Un incroyable système d’espionnage des internautes mis au jour

Les sites web de Microsoft, Adobe, Wordpress, Spotify, Skype, Samsung ou encore Pornhub contiennent un logiciel enregistrant tout ce que fait l’internaute: ses mouvements de souris, les touches frappées, les liens cliqués… Des chercheurs de Princeton ont mis au jour ces pratiques sulfureuses

Ce ne sont sans doute ni la NSA ni des pirates informatiques russes ou nord-coréens qui sont les plus curieux de la vie privée des internautes. Il s’agit plutôt de multinationales bien établies telles Microsoft, Samsung ou encore Spotify. Il y a quelques jours, des chercheurs de l’Université de Princeton (New Jersey) ont publié une étude montrant comment ces entreprises espionnaient en détail le comportement des internautes qui visitent leurs pages web – certaines ont abandonné cette pratique ces derniers jours. Via des systèmes perfectionnés, elles parviennent à enregistrer intégralement les mouvements de souris, les frappes sur le clavier et la navigation entre les pages.

Steven Englehardt, l’un des chercheurs du projet «Freedom to Tinker» de Princeton, résume ce système d’espionnage en une phrase: «Ces scripts informatiques sont conçus pour enregistrer et rejouer en play-back des sessions individuelles de navigation, comme si quelqu’un regardait par-dessus votre épaule.» Les chercheurs ont constaté que 482 des 500?000 sites les plus consultés sur la planète – selon le classement de la société Alexa – intègrent de tels scripts. Il s’agit par exemple de Microsoft, Adobe, Wordpress, Spotify, Skype, Samsung ou encore du site pornographique Pornhub.

Même du contenu effacé

Les chercheurs ont même créé une base de données permettant de trouver les sites impliqués. Cette base de données concerne les 10'000 sites les plus consultés. Et dans le fichier CSV à télécharger, qui contient la liste entière, l'on trouve des sites suisses, comme l'a trouvé un confrère de la RTS. Y figurent ainsi watson.ch, moneyhouse.ch, upc.ch, unil.ch, jobup.ch ou encore.

Ces scripts, soit des morceaux de codes informatiques, sont appelés «session replay». Il s’agit en effet de rejouer en différé le comportement complet d’un internaute pour l’analyser. Cela permet par exemple de voir s’il se perd entre deux pages ou s’il se perd au milieu d’un formulaire. Ces systèmes ne sont pas nouveaux. C’est la découverte de leur utilisation massive qui l’est, de même que leur puissance. Car ces scripts sont par exemple capables d’enregistrer ce qu’un internaute écrit dans un formulaire, même s’il efface en partie son contenu pour le récrire ensuite. Comme le rappelle le site spécialisé Motherboard, Facebook avait fait scandale en 2013 lorsqu’il avait été découvert que le réseau social enregistrait les statuts de ses membres, même s’ils étaient juste tapés, et pas enregistrés…

Pas d’anonymisation des données

Les 482 sites incriminés utilisent des scripts de plusieurs sociétés: FullStory, SessionCam, Clicktale, Smartlook, UserReplay, Hotjar et Yandex – il s’agit, dans ce dernier cas, du moteur de recherche le plus populaire en Russie. Ces scripts posent plusieurs problèmes. D’abord, les internautes ne sont souvent, voire jamais au courant du fait que leurs actions sont enregistrées. Ensuite se pose la question de la confidentialité: les informations récoltées sont envoyées sur les serveurs des éditeurs de ces scripts sans être anonymisées, et sans doute avec un degré de protection très faible.

Les chercheurs donnent l’exemple du site web de la chaîne américaine de pharmacie Walgreens. Les auteurs de l’étude notent que des informations aussi sensibles que des ordonnances, des informations sur la santé du patient mais aussi son nom sont envoyées sur les serveurs de FullStory. Certains mots de passe, lorsqu’ils sont inscrits sur des sites web consultés sur smartphone, sont aussi enregistrés, tout comme quelques chiffres provenant de numéros de cartes de crédit.

Pratiques «dangereuses»
Que penser de ces pratiques? «Elles sont très dangereuses, car le stockage de données aussi personnelles et sensibles sur des serveurs de sociétés de conseil risque de donner des idées à des pirates informatiques, estime Sylvain Pasini, spécialiste en cybersécurité à la Haute Ecole d'ingénierie et de gestion du canton de Vaud. Il faut préciser en parallèle que d'après ce qu'ont trouvé les chercheurs de Princeton, les entreprises enregistrent tout ce qui se passe sur leur site web, mais pas sur l'ensemble de l'ordinateur. Le système d'espionnage est installé sur le serveur de l'entreprise, pas sur l'ordinateur de l'internaute.»

Pour les internautes, il existe des parades pour éviter d'être pisté. Ainsi, Adblock Plus serait efficace contre ces systèmes espion.