Surveillance : le spyware FinFisher détecté dans 32 pays | Le Net Expert Informatique

Le spyware FinFisher détecté dans 32 pays

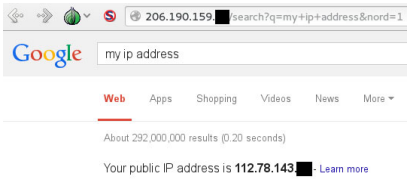
Malgré les mesures prises pour en dissimuler l'existence, le Citizen Lab a réussi à remonter à nouveau la trace du spyware FinFisher vendu aux autorités policières de nombreux états dans le monde, y compris dans des pays autoritaires.

Le business de l'espionnage des communications électroniques fonctionne toujours très bien. Alors que le piratage spectaculaire de la société Hacking Team n'a semble-t-il eu aucun effet notable sur ses relations commerciales avec les autorités qui exploitent ses services, son concurrent britannique FinFisher n'a visiblement lui non plus aucun problème à continuer ses activités, malgré la divulgation de ses codes sources et d'autres données internes en 2014.
Les gouvernements continuent de faire confiance à ces entreprises privées qui proposent ça et là des outils permettant de placer sur écoute des smartphones, d'accéder aux données d'un PC, de collecter toutes les touches frappées sur un clavier, d'activer discrètement des webcams, de géolocaliser des appareils, ou encore d'accéder au contenu de conversations en principe privées et chiffrées. Les intérêts pour la sécurité nationale priment sur les quelques questions éthiques que peuvent poser certaines méthodes, qui valent à ces firmes d'être placées sur une liste des « sociétés ennemis d'internet » par Reporters Sans Frontières.

Car les services qu'elles vendent ne sont pas achetés que par des démocraties bien sous tous rapports, malgré les restrictions à l'exportation qu'elles sont censées respecter.

Le laboratoire Citizen Lab a ainsi publié de nouvelles démonstrations de la présence des outils de Finfisher dans au moins 32 pays, dont plusieurs états peu recommandables du point de vue du respect des droits fondamentaux, comme la Malaisie, l'Arabie Saoudite, le Kazakhstan, l'Ethiopie, le Maroc ou le Bengladesh.
Déjà en 2012, le laboratoire avait prouvé que la suite d'outils d'espionnage Finfisher vendue à l'époque par la société britannique Gamma International (elle a depuis donné son indépendance à Finfisher GmbH, basée à Munich), était utilisée par au moins une quinzaine d'États dans le monde. Parmi eux figuraient déjà des pays autoritaires comme le Bahreïn, l'Ethiopie, l'Indonésie, le Turkménistan, ou les Emirats-Arabes Unies.
Comme Hacking Team, Finfisher assure qu'elle respecte l'arrangement de Wassenaar qui limite les possibilités d'exporter les outils de surveillance vers des pays autoritaires qui peuvent en faire un usage non conforme aux droits de l'homme, par exemple pour traquer des opposants politiques ou rechercher les sources de journalistes hostiles au régime. Mais la présence continue de ses outils sur des serveurs appartenant à des régimes dictatoriaux permet, au minimum, de douter de la véracité de telles affirmations.
Depuis les révélations de 2012, FinFisher a amélioré ses méthodes de dissimulation et systématiquement caché ses outils derrière des serveurs proxys, configurés pour paraître inoffensifs. Mais les chercheurs du Citizen Lab ont regorgé d'ingéniosité pour les trouver.
Depuis décembre 2014, l'organisation a scanné un maximum d'adresses IPv4 pour trouver des serveurs dont certaines caractéristiques correspondaient à ce qu'ils connaissaient de FinFisher. Ils ont trouvé 135 serveurs, dont la plupart étaient des serveurs proxys qui affichaient la page d'accueil de Google ou Yahoo. Ces serveurs là, qui servent uniquement de relais intermédiaire, n'avaient aucun intérêt puisqu'ils masquaient la géolocalisation des serveurs « maîtres » sur lesquels étaient installés les outils de FinFisher. Mais aux yeux de Google et Yahoo, c'est bien l'adresse IP du serveur maître qui communique.

PREMIÈRE ASTUCE :
« DIS-MOI MON ADRESSE IP »

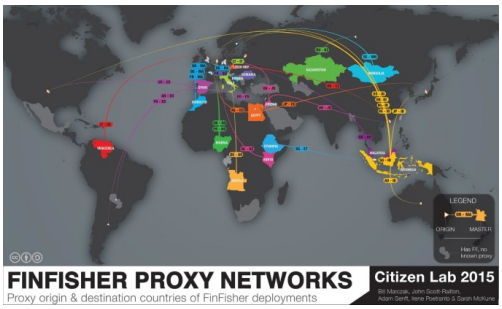


Lorsque Google était affiché, il suffisait d'exécuter la requête « my IP adress » (qui ne fonctionne pas avec Google France) pour que Google réponde au serveur maître, et que celui-ci renvoie la réponse au serveur relais, qui lui-même l'affichait à Citizen Lab. Ils ont ainsi pu trouver des adresses IP de serveurs maîtres installés dans différents pays, et découvrir leur géolocalisation.

DEUXIÈME ASTUCE :
« DIS-MOI QUEL TEMPS IL FAIT »

Sur Yahoo, la commande n'existe pas. Mais le service sait afficher la météo qui correspond au lieu qu'il associe à l'adresse IP de l'internaute. Les chercheurs ont donc demandé à Yahoo d'afficher la météo et découvert que, par exemple, un serveur qui était censément installé en Lituanie renvoyait la météo de Caracas, au Venezuela. Un pays où les journalistes sont régulièrement persécutés. Ca ne permettait pas d'obtenir en direct l'adresse IP, mais au moins de savoir où elle était attachée.

La carte des proxys :



Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.numerama.com/tech/126760-surveillance-le-spyware-finfisher-detecte-dans-32-pays.html
Par Guillaume Champeau
Crédit photo de la une : Thibaut Démare