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 17 août 2015
N° CERTFR-2015-ACT-033

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-033

1 - Maliciel XOR/DDoS

Cible et vecteur d'infection

Le CERT-FR a constaté une recrudescence du maliciel XOR/DDoS ciblant les systèmes d'exploitation GNU/Linux exposés sur Internet. Le vecteur d'infection aujourd'hui constaté est le protocole SSH : le maliciel s'installe à la suite d'une attaque réussie en force brute sur le mot de passe du compte root (attaque en ligne). Cette attaque en force brute est menée depuis une unique IP.

Installation et présence

Dès que l'attaque en force brute a réussi, le maliciel XOR/DDoS s'installe durablement sur le système. Plusieurs artéfacts peuvent être retrouvés dans le système de fichiers :

- une tâche cron est ajoutée afin de s'exécuter toutes les 3 minutes. Le script exécuté est ajouté dans le répertoire "/etc/cron.hourly/" et porte le nom d'un programme Linux légitime avec l'extension .sh ;
- des liens symboliques sont créés dans les dossiers /etc/rc.d/rcXXX.d/ ou /etc/rcXXX.d/ et portent un nom commençant par "S90" ou "S01" suivi de 10 caractères aléatoires. Ces liens pointent vers un script du répertoire /etc/init.d/ exécutant un binaire malveillant de même nom depuis /usr/bin/. La chaine de caractères aléatoires se retrouve dans le nom du script et du binaire ;
- un binaire est placé sous la forme d'un fichier .so dans le dossier /lib/ et porte le nom d'un programme Linux légitime ;
- plusieurs binaires sont déposés dans le dossier /usr/bin/ : le nom des fichiers est composé de 10 caractères aléatoires.

Le fichier d'extension .sh présent dans le dossier /etc/cron.hourly/ comprend également une portion de code visant à activer toutes les interfaces réseau disponibles (correspondant à la troisième ligne du script) et contient les lignes suivantes :

```
PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:/usr/X11R6/bin
for i in `cat /proc/net/dev|grep~:|awk -F: {'print $1'}`; do ifconfig $i up& done
cp /lib/<NOM_DE_LIBRAIRIE>.so /lib/<NOM_DE_LIBRAIRIE>.so.<SUFFIXE>
/lib/<NOM_DE_LIBRAIRIE>.so.<SUFFIXE>
```

Fonctionnalités et fonctionnement

Ce binaire peut servir d'outil d'administration à distance notamment avec des fonctions de téléchargement/exécution, de mise à jour et de collecte d'informations sur la machine infectée. Il dispose aussi d'une fonctionnalité lui permettant de recevoir des marqueurs système et réseau afin d'arrêter les processus correspondants et de supprimer le binaire associé. Ce binaire intègre également des fonctions spécifiques pour mener une attaque en déni de service (TCP SYN flood, attaque TCP ACK flood et amplification DNS).

Afin de complexifier sa détection sur le disque, lorsque le maliciel se copie sur le système, il ajoute onze octets à la fin du nouveau fichier (10 caractères aléatoires comme pour les noms de fichiers et un caractère nul de fin de chaîne de caractères) pour ne pas être détecté par des méthodes de recherche de condensat des fichiers. Par ailleurs, le maliciel se cache de la liste des processus obtenue par l'utilitaire "ps" en remplaçant son nom par une commande courante (choisie dans une liste d'une douzaine de commandes codée en dur dans le binaire).

Au niveau réseau, les communications que le binaire échange avec son serveur de contrôle et de commandes sont chiffrées au moyen d'une clef XOR de 16 octets présente dans le code du maliciel. Enfin, ce maliciel peut inclure, ou télécharger, un module noyau qui fournit des fonctionnalités de dissimulateur d'activité (rootkit), notamment la dissimulation des fichiers du maliciel présents sur le disque, mais aussi les ports réseau qu'il utilise.

Remédiation

Comme ce maliciel permet le téléchargement et l'exécution de binaires avec les privilèges de l'utilisateur root, il convient de réinstaller le système en intégralité afin de se protéger de toute modification non-détectée du système et qui aurait pu être effectuée. Si pour des impératifs de production, il n'est pas possible de réinstaller la machine, il convient d'utiliser un système de démarrage de type LiveCD et d'effectuer l'ensemble des opérations suivantes afin de supprimer complètement l'infection spécifique par ce maliciel :

- inspecter les scripts de /etc/cron-hourly/ référencés dans le fichier /etc/crontab pour voir si un des scripts correspond au maliciel XOR/DDoS ;
- noter et supprimer la ligne du fichier /etc/crontab correspondant au maliciel ;
- étudier le contenu du fichier de tâche cron préalablement relevé et supprimer les deux fichiers apparaissant dans la ligne "cp" ;
- supprimer le script cron ;
- rechercher dans /etc/rc* les liens symboliques dont le nom commence par "S90" ou "S01" suivi d'une chaine de 10 caractères dénuée de sens, dont le script cible ne fait qu'exécuter un binaire de /usr/bin/ de même nom ;
- supprimer tous les liens symboliques identifiés et avérés ainsi que les fichiers pointés.

Prévention

Étant donné que le seul vecteur d'infection connu de cette menace reste l'attaque réussie en force brute sur le mot de passe du compte root via SSH, les recommandations de configuration d'un serveur SSH de l'ANSSI sont à appliquer, notamment :

- ne pas autoriser la connexion via le compte root ;
- privilégier une authentification par clef à chiffrement asymétrique.

Il est également possible d'atténuer les risques d'une attaque triviale en modifiant le port d'écoute SSH vers une valeur non-standard. L'ensemble de ces mesures nécessite d'être préalablement testées avant d'être appliquées.

De manière générale et non spécifique à SSH, le mot de passe du compte root doit impérativement respecter les bonnes pratiques en termes de complexité de mot de passe comme recommandé par l'ANSSI. Dans l'hypothèse d'un autre nouveau vecteur d'infection, il convient d'observer l'utilisation des équipements comme moyen de déni de service : utilisation réseau, utilisation processeur, fichiers de journalisation des applicatifs installés, etc.

Liens

- Anatomie d'une campagne d'attaque en force brute :
  https://www.fireeye.com/blog/threat-research/2015/02/anatomy_of_a_brutef.html
- Bonnes pratiques ANSSI configuration SSH :
  http://www.ssi.gouv.fr/guide/recommandations-pour-un-usage-securise-dopenssh/
- Bonnes pratiques ANSSI complexité mot de passe :
  http://www.ssi.gouv.fr/guide/mot-de-passe/

2 - Mise à jour mensuelle de Microsoft

Le 11 août 2015, Microsoft a publié 14 bulletins de sécurité, dont 4 sont considérés comme critiques et 10 comme importants :

- MS15-079 (critique) qui concerne Internet Explorer ;
- MS15-080 (critique) qui concerne le composant graphique de Windows ;

– MS15-081 (critique) qui concerne Microsoft Office ;
– MS15-082 (important) qui concerne l'implémentation du protocole RDP ;
– MS15-083 (important) qui concerne le serveur SMB ;
– MS15-084 (important) qui concerne XML Core Services ;
– MS15-085 (important) qui concerne le gestionnaire de montage de Windows ;
– MS15-086 (important) qui concerne le System Center Operations Manager de Windows ;
– MS15-087 (important) qui concerne le service UDDI de Windows ;
– MS15-088 (important) qui concerne Windows ;
– MS15-089 (important) qui concerne WebDAV ;
– MS15-090 (important) qui concerne Windows ;
– MS15-091 (critique) qui concerne Edge ;
– MS15-092 (important) qui concerne Microsoft .NET Framework.

Les navigateurs de Microsoft, Internet Explorer et Edge, font l'objet de deux bulletins. Le bulletin MS15-079 corrige dans Internet Explorer treize vulnérabilités pouvant conduire à une exécution de code à distance, un contournement de la distribution aléatoire de l'espace d'adressage (ASLR) ou une élévation de privilèges. Quatre de ces vulnérabilités (CVE-2015-2441, CVE-2015-2442, CVE-2015-2446 et CVE-2015-2449) sont également corrigées dans Edge par le bulletin MS15-091.

Le bulletin MS15-080 corrige quant à lui seize vulnérabilités dans le composant Microsoft Graphics. Ces différentes vulnérabilités concernent notamment la gestion des polices de caractère par les produits Microsoft. Leur exploitation peut conduire à une exécution de code arbitraire, une élévation de privilèges ou un contournement de la distribution aléatoire de l'espace d'adressage.

Microsoft Office fait l'objet de huit vulnérabilités corrigées. Elles portent principalement sur des corruptions de mémoire. Un dépassement d'entier est également corrigé. L'exploitation de ces vulnérabilités peut notamment passer par l'ouverture d'un fichier spécialement conçu et peut conduire à une exécution de code à distance. Au moins l'une des vulnérabilités (CVE-2015-1642) est activement exploitée.

L'implémentation du protocole RDP (bureau à distance) est touchée par deux vulnérabilités. L'une d'entre elles permet une usurpation d'identité par un intermédiaire malintentionné, à cause d'une mauvaise gestion de la vérification des certificats. L'autre vulnérabilité peut conduire à une exécution de code arbitraire à distance si l'utilisateur visite un site Internet spécialement conçu.

Une vulnérabilité permettant l'exécution de code à distance est aussi corrigée dans l'implémentation de SMB de Microsoft Windows. Cette vulnérabilité se situe dans le système de journalisation des connexions. Son exploitation nécessite d'avoir déjà en sa possession des identifiants pour se connecter au système.

Concernant XML Core Services, trois vulnérabilités sont corrigées. L'une d'elles peut conduire à une divulgation d'adresses de la mémoire, si l'utilisateur visite une page Web spécialement conçue avec Internet Explorer.

Le gestionnaire de montage de périphériques de Microsoft Windows se voit corrigé d'une élévation de privilèges. Cette vulnérabilité nécessite l'insertion d'un périphérique USB malveillant dans la machine cible. À cette occasion, le CERT-FR réitère la vigilance particulière à apporter quant à la connexion de périphériques inconnus à une machine. De plus, selon Microsoft, cette vulnérabilité est activement exploitée, notamment dans le cadre d'attaques ciblées.

La vulnérabilité corrigée dans le System Center Operations Manager de Microsoft Windows permet une élévation de privilèges. Pour que cette vulnérabilité soit exploitée, la victime doit se rendre sur une page Web spécialement conçue afin d'exécuter un script malveillant.

Une élévation de privilèges est aussi corrigée dans les services UDDI (*Universal Description, Discovery and Integration*) de Microsoft Windows. Son exploitation peut conduire à la récupération de cookies d'authentification.

Concernant Microsoft Windows, deux bulletins corrigent des vulnérabilités. Le bulletin MS15-088 permet de corriger une fuite d'information suite à une transmission non sécurisée des paramètres de ligne de commandes de Windows. Quant au bulletin MS15-90, il corrige plusieurs élévations de privilèges.

Une atteinte à la confidentialité des données dans l'implémentation de WebDAV est corrigée. Cette vulnérabilité permet à un attaquant de déchiffrer une partie du trafic si la communication se déroule en SSLv2.

Enfin, le bulletin MS15-092 corrige de multiples vulnérabilités pouvant conduire à une élévation de privilèges dans le cadriciel .NET. Ces vulnérabilités résident dans de mauvaises optimisations de code réalisées par le compilateur concomitant RyuJIT.

Le CERT-FR recommande l'application dès que possible de ces correctifs de sécurité.

Documentation

- Bulletin de sécurité Microsoft MS15-079
  https://technet.microsoft.com/library/security/MS15-079
- Bulletin de sécurité Microsoft MS15-080
  https://technet.microsoft.com/library/security/MS15-080
- Bulletin de sécurité Microsoft MS15-081
  https://technet.microsoft.com/library/security/MS15-081
- Bulletin de sécurité Microsoft MS15-082
  https://technet.microsoft.com/library/security/MS15-082
- Bulletin de sécurité Microsoft MS15-083
  https://technet.microsoft.com/library/security/MS15-083
- Bulletin de sécurité Microsoft MS15-084
  https://technet.microsoft.com/library/security/MS15-084
- Bulletin de sécurité Microsoft MS15-085
  https://technet.microsoft.com/library/security/MS15-085
- Bulletin de sécurité Microsoft MS15-086
  https://technet.microsoft.com/library/security/MS15-086
- Bulletin de sécurité Microsoft MS15-087
  https://technet.microsoft.com/library/security/MS15-087
- Bulletin de sécurité Microsoft MS15-088
  https://technet.microsoft.com/library/security/MS15-088
- Bulletin de sécurité Microsoft MS15-089
  https://technet.microsoft.com/library/security/MS15-089
- Bulletin de sécurité Microsoft MS15-090
  https://technet.microsoft.com/library/security/MS15-090
- Bulletin de sécurité Microsoft MS15-091
  https://technet.microsoft.com/library/security/MS15-091
- Bulletin de sécurité Microsoft MS15-092
  https://technet.microsoft.com/library/security/MS15-092
- Avis de sécurité CERTFR-2015-AVI-333
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-333
- Avis de sécurité CERTFR-2015-AVI-334
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-334
- Avis de sécurité CERTFR-2015-AVI-335
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-335
- Avis de sécurité CERTFR-2015-AVI-336
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-336
- Avis de sécurité CERTFR-2015-AVI-337
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-337
- Avis de sécurité CERTFR-2015-AVI-338
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-338
- Avis de sécurité CERTFR-2015-AVI-339
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-339
- Avis de sécurité CERTFR-2015-AVI-340
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-340
- Avis de sécurité CERTFR-2015-AVI-341
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-341
- Avis de sécurité CERTFR-2015-AVI-342
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-342
- Avis de sécurité CERTFR-2015-AVI-343
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-343
- Avis de sécurité CERTFR-2015-AVI-344
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-344
- Avis de sécurité CERTFR-2015-AVI-345
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-345

– Avis de sécurité CERTFR-2015-AVI-346
http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-346

3 - Rappel des avis émis

Dans la période du 10 au 16 août 2015, le CERT-FR a émis les publications suivantes :

– CERTFR-2015-AVI-332 : Multiples vulnérabilités dans IBM Tivoli Monitoring
– CERTFR-2015-AVI-333 : Multiples vulnérabilités dans Microsoft Internet Explorer
– CERTFR-2015-AVI-334 : Multiples vulnérabilités dans le composant Microsoft Graphics
– CERTFR-2015-AVI-335 : Multiples vulnérabilités dans Microsoft Office
– CERTFR-2015-AVI-336 : Multiples vulnérabilités dans le protocole RDP de Microsoft Windows
– CERTFR-2015-AVI-337 : Vulnérabilité dans le protocole SMB de Microsoft Windows
– CERTFR-2015-AVI-338 : Multiples vulnérabilités dans Microsoft XML Core Services
– CERTFR-2015-AVI-339 : Vulnérabilité dans le gestionnaire de montage de périphériques de Microsoft Windows
– CERTFR-2015-AVI-340 : Vulnérabilité dans Microsoft System Center Operations Manager
– CERTFR-2015-AVI-341 : Vulnérabilité dans les services UDDI de Microsoft Windows
– CERTFR-2015-AVI-342 : Vulnérabilité dans Microsoft Windows
– CERTFR-2015-AVI-343 : Vulnérabilité dans WebDAV
– CERTFR-2015-AVI-344 : Multiples vulnérabilités dans Microsoft Windows
– CERTFR-2015-AVI-345 : Multiples vulnérabilités dans Microsoft Edge
– CERTFR-2015-AVI-346 : Multiples vulnérabilités dans Microsoft .NET Framework
– CERTFR-2015-AVI-347 : Multiples vulnérabilités dans Adobe Flash
– CERTFR-2015-AVI-348 : Multiples vulnérabilités dans Google Chrome
– CERTFR-2015-AVI-349 : Multiples vulnérabilités dans Mozilla Firefox
– CERTFR-2015-AVI-350 : Multiples vulnérabilités dans Wireshark
– CERTFR-2015-AVI-351 : Vulnérabilité dans Mozilla Firefox
– CERTFR-2015-AVI-352 : Multiples vulnérabilités dans le noyau Linux de Red Hat
– CERTFR-2015-AVI-353 : Multiples vulnérabilités dans Apple Safari
– CERTFR-2015-AVI-354 : Multiples vulnérabilités dans Apple iOS
– CERTFR-2015-AVI-355 : Multiples vulnérabilités dans Apple OS X
– CERTFR-2015-AVI-356 : Vulnérabilité dans Apple OS X Server

Gestion détaillée du document

17 août 2015 version initiale.