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 31 août 2015
N° CERTFR-2015-ACT-035

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-035

1 - Kit d'exploitation de vulnérabilités

Vue d'ensemble

Un kit d'exploitation de vulnérabilités (ou exploit kit) est une boîte à outils qui automatise l'exploitation de vulnérabilités sur des grandes quantités de postes utilisateurs. Leur utilisation est simplifiée pour que des utilisateurs sans connaissance particulière puissent superviser et contrôler leur campagne d'infection. Ils représentent une menace permanente pour la sécurité d'un système d'information et évoluent régulièrement.

Les kits d'exploitation sont la plupart du temps vendus sur des marchés noirs de l'internet profond. Ils sont un vecteur pour infecter un grand nombre de machines avec une charge malveillante. Même si les infections se font dans la grande majorité des cas via des postes utilisateurs, l'infection d'autres équipements n'est pas à proscrire. Aujourd'hui, les plus actifs comprennent entre autres : Angler, Fiesta, Magniture, Neutrino, Nuclear, Rig, Sundown ou Sweet Orange.

Fonctionnement

Le fonctionnement d'un kit d'exploitation peut être découpé en quatre étapes.

Contact La victime accède à un lien redirigeant vers un serveur hébergeant le kit. Celui-ci peut être un site légitime compromis, des publicités malveillantes (cf. CERTA-2014-ACT-002) ou encore un lien dans un message électronique.

Redirection Un profilage de la machine cible est effectué, celui-ci permettra au serveur malveillant de choisir quelle vulnérabilité peut être exploitée et de conserver des informations sur la cible (Adresse IP, pays, système d'exploitation, navigateur, etc.).

Exploitation Une fois les vulnérabilités identifiées, le serveur malveillant envoie à la cible l'exploit choisi : il peut prendre la forme d'un fichier PDF, Flash, Silverlight ou encore Java. Les kits d'exploitation utilisent parfois des failles 0 jour, mais plus généralement un grand nombre de vulnérabilités déjà publiques.

Infection L'exploitation d'une vulnérabilité permet à l'attaquant d'exécuter une charge malveillante sur le poste de la victime pouvant exécuter différentes opérations:

- vol d'informations bancaires ;
- exécution d'un rançongiciel ;
- contrôle à distance ;
- installation d'une porte dérobée ;
- participation à un réseau de machines zombies.

Recommendations

Conformément au guide d'hygiène informatique de l'ANSSI, le CERT-FR recommande de :

- mettre à jour le système d'informations (système d'exploitation, logiciels, greffons) ;
- désinstaller (ou a défaut, désactiver) les logiciels et greffons non essentiels au métier. (cf. CERTA-2012-ACT-036) ;
- mettre à jour les CMS et toutes les applications intervenant dans les serveurs web ;
- prendre connaissance des alertes communiquées par votre CSIRT ou FAI.

Documentation

- Guide d'hygiène informatique :
  http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Malware don't need Coffee :
  http://malware.dontneedcoffee.com

2 - Rappel des avis émis

Dans la période du 24 au 30 août 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-362 : Multiples vulnérabilités dans Apple QuickTime
- CERTFR-2015-AVI-363 : Vulnérabilité dans Adobe ColdFusion
- CERTFR-2015-AVI-364 : Vulnérabilité dans Siemens SIMATIC
- CERTFR-2015-AVI-365 : Multiples vulnérabilités dans Mozilla Firefox

Gestion détaillée du document

31 août 2015 version initiale.