http://www.oxygen-forensic.com
+1 877 9 OXYGEN
+44 20 8133 8450
+7 495 222 9278

Oxygen Forensic Suite
Principes de l'add-on de rootage Android

Le système de fichiers des smartphones Android est de type UNIX, ce qui signifie que la majorité des fichiers sont protégés. Il est dès lors nécessaire d'obtenir au minimum un accès root pour /data/data répertoires de données. Ce dossier contient les fichiers créés par des applications préinstallées et d'autres. Difficile cela dit d'obtenir ces droits d'accès depuis le Système d'Exploitation. Il convient par conséquent d'utiliser un processus connu sous le nom de «rootage», qui permet de «déverrouiller» le système de fichiers.

Il existe deux principaux types de rootage: temporaire et permanent. Pour faire une analogie avec les appareils Apple, où le rootage est appelé «jailbreak», le rootage temporaire est similaire au «tethered jailbreak» (incomplet), tandis que le rootage permanent est similaire au «untethered jailbreak» (complet). Ainsi, un rootage temporaire disparaît lors du redémarrage de l'appareil Android. Un rootage permanent effectue en revanche des modifications importantes du firmware du téléphone et remplace notamment plusieurs *fichiers système*.

Pour y parvenir, il suffit d'extraire les fichiers des répertoires protégés. Un rootage permanent n'est cependant pas nécessaire pour effectuer l'analyse. L'exploit d'Oxygen Android est ainsi conçu pour effectuer le moins d'actions possible afin d'accéder à ces fichiers sans modifier les parties internes du téléphone. L'exploit est copié vers /data/local/tmp (un répertoire standard des applications placé avant l'installation). Il ne s'agit pas d'une application .apk, mais bien uniquement d'une application binaire ne nécessitant pas d'installation. Elle sera simplement lancée pour effectuer sa tâche. À la fin de ce processus, le fichier de l'application est effacé, tout comme n'importe quel fichier temporaire ayant pu être créé lors du rootage (voir ci-dessous). Il est à ce moment possible d'accéder aux fichiers, toutefois les droits d'accès nécessaires ne sont pas encore obtenus. Oxygen Forensic Suite définit alors les droits d'accès temporairement, réalise la lecture de l'ensemble des fichiers et rétablit les droits dans leur état d'origine une fois le processus terminé. Le logiciel maintient le téléphone sous rootage, cependant ce dernier disparaîtra lorsque du redémarrage de l'appareil.

Afin de réaliser cette tâche, il est nécessaire d'avoir accès au système de fichiers du téléphone via l'utilitaire adb. Autrement dit, l'utilitaire adb doit être exécuté sur l'appareil. Le téléphone lui-même doit se trouver en mode «USB debugging» afin de pouvoir être connecté.

L'exploit utilise certaines failles dans différentes versions du Système d'Exploitation Android. D'un point de vue technique, il s'agit de bugs pouvant être réparés dans de nouvelles versions, ce qui signifie que l'exploit risque de ne pas fonctionner pour l'ensemble des modèles actuels et futurs. La faille du système peut en effet être corrigée, ou le téléphone peut tout simplement être livré avec un firmware modifié. Les fournisseurs ont l'habitude de réparer les bugs trouvés dans les systèmes précédents dans les nouvelles versions. Nous utilisons différentes méthodes afin d'effectuer le rootage du téléphone, allant de simples méthodes pour les anciennes versions à des méthodes très sophistiquées pour les dernières versions. Ces méthodes tentent d'obtenir des droits d'accès root à l'utilitaire adb.

Les méthodes utilisées pour le rootage des téléphones Android tournant sur les Systèmes d'Exploitation version 1.6 à 2.2 sont relativement simples et utilisent les failles de la protection mémoire du processus adb. Ces méthodes ne modifient pas le système de fichiers et ne communiquent avec aucun autre processus, leur mémoire ou leurs données sauvegardées. Seul le processus adb est concerné et les données de l'utilisateur ne risquent pas d'être modifiées. La plupart des appareils Android tournant sur les Systèmes d'Exploitation 1.6 à 2.2 peuvent subir un rootage avec cette méthode, à l'exception de quelques firmwares hautement personnalisés.

Les smartphones Android tournant sur des Systèmes d'Exploitation supérieurs à 2.1 sont protégés plus efficacement et nécessitent par conséquent des méthodes plus sophistiquées. Plusieurs variantes sont utilisées pour traiter avec les versions du firmware 2.*, 3.0.* et 4.0.* et ont recours au gestionnaire de la carte mémoire flash. Il est vivement conseillé de remplacer la carte mémoire originale par une carte vide, car il se peut que les données sauvegardées sur la carte mémoire soient perdues. De plus, la carte mémoire peut être désassemblée après le rootage et il n'est dès lors pas nécessaire de l'assembler une nouvelle fois dans l'appareil. Plusieurs fichiers temporaires sont crées au cours du processus et sont ensuite supprimés à la fin du rootage.

Un cas particulier est toutefois possible si la mémoire flash est embarquée. Les spécialistes de l'analyse ne seront pas alors capable de la remplacer par une autre carte. Il leur reviendra alors de décider de procéder ou non au rootage. L'accès illimité à l'ensemble des fichiers offre toutefois des avantages inégalés pour l'analyse des smartphones Android.