Les 10 outils les plus incroyables utilisés par la NSA pour nous espionner | Le Net Expert Informatique

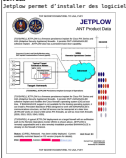
Les 10 outils les plus incroyables utilisés par la NSA pour nous espionner

Le journal allemand Der Spiegel a lancé des révélations chocs sur le cyberespionnage à partir de documents confidentiels partagés par l'ancien consultant de la NSA Edward Snowden. Voici un palmarès des outils les plus fous utilisés par la National Security Agency pour nous espionner. Il semblerait que pour chaque porte verrouillée par les fournisseurs d'équipements réseaux, les produits informatiques et les télécoms, la NSA possède une clé. La liste complète de ces outils disponible ici.(http://leaksource.wordpress.com/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/)

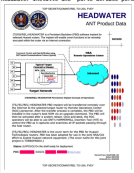
FEEDTHROUGH
Juniper Networks n'est ni plus ni moins que le 2e équipementier mondial de systèmes réseaux pour entreprises. Ses pare-feux Netscreen permettent de faire respecter la politique de sécurité d'un réseau informatique, définissant quels types de communication y sont autorisés. La NSA inflitre ce périmètre sécurisé grâce à Feedthrough.

DEITYBOUNCE
Deitybounce permet d'installer des logiciels malveillants de façon permanente, notamment sur les serveurs "PowerEdge" du fabricant mondial de PC Dell. La NSA implante son malware dans les "BIOSS", ces logiciels sur la carte mère d'un ordinateur qui sont les premiers éléments installés au démarrage de l'appareil. Le PC ou serveur infecté semble fonctionner normalement, et même s'il est nettoyé, et son contenu entièrement effacé, les logiciels espions de la NSA restent logés de façon invisible. Dell a répondu à cette révélation (http://en.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2013/12/30/comment-on-der-spiegel-article-regarding-nsa-tao-organization.aspx).

JETPLOW
Jetplow permet d'installer des logiciels espions permanents dans les pare-feux du géant mondial des réseaux informatiques Cisco. Il peut aussi "modifier le système d'opération des pare-feux de Cisco au démarrage". Une option de "porte dérobée permanente" permet aussi "un accès complet". Cisco a répondu à cette révélation (http://blogs.cisco.com/news/comment-on-der-spiegel-articles-about-nsa-tao-organization).



HEADWATER
Headwater installe une "porte dérobée permanente" (Persistent Backdoor) sur certains routeurs du fabricant de matériel informatique chinois Huawei. Ces "implants" espions peuvent être installés à distance via internet.

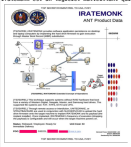


NIGHTSTAND
Nightstand est un appareil sans fil d'exploitation et d'insertion de données, "typiquement utilisé quand on ne peut accéder à une cible via une connexion internet." Il permet des attaques de loin, jusqu'à près de 13 kilomètres de distance de la cible.

PICASSO
D'apparence assez habituelle voire désuète, Picasso est un téléphone sans fil avec puce GSM (dont deux modèles de Samsung) qui permet de "collecter les données d'utilisateurs, des informations de géolocalisation et le son d'une pièce". Ces données peuvent être récupérées via un ordinateur portable ou bien par SMS "sans alerter la cible".

COTTONMOUTH-I
Pour le novice, cet outil ressemble à un port et câble USB inoffensifs. Mais à l'intérieur, se cache une carte mère qui fournit "un pont sans fil dans un réseau cible, ainsi que la possibilité d'introduire des logiciels « exploit » sur des ordinateurs portables ciblés." (Un "exploit" permet à un logiciel malveillant d'exploiter une faille de sécurité informatique dans un système d'exploitation ou un logiciel.) Autrement dit, la NSA peut introduire un cheval de Troie dans n'importe quel ordinateur.

IRATEMONK
Iratemonk est un logiciel malveillant qui infecte des ordinateurs portables et de bureau en attaquant le firmware de disques durs fabriqués par Western Digital, Seagate, Maxtor et Samsung, qui sont toutes à l'exception de la dernière, des entreprises américaines. Le firmware, ou microprogramme, concerne l'ensemble des instructions et des structures de données qui sont intégrées dans le materiel informatique.



TOTEGHOSTLY 2.0
Toteghostly 2.0 est un implant logiciel à destination du système d'exploitation Windows Mobile, qui permet d'extraire et d'installer des données à distance. La NSA peut ainsi accéder aux SMS, liste de contacts, messages vocaux, géolocalisation, fichiers audio et vidéo, etc. de l'appareil.

CANDYGRAM
Candygram est une "station GSM active", qui permet d'imiter le comportement d'une tour de téléphonie cellulaire et ainsi de repérer et monitorer des téléphones portables. Quand un appareil ciblé entre dans le périmètre de la station Candygram, le système envoie un SMS à l'extérieur du réseau à des téléphones "espions" préalablement enregistrés.

Tout cela sans compter Dropoutjeep qui permet à la NSA peut installer des logiciels espions sur les iPhone (http://www.usine-digitale.fr/article/la-nsa-peut-infiltrer-iphone-et-ipad-a-distance.N229076), et sur tous les appareils iOS et collecter ainsi des données sans que la "cible" s'en aperçoive.

Enfin, petit cadeau, dont Jean-Paul PINTE fait mention dans son blog le 6 juillet 2015, l'organigramme pratique des outils Internet de la NSA.

Source : http://www.usine-digitale.fr/article/les-10-outils-les-plus-incroyables-utilises-par-la-nsa-pour-nous-espionner.N229157
Par Nora Poggi