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 07 avril 2015
N° CERTFR-2015-ACT-014

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-014

1 - Opération de cybersabotage avec Destover

Fin 2014, une grande entreprise de divertissement a été victime d'une attaque ciblée et d'une opération de sabotage. La phase terminale de l'attaque a permis la destruction de nombreux systèmes d'information de l'entreprise. Pour effectuer cette opération, les attaquants ont utilisé un code malveillant nommé *Destover*, permettant de détruire les disques connectés à une machine.

Déploiement du code

Le code arrive sur la machine cible (servant de point d'entrée sur le réseau) sous forme d'un déployeur de charge. Une fois lancé, ce code s'installe en tant que service. Il dépose alors sur la machine cible la charge utile de destruction et, en parallèle, parcourt le réseau Windows à la recherche d'autres machines à infecter.

Une fois de nouvelles machines cibles repérées, il dépose et installe chez elles la charge.

De cette façon, le code se répend sur le réseau interne de l'entreprise pour toucher un maximum de systèmes.

Charge utile

La charge utile déposée est le code principal de *Destover*. Ce code prend une valeur en argument et c'est par ce biais qu'il active ses différentes fonctionnalités :

- sans argument : lancement d'une instance de lui-même avec l'argument `-i` puis fermeture ;
- `-i` : mise en place de la persistance *via* un service ;
- `-k` : initiation de la destruction des données ;
- `-w` : dépôt d'un serveur web pour transmission du message de revendication ;
- `-m` : écrasement du MBR ;
- `-d` : suppression des données sur les disques.

Déroulement des opérations

Destover commence par mettre en place son moyen de persistance (argument `-i`). Pour cela, il crée un nouveau service nommé `brmgmtsvc` (`Backup and Restore Management Service`), dont le binaire est lui-même exécuté avec l'argument `-k`. Une fois le service installé, il charge le code puis s'arrête.

Le lancement du service a pour conséquence de démarrer la destruction des données. Cette phase se déroule de la façon suivante :

1. mise en sommeil du processus pendant 10 minutes ;
2. copie du binaire dans un fichier nommé `taskhost[a-z].exe` (`[a-z]` tiré aléatoirement) et situé dans le même répertoire puis exécution avec l'argument `-w` (serveur web) ;
3. mise en sommeil du processus pendant 3 secondes ;

4. copie du binaire dans un fichier nommé `taskhost[a-z].exe` (`[a-z]` tiré aléatoirement) et situé dans le même répertoire puis exécution avec l'argument `-m` (écrasement du MBR) ;
5. mise en sommeil du processus pendant 3 secondes ;
6. copie du binaire dans un fichier nommé `taskhost[a-z].exe` (`[a-z]` tiré aléatoirement) et situé dans le même répertoire puis exécution avec l'argument `-d` (effacement des fichiers) ;
7. mise en sommeil du processus pendant 3 secondes ;
8. récupération du nom de la machine sur le réseau local puis envoi à l'un de ses trois serveurs C&C ;
9. exécution la commande `cmd.exe /c net stop MSExchangeIS /y` (arrête le service de banque d'informations de Microsoft Exchange) ;
10. mise en sommeil du processus pendant 2 heures ;
11. redémarrage du système.

Il lance donc trois processus en parallèle, chacun exécutant une fonctionnalité.

Écrasement du MBR Pour rendre les disques durs non fonctionnels, *Destover* écrase les 65536 premiers octets de chacun des disques logiques de la machine.

Pour effectuer cette opération, il se base sur un pilote commercial permettant de manipuler en brut les données d'un disque dur : `elrawdsk.sys` du logiciel *ElRawDisk* de EldoS Corporation. Ce pilote est contenu dans les ressources. Le pilote est déposé sous le chemin `%TEMP%\usbdrv_3.sys` puis enregistré en tant que service.

Pour manipuler les données d'un disque logique à travers le pilote, le code malveillant commence par créer un handle vers le fichier `\\?\ElRawDisk\??\PhysicalDrive0#<licence>` : `PhysicalDrive0` est incrémenté pour s'attaquer à tous les disques et la chaîne `<licence>` précédée par `#` est un numéro de licence pour utiliser le pilote. Il génère ensuite trois tampons de 65536 octets :

- le premier est la répétition de l'octet `0xAA` ;
- le deuxième est la répétition de l'octet `0x55` ;
- le troisième est un ensemble de données aléatoires.

Voici le code de génération de ces trois tampons :

```
     .text:0040145C                 mov     bl, 0x55
  +-> .text:0040145E boucle:
  |   .text:0040145E                 mov     [esp+edi+300E0h+buf1], 0xAA
  |   .text:00401466                 mov     [esp+edi+300E0h+buf2], bl
  |   .text:0040146D                 call    _rand
  |   .text:00401472                 mov     cl, 0xFB
  |   .text:00401474                 imul    cl
  |   .text:00401476                 mov     [esp+edi+300E0h+buf3], al
  |   .text:0040147D                 inc     edi
  |   .text:0040147E                 cmp     edi, 65536
  +-- .text:00401484                 jl      short boucle
```

Une fois ces trois jeux de données créés, grâce au handle, il les écrit successivement au début du disque courant.

Cette opération a donc pour effet d'effacer les 65536 premiers octets de chacun des disques. De cette façon, il s'assure d'écraser le MBR et toute autre donnée (table des partitions, etc.) permettant au disque d'être utilisable : les disques sont donc rendus inopérants (démarrage impossible de la machine et effacement des informations sur les fichiers contenus dedans).

Effacement des fichiers Le code malveillant dispose d'une fonctionnalité permettant d'effacer l'ensemble des fichiers présents sur les disques montés sur la machine. Pour cela, il commence par récupérer la liste des disques logiques du système. Ensuite, il regarde le type de chacun des disques : il ne lance la procédure d'effacement que sur les disques internes (disques durs ou SSD par exemple) ou les partages réseau.

La procédure d'effacement consiste à parcourir l'ensemble d'un disque de manière récursive (sur chacun des répertoires) et à supprimer chaque fichier (dans le cas où le fichier ne se termine pas par l'extension `.exe` ou `.dll`, le contenu du fichier est réécrit avant suppression). Néanmoins, une exception est faite dans le cas où le répertoire est `%PROGRAMFILES` ou `%WINDIR%` : dans ce cas, le répertoire est évité.

Serveur de fichiers Cette fonctionnalité, activée avec l'argument `-w`, permet de déposer un dernier code sur le système sous le chemin `C:\Windows\iisvr.exe`. Ce code est un serveur de fichiers (écoute sur le port 80) qui met à disposition sur le réseau local trois fichiers (chiffrés en ressources) : un fichier HTML, un fichier JPEG et un fichier WAV. Ces trois éléments représentent le message de revendication des attaquants affichés sur les postes une fois l'attaque effectuée.

Recommandations

L'attaque menée contre cette entreprise montre que les conséquences d'une intrusion peuvent parfois causer de lourds dommages. En effet, si les premières phases de l'attaque sont relativement classiques (intrusions, reconnaissance du réseau, exfiltration de données sensibles), la phase finale a consisté en une destruction irrémédiable des ordinateurs de bureau et serveurs de l'entreprise. La conséquence de l'attaque est donc similaire à celles issues d'une campagne de type rançongiciel (sans la récupération des fichiers).

Le CERT-FR insiste sur la nécessité de réaliser des sauvegardes des données les plus critiques sur des supports hors ligne, afin de minimiser l'impact d'une attaque de ce type. D'une façon plus générale, le CERT-FR recommande de maintenir une certaine vigilance et d'appliquer les recommandations de l'ANSSI mentionnées dans le guide d'hygiène informatique cité en référence.

Documentation

- Guide d'hygiène informatique
  http://ssi.gouv.fr/guide/guide-dhygiene-informatique
- Campagne de type rançongiciel
  http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ALE-003/index.html
- Alerte de l'US-CERT
  https://www.us-cert.gov/ncas/alerts/TA14-353A

2 - Recommandations de configuration matérielle de postes clients et serveurs x86.

Le 25 mars 2015, l'ANSSI a publié une note technique de recommandations pour la configuration matérielle des postes clients et serveurs x86. Ce document revient aussi bien sur les fonctionnalités matérielles des processeurs x86, qui offrent de nouvelles protections aux systèmes d'exploitation, que sur celles qui introduisent de nouvelles vulnérabilités.

Plusieurs recommandations sont proposées pour :
- le choix du type de processeur (x86 64 ou 32 bits);
- la configuration du droit d'exécution mémoire (Bit NX/XD);
- les vulnérabilités introduites par la technologie d'Hyper-Threading;
- l'élévation de privilège (SMEP et SMAP);
- les nouvelles instructions cryptographiques x86 (AES-NI / RDRAND / RDSEED);
- les fonctions de virtualisation VT-x/AMD-V et VT-d/AMD-Vi;
- la configuration du BIOS/UEFI.

Cette note technique peut être consultée ou téléchargée en suivant le lien ci-dessous :
http://www.ssi.gouv.fr/uploads/2015/03/NP_ConfigMateriel.pdf

3 - Rappel des avis émis

Dans la période du 30 mars au 05 avril 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-129 : Vulnérabilité dans Huawei Campus Switch
- CERTFR-2015-AVI-130 : Multiples vulnérabilités dans Xen
- CERTFR-2015-AVI-131 : Multiples vulnérabilités dans les produits Mozilla
- CERTFR-2015-AVI-132 : Multiples vulnérabilités dans les produits Schneider Electric
- CERTFR-2015-AVI-133 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2015-AVI-134 : Multiples vulnérabilités dans Cisco Unity Connection
- CERTFR-2015-AVI-135 : Vulnérabilité dans Cisco Prime DCNM

Gestion détaillée du document

07 avril 2015 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-2015-ACT-014