Espionnage

Pegasus: «L'Europe doit réagir fermement», estime Bernard Barbier (ex-DGSE)

Spécialiste du cyber, l'ancien directeur technique de la DGSE livre à l'Opinion son analyse sur le logiciel espion israélien qui aurait été utilisé contre Emmanuel Macron

Les faits — Emmanuel Macron a présidé jeudi matin un conseil de défense exceptionnel consacré à l'affaire Pegasus, un logiciel espion israélien qui aurait été utilisé par les services de renseignement marocains pour pirater ou tenter de pirater des téléphones de responsables politiques et journalistes français, a annoncé le porte-parole du gouvernement, Gabriel Attal. D'après une enquête menée par un consortium de médias, dont *Le Monde* et Radio France, un des numéros d'Emmanuel Macron figurait parmi les cibles potentielles du logiciel Pegasus.

« L'Europe doit réagir très fermement » à l'affaire d'espionnage Pegasus, affirme à l'Opinion Bernard Barbier, l'ancien Directeur technique de la DGSE (2006-2013). Spécialiste de cyberdéfense et du renseignement électronique, cet ingénieur, aujourd'hui à la retraite, a dirigé l'équivalent français de la NSA américaine. « C'est une question de souveraineté : l'Europe doit avoir les capacités techniques nécessaires pour se protéger » face à des intrusions dans les téléphones portables et les ordinateurs individuels.

Pegasus est un logiciel espion très performant, mis au point et commercialisé par la société israélienne NSO. Un consortium international de journalistes, Forbidden Stories, vient de révéler que plusieurs gouvernements étrangers l'utilisaient largement, contre des opposants et des journalistes. Le Maroc est soupçonné de s'en être servi pour espionner Emmanuel Macron et d'autres ministres. Un conseil de défense consacré à cette question s'est tenu ce jeudi matin à l'Elysée.

Comme Bernard Barbier, les spécialistes ne sont pas surpris par l'existence de ce logiciel. Dès 2016, le magazine 01net racontait « comment fonctionne Pegasus, ce malware qui vole toutes les données de l'iPhone ». En revanche, « l'usage incontrôlé » qui en fait par des gouvernements pose de sérieuses questions, à la fois de sécurité nationale et de libertés publiques.

Un peu de technique d'abord. Du fait du cryptage des communications, les « écoutes téléphoniques » à l'ancienne sont désormais presque totalement inefficaces. « Il faut by-passer le chiffrement et pour cela entrer au cœur du système, jusque dans les couches très basses de l'operating system » des téléphones, explique Bernard Barbier.

Unité 8-200. La société israélienne NSO a mis au point des « techniques extrêmement performantes » en la matière, en s'appuyant sur sa proximité avec les anciens personnels de l'Unité 8-200 de l'armée, l'agence de renseignement électronique. Grâce au service militaire obligatoire et à l'emploi de réservistes, il existe en Israël un vrai écosystème militaro-industriel entre les unités opérationnelles, les centres de recherche et les entreprises technologiques. NSO en est un exemple abouti. Désormais possédée par des capitaux américains, elle pèserait 2 milliards de dollars. « Il s'agit d'un transfert vers le privé de compétences étatiques », indique Bernard Barbier.

Pour pénétrer dans un téléphone portable, le logiciel Pegasus utilise les failles, les erreurs qui existent dans tous les systèmes d'exploitation : « IOS, c'est quarante millions de lignes de codes », rappelle Bernard Barbier. Ils sont régulièrement modifiés et améliorés : ce sont les « mises à jour » de votre portable. A chaque fois, le logiciel Pegasus doit s'adapter pour trouver les nouvelles portes d'entrée. NSO et ses semblables cherchent les « Zero-Day », les failles de sécurité non encore découvertes. Il existe un marché du « Zero-Day » avec des sociétés spécialisées, comme Zerodium fondée par le Français Chaoukri Bekrar. « C'est une guerre permanente » entre le glaive et le bouclier, dit l'ancien directeur technique de la DGSE.

Les grands services de renseignement, dont la DGSE en France, possèdent leurs propres systèmes pour introduire des « malwares » dans les téléphones, même sans aucune action de la part de la cible, répondre à un message, par exemple. Mais de nombreux pays ne possèdent pas de telles capacités en propre. Ils doivent faire appel à des prestataires privés, qui leur fournissent non pas la compétence technologique, mais le service plus ou moins clés en main. C'est la niche de marché de NSO qui travaillerait pour une quarantaine de pays.

Open bar. Cela se fait évidemment avec l'accord des autorités politiques de l'Etat d'Israël. Ainsi, NSO ne fournit pas de services permettant d'espionner les Etats-Unis, la Russie ou la Chine. Pour l'Europe, en revanche, c'est open bar. C'est également le cas de pays arabes comme le Maroc, les Emirats arabes unis, Bahreïn, l'Arabie saoudite qui ont des liens sécuritaires avec l'Etat juif. Ce n'est pas un hasard s'il s'agit des pays ayant récemment établi des liens diplomatiques (sauf pour les Saoudiens, du moins officiellement) avec Israël.

D'autres alliés de l'Etat juif en bénéficient, comme l'Azerbaïdjan, l'Inde, le Rwanda ou, seul pays européen concerné, la Hongrie. Les experts français s'accordent à penser que les services de renseignement israéliens bénéficient des informations ainsi

recueillies, via la société NSO ou d'autres intervenants sur le même marché.

La France a été sur les rangs pour faire appel à la NSO, mais le projet n'a pas abouti, du fait de très fortes oppositions au sein de l'appareil d'Etat. Dans les années 2010, la DGSI (sécurité intérieure) s'intéressait à ce logiciel, parce qu'elle ne disposait pas des mêmes capacités techniques que la DGSE (sécurité extérieure). Même si elle a progressé, la « mutualisation » des moyens d'espionnage électronique au sein de la communauté du renseignement reste un sujet complexe. A la même époque, la DGSI a acquis le logiciel américain Palantir pour l'analyse des données. Dans les services français, beaucoup estiment ce logiciel trop perméable avec la NSA américaine.

Alors que les regards sont tournés vers Pegasus, Guillaume Poupard, le directeur de l'Agence nationale de sécurité des systèmes d'information vient de tirer une autre sonnette d'alarme sur Lindekin contre « une vaste campagne de compromission, toujours en cours et particulièrement virulente, touchant de nombreuses entités françaises. Elle est conduite par le mode opératoire APT31. » En clair : de l'espionnage d'entreprises stratégiques par les Chinois.

L'AUTEUR VOUS RECOMMANDE

Tribune libre
«Pégasus: gare à la dépendance technologique», par Alain Bauer
Alain Bauer

Espionnage
Affaire Pegasus: selon un cadre de NSO, Macron n'a pas été ciblé par le logiciel espion
l'Opinion

Piratage
L'affaire Pegasus, symbole de la nonchalance numérique des dirigeants français
Raphaël Proust

VIDÉO RECOMMANDÉE