StuxNet

ou le projet "Olympic Games"

COMPTE RENDU
DE PRESENTATION

G.OLLIER / C.SONNTAG | M1 INFO GL | 25/10/2017

Sommaire

I – L'histoire de StuxNet

Stuxnet est un **ver informatique** spécifique au système Windows.
Découvert en 2010, il aurait été conçu par la NSA, en collaboration avec l'unité israélienne de renseignement nommé « 8200 », pour s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium.

Le programme semble avoir été initié sous l'administration Bush vers 2008 et aurait continué sous l'administration Obama.

Il ferait partie de l'opération « Olympic Games » qui vise à **ralentir** le programme nucléaire iranien.

Il a été découvert en juin 2010 par « VirusBlokAda », société de sécurité informatique basée en Biélorussie.

Le nombre de « Zero-days » utilisé, c'est à dire les failles ne possédant aucune publication à son sujet, est très inhabituel, ces « exploits » sont très précieux et **les pirates n'en utilisent jamais plusieurs à la fois**.

La présence de différent code, en plus de code Assembleur, C et C++, est pour un malware quelque chose de très inhabituelle aussi.

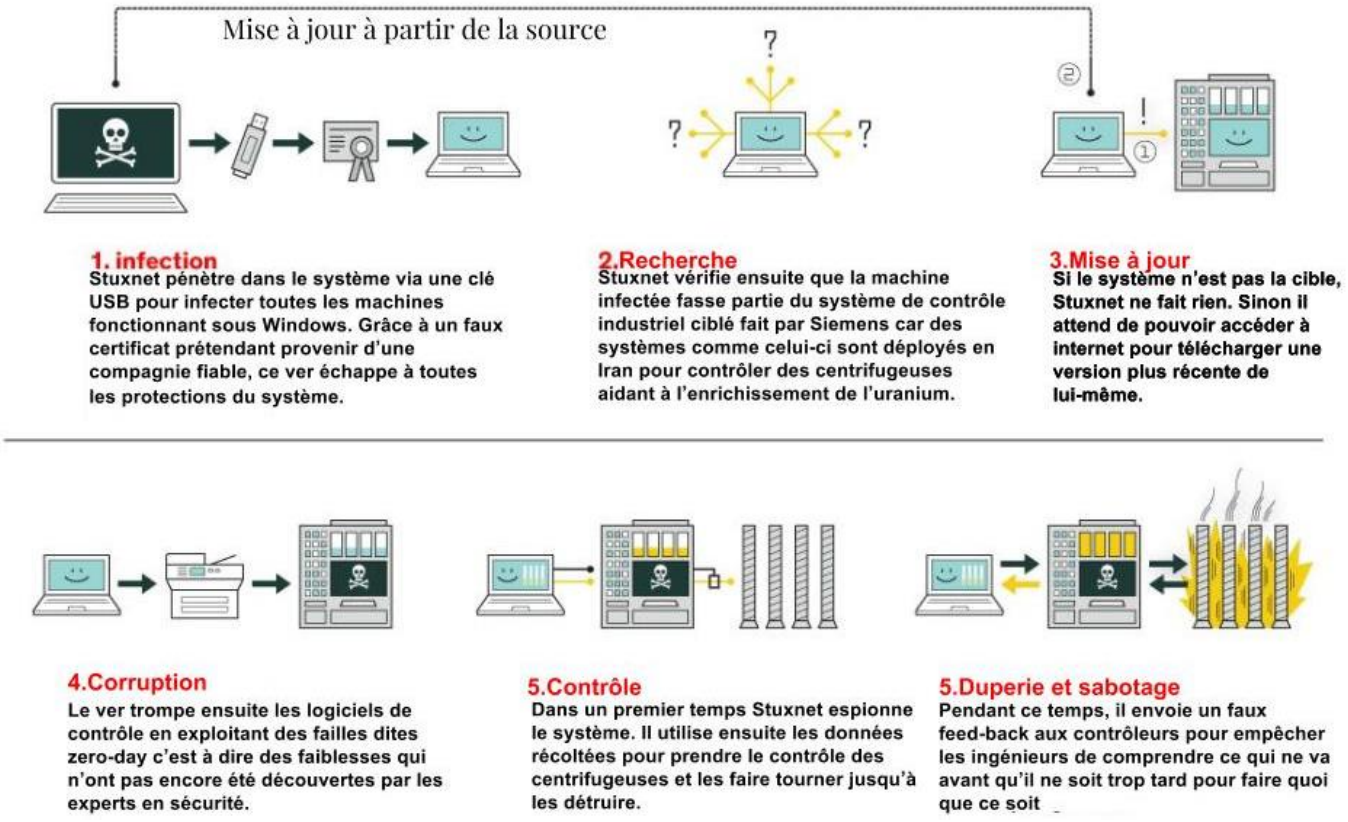
Vulnérabilité « Zero-Day »

Les vulnérabilités « Zero-days » sont donc des failles d'une grande envergure, elles peuvent causer des **dommages irréparables sur des grandes infrastructures**, tel qu'un gouvernement.

Ainsi, les développeurs d'antivirus et de système d'exploitation, tel que Microsoft, doivent constamment soumettre des tests, pour trouver les possibles failles.
Alors enfin, des correctifs, ou mise à jours, classées importantes seront promu pour éviter toutes failles « Zero-day » nouvellement trouvées.

Il faudra cependant que les utilisateurs appliquent ces correctifs, ce qui n'est pas toujours le cas.

II – Comment StuxNet fonctionne



Vulnérabilités rencontrées :

Ainsi, dans ce processus de corruption, l'on peut retrouver différentes vulnérabilités exploitées.

- « 1. Infection » :
  Utilise la vulnérabilité « CPLNK » pour s'exécuter.
  Un faux certificat Windows est inclus dans le programme, pour outrepasser les dispositifs de détection antivirus.

- « 4. Corruption du réseau » :
  Utilise la vulnérabilité « PrintSpooler » ainsi que
  « ServerService RemoteCodeExecution » pour diffuser le ver.

- « 5. Contrôle » / « 6. Duperie et sabotage » :
  Utilise la vulnérabilité « ServerService RemoteCodeExecution » pour à la fois, exécuter du code sur les automates Siemens, et pour interférer/corrompre les retours d'information renvoyer par ces automates.

III – Vulnérabilités utilisées

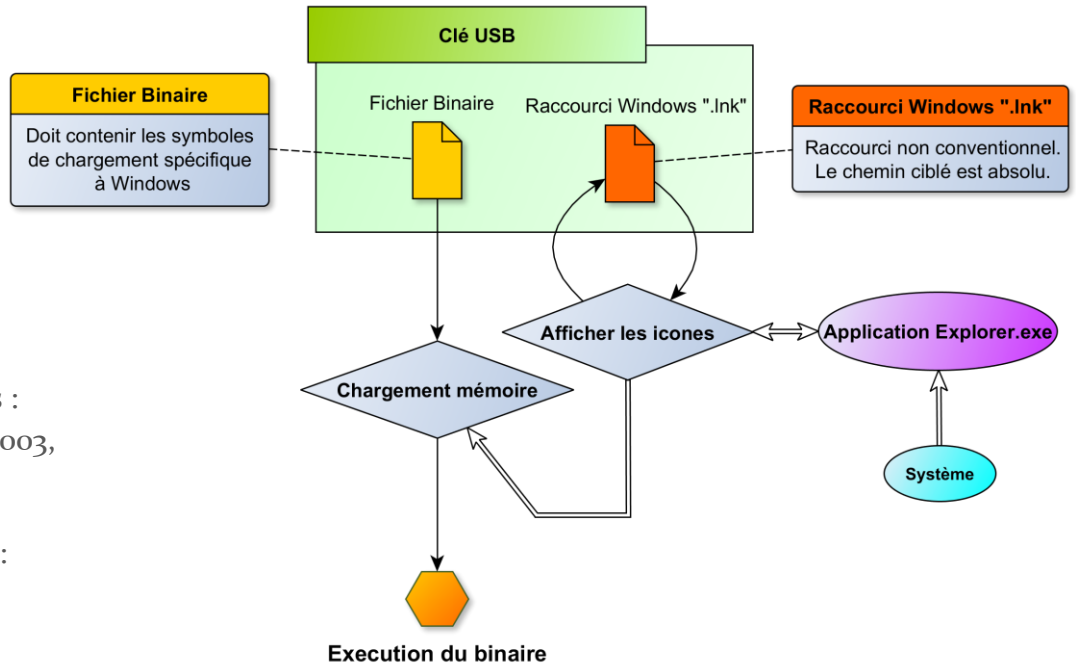
- Vulnérabilité « CPLNK »

Ce module exploite la vulnérabilité au processus « explorer.exe ».
Cette faille repose sur **le chargement en mémoire de fichier binaire** par le simple moyen d'afficher un raccourci Windows.

Un raccourci Windows est un fichier d'extension « .lnk » qui cible un programme, dossier ou fichier. Contrairement à un raccourci conventionnel, celui utilisé pour cette vulnérabilité comporte seulement quelques informations et le chemin du fichier ciblé.

Lors de l'ouverture d'un dossier avec le processus « explorer.exe », tel que l'ouverture automatique d'une clé USB, celui-ci va **essayer de charger les icônes** liées aux applications, raccourcis Windows et dossiers.

Cependant, lorsque le processus « explorer.exe » est confronté à un raccourci Windows, si le fichier **ciblé est un fichier binaire** particulier, alors ce fichier est **chargé en mémoire**, incluant une **exécution implicite**. En particulier, ce fichier binaire doit être de format « DynamicLibrary » avec des symboles d'entrées spécifique à Windows, par exemple « DllEntryPoint ».



Système concernés :
Version de Windows :
XP, Vista, Server 2003, Server 2008, 7

Découverte de la faille :
15 juillet 2010

Voir fichier joint « ExploitCPLNK.tar.gz » pour trouver un exemple d'utilisation de l'exploit (fichiers sources utilisés pour la démonstration lors de la présentation). Attention toutefois à une alerte Antivirus. Une vidéo de démonstration est aussi disponible ici :
http://open.store.u4a.at/Luminy/Presentation/ManipCPLINK.mp4

Plus d'informations : http://www.securityfocus.com/bid/41732/discuss

- Vulnérabilité « PrintSpooler »

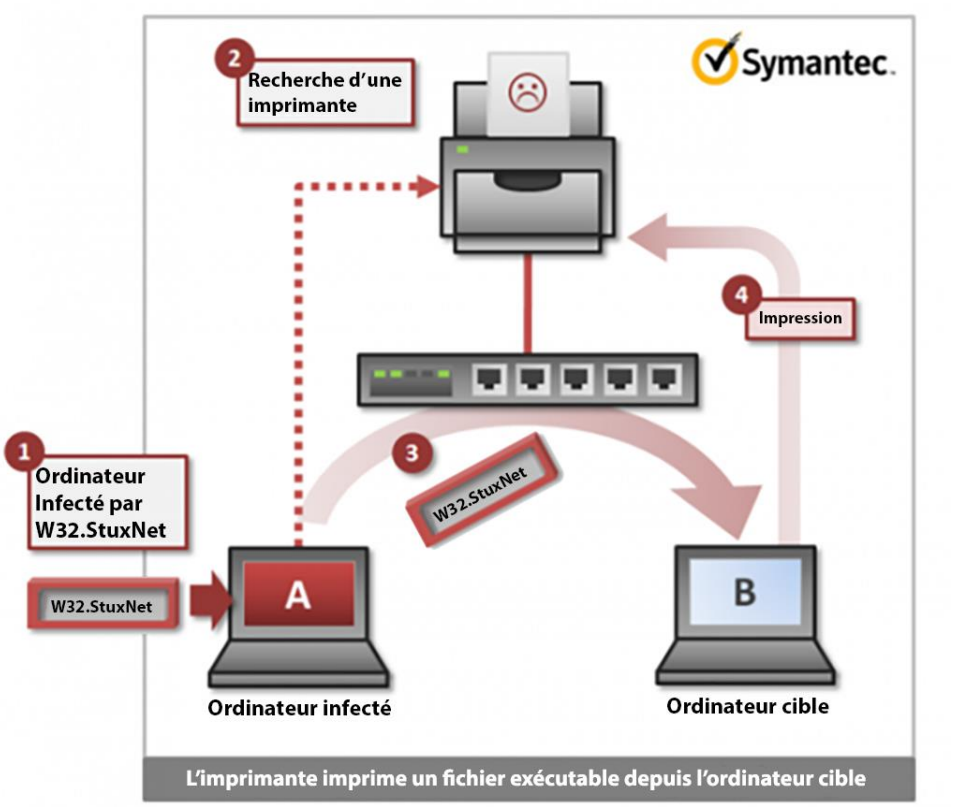
Ce module exploite la vulnérabilité d'emprunt d'identité de service RPC détaillée dans Microsoft Bulletin MS10-061. En effectuant une requête **RPC** DCE spécifique à la procédure StartDocPrinter, un attaquant peut emprunter l'identité du **service Spouleur d'imprimante** pour créer un fichier.

Un attaquant peut spécifier n'importe quel nom de fichier, y compris une traversée de **répertoire** ou des chemins complets. En envoyant des requêtes « WritePrinter », un attaquant peut entièrement contrôler le contenu du fichier créé. Afin d'obtenir l'exécution de code, ce module écrit dans un **répertoire** utilisé par **Windows Management Instrumentation** (**WMI**) pour déployer des applications.

Ce **répertoire** (Wbem\Mof) est analysé périodiquement et tous les nouveaux fichiers « .mof » sont traités automatiquement

Système concernés :
Version de Windows :
XP, Vista, Server 2003, Server 2008, 7

Découverte de la faille :
14 septembre 2010

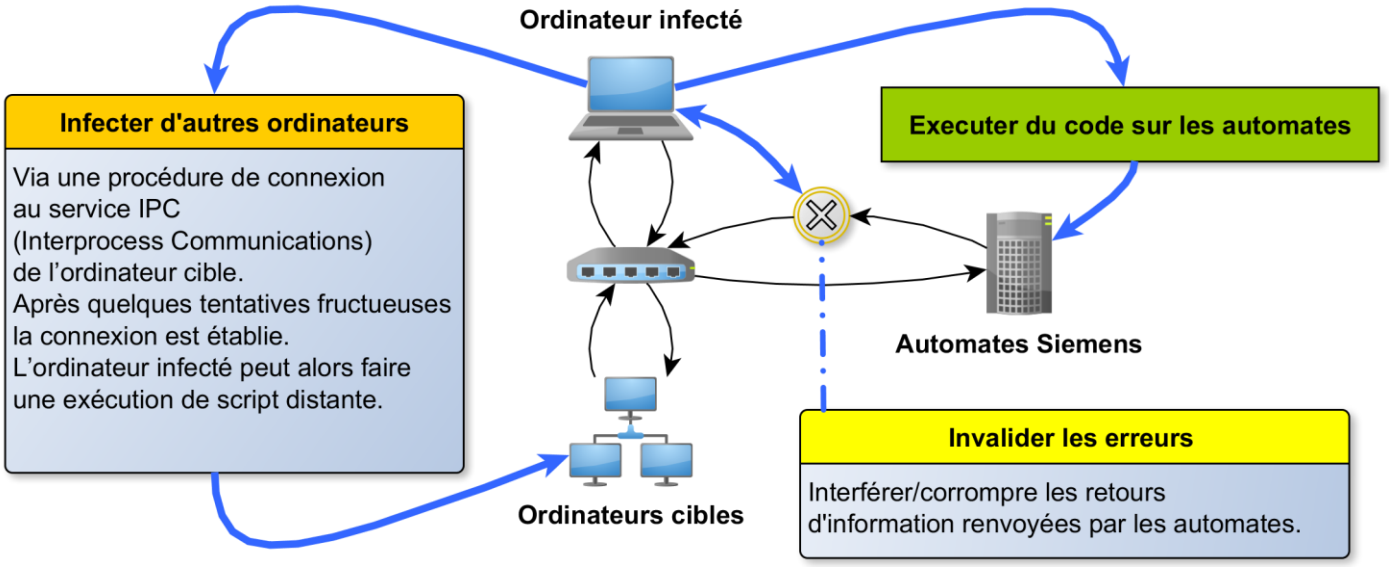


Plus d'informations : http://www.securityfocus.com/bid/43073/discuss

- Vulnérabilité « ServerService RemoteCodeExecution »

Ce module exploite la vulnérabilité **d'exécution de code à distance** gérée par le service de gestion des appels « **RPC** » (**Remote Procedure Call**) inclus dans le service Serveur de Windows.

Les instructions sont alors directement faites avec l'application « **net.exe** » de Windows.
Exemple : « `net use \\IPADDRESS\IPC$ /user:user creds` »



Remarque, sur les versions Windows, Vista et Server 2008, il faut s'authentifier au service.

Système concernés :
Version de Windows : 2000, XP, Vista, Server 2003, Server 2008
Serveur/Moniteur : Siemens, Nortel Networks, Avaya Messaging

Découverte de la faille : 22 octobre 2008

Plus d'informations : http://www.securityfocus.com/bid/31874/discuss

Conclusion

Ces attaques d'un genre nouveau nous montrent à quel point nos infrastructures publique pourrait être **vulnérable à une cyberattaque**.

Il devient donc urgent de renforcer nos systèmes de sécurité afin de nous en protéger.
La Russie, la Chine et la Corée du Nord et les organisations terroristes étant les plus susceptible d'attaquer l'Europe.

Et c'est déjà arrivé ! En 2007, les sites internet gouvernementales estoniens **furent bloqués** par des ultranationalistes russes pour avoir déboulonné une statue soviétique.