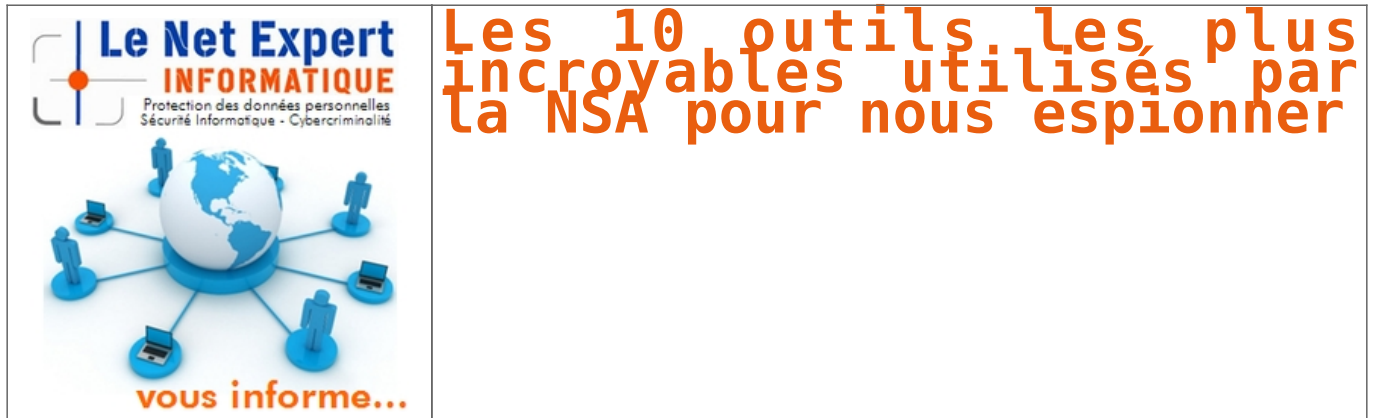


Les 10 outils les plus incroyables utilisés par la NSA pour nous espionner | Le Net Expert Informatique



Le journal allemand Der Spiegel a lancé des révélations choc 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 fiers utilisés par la National Security Agency pour espionner. Il semblerait que pour chaque porte verrouillée par les fournisseurs d'équipements réseau, les produits informatiques et les télécoms, la NSA possède un clé. La liste complète de ces outils disponible ici: (<http://leaksource.wordpress.com/2013/12/20/naas-ent-dixision-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/>)

FEEDTROUGH

Le logiciel permet d'installer des logiciels espions permanents dans les pare-feux du géant 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 infiltre ce périmètre sécurisé grâce à Feedtrough.




DETTROUZE

DeTTroUze permet d'installer des logiciels espions de façon permanente, notamment sur les serveurs "PowerEdge" du fabricant mondial de PC Dell. La NSA implante son malware dans les "BIOS", 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://www.community.dell.com/blogs/insider/2013/12/20/comment-on-der-spiegel-article-regarding-naa-tee-organization.aspx>).

DETTROUZE

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



JETFLOW

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

JETFLOW

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




HEADWATER

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

HEADWATER

Le logiciel permet d'installer des logiciels espions permanents dans les routeurs Huawei. Ces "logiciels" espions peuvent être installés à distance via internet.



NIGHTSTAND

Nightstand est un appareil sans fil d'exploitation et d'injection 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 12 kilomètres de distance de la cible.

NIGHTSTAND

Le logiciel permet d'installer des logiciels espions permanents dans les routeurs Huawei. Ces "logiciels" espions peuvent être installés à distance via internet.



PICASO

D'apparence assez habituelle voire désuète, Picaso est un téléphone sans fil avec pare OSR (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".

PICASO

Le logiciel permet d'installer des logiciels espions permanents dans les routeurs Huawei. Ces "logiciels" espions peuvent être installés à distance via internet.



COTTONPOUFF

Pour le moins, cet outil ressemble à un port et câble USB inoffensifs. Mais à l'intérieur, se cache une carte mère qui fournit "un port sans fil dans un réseau cible, ainsi que la possibilité d'introduire des logiciels « exploit » sur des ordinateurs portables cibles." (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.

COTTONPOUFF

Le logiciel permet d'installer des logiciels espions permanents dans les routeurs Huawei. Ces "logiciels" espions peuvent être installés à distance via internet.



BRATEMONK

Bratemonk 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 touchés 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 matériel informatique.

BRATEMONK

Le logiciel permet d'installer des logiciels espions permanents dans les routeurs Huawei. Ces "logiciels" espions peuvent être installés à distance via internet.



TOTEHOSTLY 2.0

Totehostly 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.

TOTEHOSTLY 2.0

Le logiciel permet d'installer des logiciels espions permanents dans les routeurs Huawei. Ces "logiciels" espions peuvent être installés à distance via internet.



CANDYGRAM

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

CANDYGRAM

Le logiciel permet d'installer des logiciels espions permanents dans les routeurs Huawei. Ces "logiciels" espions peuvent être installés à distance via internet.



Pour info sans compter Droguejazz qui permet à la NSA peut installer des logiciels espions sur les iPhone (<http://www.uscni-digitala.fr/article/la-na-peut-infiltre-iphone-et-ign-e-distance-N226761>), et sur tous les appareils iOS et collecter ainsi des données sans que la "cible" s'en aperçoive. Enfin, petit cadeau, dont Jean-Paul P2012 fait mention dans son blog le 6 juillet 2013, l'organigramme pratique des outils Internet de la NSA.

Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique, à la cybersécurité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Plus d'informations complémentaires ?
Contactez-nous
06 10 20 20 20
Tel : 06 10 20 20 20
Formateur N°93 de 0204 04

Expert Informatique Assessment et Formateur spécialisé en sécurité informatique, en cybersécurité et en déclarations à la CNIL. Denis JACQY et Le Bert Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique de votre entreprise.
Contactez-nous

Cet article vous plaît ? Partagez !
Ou aidez l'auteur avec un commentaire !

Source : <http://www.uscni-digitala.fr/article/les-10-outils-les-plus-secrets-utilises-par-la-na-pour-espionner-N226157>
Par Nore Pogg