Casper, le logiciel espion qui surveillait la Syrie | Le Net Expert Informatique

	Casper, le logiciel espion qui surveillait la Syrie

Un chercheur en informatique a découvert un nouveau programme espion, qu'il attribue aux mêmes développeurs que le programme Babar, pour lequel la France est soupçonnée.

Les développeurs des programmes espion Babar et Evil Bunny, que le Canada soupçonne être les services de renseignement français, ont créé un troisième programme espion qui ciblait la Syrie.
Pour rappel, Le programme espion Babar a un « grand frère » : Evil Bunny
C'est la conclusion à laquelle aboutit Joan Calvet, un expert de l'entreprise de sécurité informatique ESET dans un rapport qui doit être publié jeudi 5 mars. Il a pu mettre la main sur un exemplaire de ce nouveau programme, dont le nom que lui ont donné ses créateurs reprend à nouveau celui d'un célèbre dessin animé. Cette fois-ci, les développeurs ont baptisé leur création Casper.

Une dizaine de personnes visées en Syrie
Ce logiciel a été retrouvé sur les ordinateurs d'une dizaine de personnes, toutes situées en Syrie. Il n'est pas exclu que ce programme ait été mis en œuvre ailleurs. Il a aussi été utilisé très récemment – contrairement à Babar – et faisait partie d'une opération bien précise : il a été actif en Syrie seulement quelques jours, entre le 9 et le 16 avril 2014.
La trace de ce programme a été retrouvée sur un site officiel du gouvernement syrien, celui d'une commission créée en 2011 sous l'égide du ministère de la réconciliation nationale afin que les Syriens victimes de destructions lors de la guerre civile puissent porter réclamation.

Un programme de reconnaissance
A l'inverse de Babar, Casper ne capture pas d'informations directement : c'est un programme de reconnaissance. Lorsqu'il pénètre dans un ordinateur, il en établit un descriptif précis – langue utilisée, programmes installés, logiciels antivirus configurés – avant de le faire parvenir à ses commanditaires. Ensuite, ces derniers décident si la cible est réellement digne d'intérêt.
Le deuxième stade est vraisemblablement celui de l'envoi d'un autre programme espion capable, lui, d'intercepter des informations. Casper prévoit d'ailleurs ce cas de figure : il peut lui être ajouté des modules complémentaires. Cette technique est de plus en plus courante dans les attaques étatiques sophistiquées.

Un programme fantomatique et complexe, une « partie d'échecs » avec les logiciels antivirus.
Ce programme espion au nom de fantôme porte bien son nom, tant il est difficile à détecter. Lorsqu'il atterrit sur un ordinateur, Casper s'adonne à une « partie d'échecs » avec les logiciels antivirus : il analyse très finement lesquels sont présents sur la machine et adapte son mode d'infection. Dans certains cas, il peut tout bonnement s'autodétruire lorsqu'il estime que les risques sont trop grands. « On voit rarement ce niveau de précision dans l'évitement des antivirus chez les programmes espion », note Joan Calvet, signe là encore d'une grande sophistication.
« Casper est tellement furtif et sous le radar des entreprises de sécurité, qu'on ne retrouve sa trace qu'épisodiquement pour le moment. J'espère qu'en publiant ces informations, d'autres chercheurs vont pouvoir amener leur pièce au puzzle ! », explique aussi M. Calvet.
Signe supplémentaire de sa complexité et de la motivation des attaquants, il utilise une faille dite « 0-Day », c'est-à-dire une vulnérabilité inconnue. Ce type de vulnérabilité, inédite donc invisible pour les antivirus, intéresse de près les chercheurs en sécurité informatique. Utiliser une telle faille, c'est prendre le risque de l'exposer en plein jour et de la voir rapidement corrigée.

Les mêmes auteurs que Babar
Pour Joan Calvet, il n'y a guère de doute. Casper est l'œuvre des développeurs qui ont créé Babar et Evil Bunny. Outre des portions du code rigoureusement identiques entre ces programmes, il leur a trouvé de nombreux points communs, notamment dans leur manière de se cacher ou de détecter les antivirus.
« Toutes les fonctionnalités communes nous font dire avec un haut degré de certitude que Bunny, Babar et Casper ont été développés par la même organisation », écrit Joan Calvet.

Un Etat à la manœuvre ?
Casper, comme Babar, n'est pas un programme d'espionnage massif, comme certains dispositifs révélés par les documents d'Edward Snowden. Il s'agit d'outils de haut niveau destinés à obtenir des informations précises sur des cibles déterminées. Selon M. Calvet, « le ciblage précis d'individus en Syrie montre un intérêt géopolitique probable » :
« Non seulement Casper est bien développé, mais en plus ses auteurs semblent bien comprendre comment nous – les chercheurs en sécurité – travaillons, et ils ont fait en sorte de rendre notre tâche difficile. En regardant rapidement le programme, on peut avoir l'impression d'avoir sous les yeux un logiciel malveillant banal, sans se douter de toute la machinerie de reconnaissance contenue dans Casper. Je dirais donc que Casper a été développé par une équipe de professionnels, soucieuse de faire un logiciel malveillant discret. Ce "professionnalisme" peut tout à fait correspondre à une entité étatique. »

France : quelle implication ?
En 2014, Le Monde révélait sur la base de documents fournis par Edward Snowden que les services de renseignement canadiens soupçonnaient la France d'avoir développé un programme espion nommé Babar.
Rappel : Quand les Canadiens partent en chasse de « Babar »
Il y a quelques semaines, deux chercheurs en informatique révélaient davantage d'informations sur Babar et dévoilaient du même coup l'existence d'Evil Bunny, le « grand frère », moins évolué, de Babar, développé par la même organisation.
Pas de trace nouvelle d'une implication hexagonale dans Casper. La France, qui à ce stade n'est que soupçonnée par les services de renseignement canadiens d'être derrière Babar, et donc derrière Casper, s'est dotée, comme les autres grandes puissances militaires mondiales, de capacités offensives sur Internet, confiées à l'armée et aux services extérieurs, la DGSE. Les autorités refusent de s'exprimer sur ce sujet extrêmement sensible, couvert par le plus haut niveau du secret-défense. Récemment, une vidéo réalisée par l'armée française rompait légèrement avec ce mutisme en vantant ses capacités d'« attaque » et « destruction » dans ce « combat numérique ».

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemonde.fr/pixels/article/2015/03/05/casper-le-logiciel-espion-cousin-de-babar-qui-surveillait-la-syrie_4586723_4408996.html
Par Martin Untersinger