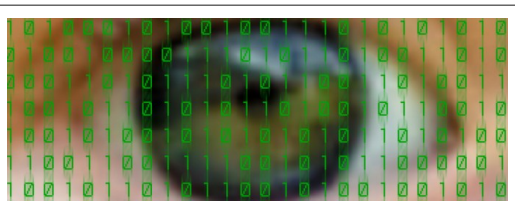
NSA Playset : un kit de surveillance électronique en open source | Le Net Expert Informatique



NSA Playset : un kit de surveillance électronique en open source

Une équipe de chercheurs tente d'imiter les techniques de la NSA à travers une série d'outils open source destinés à mettre en place des écoutes sophistiquées.

Via de petits outils ou gadgets bon marché dont le design est placé en open source, une communauté de chercheurs en sécurité informatique travaille à rendre accessibles au plus grand nombre les techniques les plus pointues de la NSA.
Les fruits d'une année de travaux ont été présentés la semaine passée dans le cadre de la conférence Black Hat USA 2015, organisée à Las Vegas.
Pour mettre au point leurs solutions d'espionnage électronique, les chercheurs se sont inspirés du catalogue ANT, du nom de cette entité qui fournit, au sein de la NSA, des services de piratage « sur étagère » aux différentes divisions de l'agence de renseignement.
Le catalogue en question avait été révélé fin 2013 par le quotidien allemand Der Spiegel, sur la base de documents exfiltrés par Edward Snowden. D'une cinquantaine de pages, il regroupe des exploits basés sur certaines techniques bien connues… et d'autres plus inédites, reposant notamment sur l'interception de signaux au coeur même des appareils ciblés.
Les outils – finalisés ou en cours de développement – doivent surtout permettre de préparer des systèmes qui peuvent y résister. Ils sont classés en cinq catégories.

Première sur la liste, l'interception radio passive. On y trouve, entre autres, Levitivus (analyseur de spectre GSM qui prend la forme d'un téléphone Motorola dont le firmware a été modifié) et KeySweeper (enregistreur de frappe basé sur un matériel Arduino et déguisé en chargeur USB ; voir, à ce propos, notre article « Sécurité IT : les adaptateurs secteur ont des oreilles »).
Deuxième catégorie, la « domination physique » avec, entre autres, le dispositif Slotscreamer, qui s'insère dans un port PCIe sur la machine, offrant un accès direct à la mémoire et aux entrées-sorties. Le tout en contournant les mesures de sécurité physiques et logiques.
Troisième rubrique : les implants hardware, symbolisés par Chuckwagon, qui tire parti du port I2C – présent sur nombre d'ordinateurs – pour l'installation de malware.
En quatrième sur la liste, les techniques d'injection radio active, par exemple à travers Tiny Alamo, qui cible souris et clavier Bluetooth pour insérer des informations dans le système ciblé.
Ultime rubrique : les rétroréflecteurs, illustrés par Congaflock, destiné à être implanté sur tout type d'appareil transmettant des signaux par câble. Son rôle : récupérer de nombreuses données, de la frappe clavier aux images affichées sur l'écran.

Source : http://www.itespresso.fr/nsa-playset-kit-surveillance-electronique-open-source-104776.html