Regin : le malware d'espionnage le plus sophistiqué au monde réussit à pirater États, institutions et même pros du cryptage

L'éditeur de logiciels de sécurité Symantec a annoncé dimanche 23 novembre avoir découvert le malware Regin, mis en place depuis 2008 et qui pourrait bien être l'œuvre commune de plusieurs États. Parmi les suspects, les États-Unis, Israël et même la France.

Avec Fabrice Epelboin

Atlantico : Que sait-on concrètement de ce malware ? Quel est son mode de fonctionnement ?

Fabrice Epelboin : Ce malware est extremement sophistiqué, et modulaire qui plus est, il peut aussi bien être configuré pour être utilisé pour attaquer les infrastructures d'un opérateur télécom afin d'intercepter une conversation telephonique que pour espionner une entreprise et accéder à ses systèmes d'information. **C'est un véritable couteau Suisse permettant de mettre au point une multitude d'attaques informatiques répondant à une multitude de missions de surveillance, massives ou ciblées.**

Une telle prouesse n'est pas du tout à la portée d'un groupe de hackers, même les plus doués, cela dépasse et de loin aussi bien leurs capacités d'investissement que leur capacité à gérer de tels projet. Il s'agit sans l'ombre d'un doute d'un malware mis au point par une ou plusieurs agences de renseignement, tout comme Stuxnet, le malware qui avait permis de saboter une usine de raffinement de carburant nucléaire en Iran en 2010.

Quelles ont été les cibles de ce malware jusqu'à présent, et en quoi cela peut-il nous renseigner sur l'origine des éditeurs ?

Des entreprises, des infrastructures telecom, les cibles sont très variées, et ne traduisent pas grand chose au final. Il faut garder à l'esprit que ce genre d'outil peut être configuré un jour pour mettre sous écoute des échanges téléphoniques satellitaires un jour et utilisés pour siphoner les données relatives aux transactions financières d'une banque le lendemain.

Derrière ces multiples cibles infectées par ce malware se cachent une multitude de missions de surveillance. Au vu du nombre de cibles et de leur hétérogénéité, on ne peut guère en déduire autre chose que le fait qu'il y a tout un tas d'opérations de surveillance en cours surveillant tout un tas de choses.

La répartition géographique des principales infections - combiné à la sophistication de l'outil - nous raconte un peu la même chose : quel point commun entre la Russie, le Mexique, l'Arabie Saoudite et l'Islande, si ce n'est d'êttre les cibles de membre du réseau Echelon élargi ?

Cela aurait tendance à désigner les auteurs de ce malware, ou tout du moins cela dresse**une liste des "usual suspects" : Etats-Unis, Angleterre, France, Israel.**.. il y a toutes les chances que ce malware soit l'œuvre - probablement combinée - des travaux issus

de plusieurs de ces pays.

Les particuliers sont-ils hors d'atteinte (non visés) ? Comment ces derniers peuvent-ils s'en prémunir ?

Pas du tout, l**es ordinateurs des particuliers sont concernés, et les particuliers, tout comme les entreprises, sont de nos jours surveillés - s'il n'y avait qu'une seule chose à retenir de l'affaire Prism, c'est bien cela.** La dernière version de l'antivirus de Symantec - qui a fait l'annonce de sa découverte - permet d'identifier une infection, mais cela ne règlera rien. **Ce malware sera très probablement mis a jour pour échapper à toute détection, tout comme il l'a été entre 2011 et aujourd'hui, où il a disparu des écrans radars alors qu'il avait été repéré dès 2008.** Ce type de logiciel ne cesse de se sophistiquer et de se mettre à jour, comme le système d'exploitation de votre ordinateur.

Il faut être honnête et dire franchement qu'il n'y a pas moyen de se prémunir de la surveillance d'Etat, sauf à être un hacker de haut niveau. On peut au mieux apprendre les rudiments du chiffrement, abandonner certains services en lignes "gratuits" qui se nourrissent de vos données personnelles, afin de s'en prémunir au mieux. Mais cela a des limites, et ce malware en est une bonne illustration.

Pour une entreprise, il faut faire appel aux services de l'Etat ou trouver une officine qui permettra de mettre à niveau ses installations et - surtout - ses pratiques. Cela relève des travaux d'Hercule pour les grosses entreprises, mais pour un cabinet d'avocat, par exemple, c'est faisable. Habituellement, quand il y a un risque critique pour une entreprise, ce type de mission en France est confié à l'Ansi, mais si vous êtes un avocat et que vous cherchez précisément à vous défendre de la surveillance de l'Etat - imaginez Thierry Herzog - alors vous êtes en slip, pour ainsi dire. Dans le méandre des accords commerciaux qui lient tout le petit monde de la sécurité avec les Etats et les agences de renseignement, trouver un prestataire qui vous protégera de la surveillance d'Etat n'est pas chose aisée.

Que sait-on justement aujourd'hui du marché des logiciels espions élaborés à des fins de surveillance ?

C'est un marché complexe et évidemment très discret sur son mode de fonctionnement. Les logiciels espions 'étatiques' peuvent être développés par des société privées - comme Gamma Group - qui fabrique FinFisher, un logiciel utilisé, par exemple, par le régime de Mubarack pour surveiller ses opposants, mais également identifié récemment sur les machines de plusieurs ONG au Maroc.

Des malware comme Regin, qui fait la Une aujourd'hui, ou Stuxnet, sont l'œuvre d'agences de renseignements. Enfin **il existe tout un ecosystème de spécialistes de la sécurité IT qui fournissent par exemple des "zero-day", des méthodes d'intrusion exclusives permettant à leurs acheteurs de disposer d'un avantage tactique certain.** C'est le cas du Français VUpen qui travaille aussi bien pour la NSA que pour les services Français.