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 03 octobre 2014
N° CERTFR-2014-ACT-040

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-040

1 - De l'utilisation de distributions Linux sur périphérique amovible pour l'investigation numérique d'un poste

Lorsqu'un poste de travail ou un serveur est soupçonné de compromission, une investigation numérique doit être conduite pour qualifier l'incident et, le cas échéant, comprendre les détails de la compromission (vecteur de compromission, vulnérabilités exploitées, activités malveillantes réalisées...).

Cette investigation porte sur tout ou partie des éléments du poste, comme le disque dur, la mémoire, les supports amovibles et de son environnement, par exemple les journaux du serveur mandataire, du contrôleur de domaine, des équipements de sécurité, etc. La source la plus riche d'indices est cependant le plus souvent le disque dur du poste compromis.

Pour mener cette analyse, un procédé rapide consiste à utiliser une distribution Linux qui contient des outils forensics classiques sur un support amovible amorçable, en éteignant le poste et en le démarrant sur le support en question plutôt que sur le disque suspect.

Pour que son analyse soit fiable et reconductible, voire recevable en tant que preuve dans un cadre juridique, l'investigateur doit figer la « scène de crime » et idéalement son observation ne doit apporter aucune modification aux éléments analysés.

Il est donc important que lors de la phase d'acquisition de traces, puis pendant l'analyse, ces systèmes d'exploitation conservent l'intégrité du disque. Une étude a été conduite par une équipe de chercheurs en sécurité pour vérifier le comportement de plusieurs distributions forensics (Helix, Kali, Knoppix).

La procédure d'analyse était simple :

- création d'une première copie du disque hors-ligne avec utilisation d'un bloqueur ;
- démarrage de la machine sur le support amovible contenant la distribution ;
- montage du disque en lecture seule ;
- analyse rapide par les outils fournis ;
- arrêt de la machine ;
- création d'une seconde copie du disque hors-ligne ;
- comparaison des deux images obtenues.

Leur analyse a montré que les trois distributions peuvent porter atteinte à l'intégrité des disques à analyser, à des degrés divers. En particulier, cela concerne la date d'accès de certains fichiers d'un disque NTFS (C:\$I30, C:\$MFT).

Le CERT-FR recommande l'utilisation de bloqueurs physiques, en complément de ces distributions forensiques, afin d'avoir une garantie supplémentaire et indépendante sur l'intégrité des disques analysés.

Documentation

- http://www.dfrws.org/2014/proceedings/DFRWS2014-3.pdf

2 - Étude d'impact des vulnérabilités dans bash

Différentes failles critiques ont été découvertes au sein de l'interpréteur de commandes `bash` la semaine dernière. Ces failles font l'objet de l'alerte CERT-FR-2014-ALE-006. Une analyse des différentes tentatives d'attaques observées par le CERT-FR est présentée dans la suite de cet article.

Volumétrie

Depuis la mise en place de la détection des tentatives d'exploitation de cette faille, le CERT-FR a pu constater que le volume de ces attaques à l'encontre des administrations était relativement important.

Caractéristiques des tentatives d'exploitation

Vecteurs d'attaques

La majorité des tentatives d'exploitation visaient des services Web, en particulier via des en-têtes HTTP spécialement modifiés. La répartition par en-tête HTTP est la suivante :

Entête	Pourcentage
`User-Agent`	63%
`Referer`	16%
`Cookie`	3%
Entêtes personnalisés	18%

On peut remarquer la prévalence des tentatives utilisant des en-têtes standards, en particulier l'importance de l'entête `User-Agent`

Contenu des attaques

La majorité des tentatives d'exploitation observées était constituée de tentatives de balayage des serveurs vulnérables.

Certains de ces balayages ont été effectués par des organismes à des fins de recherche et d'autres vraisemblablement en vue de préparer des attaques ciblées. Une autre partie des tentatives d'exploitation tentait de récupérer des informations sur le système, en particulier en essayant d'afficher les détails de la distribution Linux (commande `uname`), ou encore de récupérer des identifiants en affichant le contenu de `/etc/passwd`.

Les autres charges malveillantes étaient principalement composées de robots IRC, de programmes d'accès à distance, aussi bien sous forme de binaires que de scripts shells, Perl ou Python.

Conclusion

Le CERT-FR encourage les administrateurs à mettre à jour leurs systèmes.

Le mode d'exploitation de ces vulnérabilités est facilement détectable. Il est donc recommandé de mettre en place des protections applicatives ainsi que des règles de détection, afin de pouvoir bloquer et analyser les tentatives de compromission.

Documentation

- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ALE-006/

3 - Rappel des avis émis

Dans la période du 26 septembre au 02 octobre 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-403 : Multiples vulnérabilités dans Juniper
- CERTFR-2014-AVI-404 : Multiples vulnérabilités dans Blue Coat
- CERTFR-2014-AVI-405 : Multiples vulnérabilités dans Apple OS X bash
- CERTFR-2014-AVI-406 : Vulnérabilité dans Xen

Gestion détaillée du document

03 octobre 2014 version initiale.

Conditions d'utilisation de ce document :	http://cert.ssi.gouv.fr/cert-fr/apropos.html
Dernière version de ce document :	http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-040