurité auprès de la cour d'appel de Paris, Guichard décortique aussi pour les services antiterroristes, DGSI et Sdat, ordis et smartphones des suspects.

Il vient de mettre au point un logiciel anti-Pegasus, ce spyware israélien vendu notamment à des États autoritaires pour espionner opposants politiques et défenseurs des libertés. En juillet dernier, le consortium de

journalistes Forbidden Stories, aidé d'Amnesty International, révélait un espionnage de grande ampleur réalisé par Pegasus, bien que NSO, son propriétaire, s'en défende.

En effet, à l'origine, cette technologie permet de lutter contre le terrorisme et le crime organisé. Pour les mettre hors d'état de nuire, Pegasus pénètre les smartphones, quel que soit le système d'exploitation : iOS pour Apple ou Android pour Google. Toutes les données sont à sa portée : contacts, photos, mots de passe… Il peut lire les mails, suivre les conversations en direct, y compris sur les messageries chiffrées, géolocaliser l'appareil et activer micros et caméras pour transformer l'appareil en un véritable mouchard.

S'il existe des logiciels espions depuis plusieurs années, les créateurs de Pegasus, des anciens des services secrets intérieurs de l'État hébreu, ont trouvé le moyen d'installer leur « micro-espion » à distance via un SMS masqué, par exemple, sans interaction physique avec leur cible, contrairement aux logiciels espions traditionnels. Ainsi que l'indique sa notice de présentation, Pegasus installe discrètement un logiciel invisible sur l'appareil d'une cible. Le software extrait et transmet en toute sécurité les données collectées pour les analyser. Cette opération ne nécessite aucune interaction physique avec la cible et ne laisse aucune trace sur l'appareil.

En outre, Pegasus a créé son propre réseau de transmission anonymisé, le PATN, qui empêche toute remontée jusqu'au client.

Patrice Guichard a bûché derrière ses ordis et a trouvé la parade pour désarmer Pegasus : Erato – du nom d'une des muses de la mythologie grecque –, un boîtier qui est en mesure de détecter le logiciel espion. Grâce au codage de plusieurs milliers d'indicateurs de compromissions, Erato peut retrouver Pegasus et autres malwares et les mettre hors d'état de nuire. « C'est le fruit d'un long travail : si la détection du logiciel espion prend plusieurs minutes, retrouver sa trace après qu'il a été détruit à distance par l'installateur prend davantage de temps. Là, il faut entrer dans une investigation numérique.
On entre dans la mémoire du téléphone pour savoir s'il a été *pawné* [compromis, de l'anglais *pawned*, NDLR]. Nous avons conçu une architecture qui nous permet de répondre à tous les types d'attaques et de compromissions », se félicite Patrice Guichard, dont les journées de travail s'étirent souvent jusqu'à 2 heures du matin, sa cafetière remplie

de dosettes vides en témoigne. On n'en saura pas plus, les détails techniques plus approfondis relèvent du secret industriel.
« Cet été, nos deux équipes, celle de Patrice Guichard et celle de Tehtris, ont collaboré après les révélations sur l'espionnage Pegasus », explique Ingrid Sollner, de Tehtris, inventeur du logiciel Mobile Threat Defense, l'autre solution française anti-Pegasus. Patrice Guichard fait le lien entre les deux boîtiers anti-Pegasus, il fait partie de l'écosystème Tehtris pour lequel il ausculte la mémoire des téléphones mobiles.

Erato Celteam Patrice Guichard© KHANH RENAUD POUR « LE POINT »

Une sacrée performance pour celui qui s'est fait connaître en 1987, sous la présidence de François Mitterrand, lorsqu'il s'était introduit dans les serveurs informatiques de l'Élysée – « embryonnaires à base de Minitel, tient-il à préciser. Il avait notamment pu récupérer les numéros de téléphone du chef de l'État, de ses principaux conseillers et des ministres régaliens !
Il avait 22 ans et près de dix ans d'expérience des backdoors. Depuis, il est retourné au château sous le mandat de François Hollande, de manière tout à fait légale cette fois : Celteam, sa PME, devait débusquer des malwares et trouver un pare-feu à l'espionnage américain mis en

place depuis l'ambassade alliée à quelques encablures du palais présidentiel.
Les espions de Washington, il connaît : il a assuré la cybersécurité du candidat indépendant Ross Perot, adversaire de George Bush père et de Bill Clinton.

Pour des entreprises du CAC 40, il doit contrecarrer les attaques des Anonymous, des espions chinois ou les cybercriminels spécialisés dans le blocage des sites avec paiement d'une rançon pour les débloquer.
Une technique criminelle qui monte en puissance depuis trois ans et qui touche désormais de nombreuses PME. Plusieurs clients, notamment des PDG de multinationales, ont d'ores et déjà pris rendez-vous avec Cristal Group pour mettre en place Erato et équiper leur flotte de mobiles.
Et bientôt la DGSE ou la DGSI ?