Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 30 janvier 2017
N° CERTFR-2017-ACT-005

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-005

1 - Présentation d'une méthodologie de détection des bootkits BIOS à CoRI&IN 2017

Le 23 janvier 2017, lors de la Conférence sur la Réponse aux Incidents et l'Investigation Numérique (CoRI&IN), l'ANSSI présentait une méthodologie de détection *post-mortem* des *bootkits* (cf. Documentation [1]).

Les bootkits sont des logiciels malveillants atypiques en cela qu'ils n'utilisent pas le système de fichiers pour stocker leurs codes. En effet, ces derniers se retrouvent dans les secteurs de démarrage ainsi que dans les espaces non partitionnés du disque. Les fonctionnalités généralement offertes par ces codes sont celles d'un outil de dissimulation d'activité ou *rootkit*, d'où le terme "bootkit" (contraction de "boot" et "rootkit").

Le détournement de la chaîne de démarrage possède de multiples avantages pour l'attaquant :

- furtivité : ces emplacements du disque sont souvent moins surveillés par les logiciels anti-virus et parfois omis des méthodologies d'analyse manuelle ;
- persistance : les secteurs de démarrage contiennent du code exécuté, en toute logique, à chaque démarrage de la machine, offrant donc une persistance garantie ;
- haut niveau de privilège : la chaîne légitime de démarrage a pour but de charger le noyau du système d'exploitation, mais lorsque celle-ci est détournée, l'attaquant possède alors la capacité de modifier ce noyau pour injecter son propre code et ainsi l'exécuter avec le niveau de privilège le plus élevé ;
- contournement de la sécurité : l'exécution préalable au démarrage du système d'exploitation permet d'avoir une grande liberté d'action et l'objectif est généralement d'intercepter le chargement du noyau pour désactiver les fonctions de sécurité risquant d'empêcher le fonctionnement du rootkit (Code Integrity, PatchGuard, ELAM, etc.).

Les noyaux des systèmes d'exploitation modernes possèdent de plus en plus de mesures de sécurité rendant extrêmement complexe l'installation de rootkit une fois le système chargé. En revanche, avant le chargement du noyau, le BIOS n'implémente quasiment aucune sécurité. Il est donc naturel de voir les codes malveillants s'orienter vers la chaîne de démarrage pour s'assurer de leur exécution.

Cela nécessite cependant des connaissances en programmation bas-niveau, moins répandues. Un inconvénient supplémentaire lié au précédent aspect est qu'il n'est pas trivial d'écrire du code portable capable d'infecter fiablement des machines très hétérogènes en termes de version de système d'exploitation, d'architecture ou même de niveau de mise à jour.

Les bootkits sont donc des logiciels malveillants particulièrement discrets et persistants dont la détection est primordiale dans le cadre d'une compromission afin de s'assurer que la remédiation sera efficace.
A cette fin, l'ANSSI a développé et met à disposition un outil de traitement des principaux codes liés à la chaîne de démarrage basée sur le BIOS (cf. Documentation [2]).

L'outil vérifie l'intégrité du MBR (Master Boot Record), du VBR (Volume Boot Record) et de l'IPL (Initial Program Loader) à partir d'une copie hors ligne de ces codes ou d'une copie complète de disque. Cette vérification se base sur la comparaison du condensat des sections de codes avec une liste blanche de signatures connues et que l'analyste aura qualifiées de légitimes.

Documentation

1. https://www.cecyf.fr/activites/recherche-et-developpement/coriin-2017
2. https://github.com/ANSSI-FR/bootcode_parser

2 - Rappel des avis émis

Dans la période du 23 au 29 janvier 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-ALE-001 : Vulnérabilité dans Cisco WebEx
- CERTFR-2017-AVI-025 : Vulnérabilité dans Adobe Acrobat
- CERTFR-2017-AVI-026 : Multiples vulnérabilités dans le noyau Linux de Suse
- CERTFR-2017-AVI-027 : Multiples vulnérabilités dans Wireshark
- CERTFR-2017-AVI-028 : Multiples vulnérabilités dans les produits Apple
- CERTFR-2017-AVI-029 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2017-AVI-030 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2017-AVI-031 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2017-AVI-032 : Multiples vulnérabilités dans WordPress
- CERTFR-2017-AVI-033 : Multiples vulnérabilités dans Mozilla Thunderbird

Gestion détaillée du document

30 janvier 2017 version initiale.