NSA Playset : les attaques de la NSA à la portée de tous

Inspirée par le catalogue ANT de la NSA, une division de l'agence de renseignement qui fournit des services de piratage sur étagère aux différentes divisions internes afin de faciliter leurs opérations d'espionnage, une communauté de chercheurs en sécurité travaille à rendre ces techniques accessibles au plus grand nombre. Via de petits outils ou gadgets bon marché et dont le design est placé en Open Source. Les premiers résultats d'une année d'efforts de ces chercheurs ont été présentés lors de la conférence Blackhat (qui se tenait la semaine dernière à Las Vegas).

Il s'agit de mettre entre les mains de la communauté des techniques leur permettant de toucher du doigt des menaces avancées. En la matière, la sophistication du catalogue ANT, dévoilé par *Der Spiegel* fin 2013 sur la base de documents exfiltrés par Edward Snowden, permet de lever un coin de voile sur les mécanismes exploités par les assaillants ayant accès au plus niveau de sophistication.

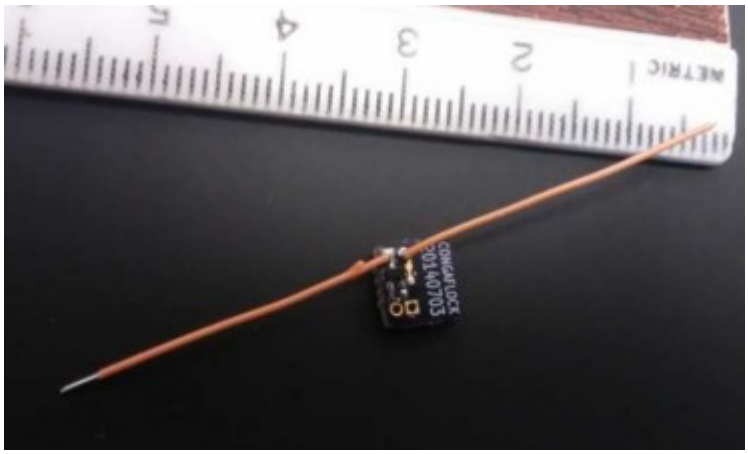
Apprendre de la NSA

Ce catalogue de 50 pages renferme des exploits basés sur des techniques bien connues mais également d'autres plus inédites, reposant notamment sur l'écoute et l'interception de signaux au cœur même des appareils ciblés. C'est ce qui a poussé les chercheurs à l'origine du projet NSA Playset à développer, depuis un an, un ensemble « *de gadgets et d'outils* » qu'ils présentent sur leur site Web. « *En tant que communauté de la sécurité, nous pouvons profiter de la divulgation de ces informations (issues du catalogue ANT, NDLR) pour apprendre* », a expliqué lors de la Blackhat Michael Ossmann, chercheur spécialiste de la sécurité des réseaux sans fil. Connaître les nouvelles menaces permet en effet de préparer les systèmes prêts à leur résister.

Les outils développés ou en cours de développement par les chercheurs sont classés en 5 catégories : interception radio passive, domination physique, implants hardware, injection radio active et rétroréflecteurs. Dans la première de ces catégories, on trouve par exemple Leviticus, un analyseur de spectre GSM qui prend la forme d'un téléphone Motorola dont le firmware a été modifié. Autre exemple, toujours dans la même catégorie : KeySweeper, basé sur un matériel Arduino, un keylogger camouflé en chargeur USB qui transmet les données recueillies par GSM (en photo ci-dessus).

Accès direct à la mémoire

La catégorie domination physique renferme elle un dispositif appelé Slotscreamer, un appareil « *bon marché* » s'insérant dans un port PCIe sur la machine cible et permettant d'accéder directement à la mémoire et aux entrées/sorties, contournant ainsi les mesures de sécurité physiques et logiques. Dans le domaine des implants physiques, signalons Chuckwagon, un dispositif tirant parti du méconnu port I2C, présent sur nombre d'ordinateurs, pour installer des malwares.



Dans les techniques d'injection radio active, on trouve Tiny Alamo, une technique ciblant les souris et claviers Bluetooth et permettant d'insérer des informations dans le système visé. Enfin, le projet NSA Playset propose, dans la catégorie rétroréflecteurs, le projet Congaflock (ci-contre), un dispositif destiné à être implanté dans tout type d'appareils où un signal est transmis via un câble. Ce type d'attaques permet de récupérer les données au cœur même des terminaux ciblés, par exemple les frappes clavier ou les images affichées sur un écran.

A lire aussi :

NSA : les matériels Cisco, Juniper et Huawei transformés en passoire

Gérôme Billois, Solucom : « La NSA a une des meilleures DSI au monde »

Espionnage de la NSA : les 8 leçons d'Edward Snowden