LEXSI
INNOVATIVE SECURITY

STUXNET

DE LA VULNÉRABILITÉ LNK AU SABOTAGE INDUSTRIEL

CERT LEXSI

JANVIER 2011

LEXSI
INNOVATIVE SECURITY

SOMMAIRE

1 Introduction

Le 10/07/2010, l'éditeur antivirus biélorusse VirusBlockAda annonce[1] avoir trouvé le 17/06/2010 dans la nature un nouveau malware exploitant une vulnérabilité non connue dans Microsoft Windows. Au lieu d'utiliser le classique AutoRun sur clés USB, la propagation de ce malware est en effet assurée par l'utilisation de fichiers de raccourcis LNK, sans nécessiter d'autre interaction de l'utilisateur que la simple visualisation du périphérique dans l'explorateur Windows. L'annonce est passée inaperçue dans la communauté de la sécurité jusqu'à ce qu'elle soit reprise sur des blogs à fort trafic comme Kaspersky[2] ou Krebs on Security[3] : il s'agit bel et bien d'une 0-day dans Windows exploitée dans la nature par un malware.

La première analyse technique publiée par VirusBlockAda[4] révèle que ce malware est innovant à plusieurs titres :

- Il exploite une vulnérabilité 0-day dans la façon dont le shell de Windows traite les fichiers LNK afin d'infecter les machines via les clés USB, impactant toutes les versions de Windows y compris Windows 7 ;
- Sa rootkit en mode noyau utilise un pilote signé par un certificat légitime ;
- Il cible les équipements industriels SCADA.

Le malware existerait depuis au moins 2009[5]. Dans les semaines qui vont suivre cette découverte, d'autres analyses vont montrer qu'il réserve encore plus de surprises.

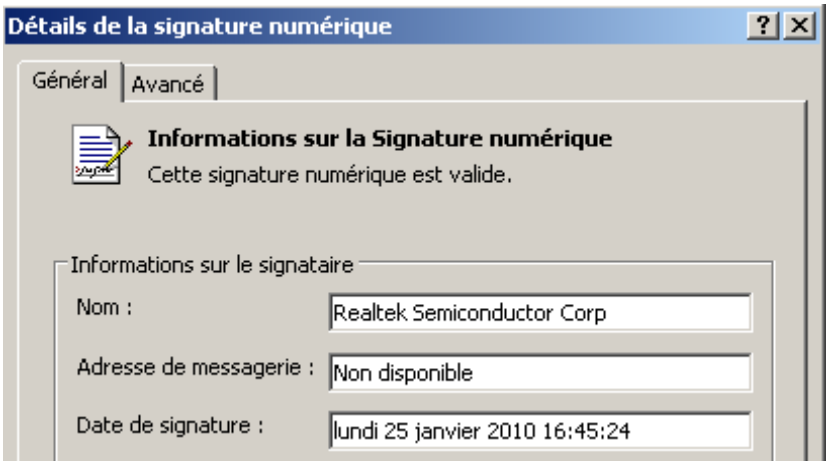
[1] http://anti-virus.by/en/tempo.shtml
[2] http://www.securelist.com/en/blog/269/Myrtus_and_Guava_Episode_1
[3] http://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw/
[4] http://www.secureblog.info/files/new_rootkit.pdf
[5] http://threatpost.com/en_us/blogs/Stuxnet-attack-shows-signs-nation-state-involvement-experts-say-080410

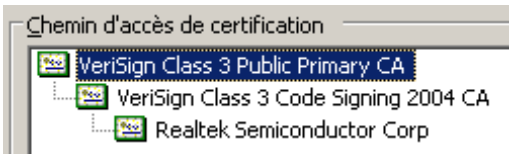
2 Pilotes signés

L'une des innovations de Stuxnet réside dans l'installation de pilotes noyaux signés. Sous Windows, la signature des exécutables se base sur la fonctionnalité Authenticode qui permet d'associer une signature cryptographique à certains types de fichiers afin de pouvoir vérifier leur intégrité et l'authenticité de leur éditeur. Lors de son exécution, Stuxnet dépose deux pilotes sur le disque :

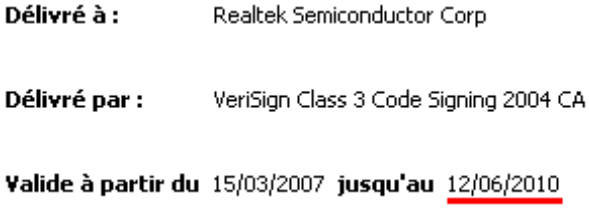
- C:\WINDOWS\system32\Drivers\mrxcls.sys ;
- C:\WINDOWS\system32\Drivers\mrxnet.sys.

Ces pilotes ont été signés le 25/01/2010, soit bien avant que le malware n'ait été mis au jour par VirusBlockAda, à l'aide d'une clé privée appartenant à la société Realtek. Le certificat associé à cette clé privée a été signé par l'autorité VeriSign Class 3 Code Signing 2004 CA, elle-même signée par l'autorité VeriSign Class 3 Public Primary CA installée par défaut dans le magasin de certificats Windows. La signature des binaires est donc parfaitement valide :

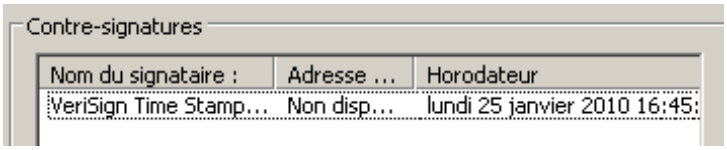




Remarque intéressante, le certificat Realtek n'est valide que jusqu'au 12/06/2010 :



Pourtant, Windows considérait encore la signature valide au mois de juillet lorsque l'existence de ce malware a été rendue publique. Le certificat possède effectivement un champ supplémentaire dit de "contre-signature", **ce qui permet au binaire d'être considéré valide par Authenticode même si le certificat l'ayant signé ne l'est plus**[6] :



Sur les versions 32 bits de Windows XP, Vista et 7, le système affiche un avertissement avant de charger un pilote noyau non signé ; sur les versions 64 bits, la signature est même obligatoire. Stuxnet contourne donc ces protections et peut donc charger son pilote sans aucune notification utilisateur. Verisign a révoqué le certificat le 16/07, en partenariat avec Microsoft et avec l'aval de Realtek[7].

Une autre variante de la rookit a été détectée le 17/07 par ESET[8], signée avec une autre clé privée légitime appartenant à la société JMicron. Il est intéressant de noter que les sociétés RealTek et JMicron ont des bureaux à Taiwan dans un même technopôle nommé Hsinchu Science Park. Les méta-informations du pilote semblent indiquer qu'il a été compilé le 14/07. Verisign a révoqué le certificat de Jmicron le 22/07.

Si ce n'est pas la première fois qu'un malware reçoit une signature Authenticode valide, **c'est en revanche la première fois que des certificats légitimes sont détournés afin de signer un malware**.

[6] http://msdn.microsoft.com/en-us/library/bb931395(VS.85).aspx
[7] http://blogs.technet.com/b/mmpc/archive/2010/07/16/the-Stuxnet-sting.aspx
[8] http://blog.eset.com/2010/07/19/win32Stuxnet-signed-binaries

3 Vulnérabilités exploitées

3.1 Vulnérabilité LNK (MS10-046, Ref. Lexsi 13709)

> *Jusqu'à présent, l'infection par clés USB utilisait principalement les fichiers autorun.inf afin de modifier la boite de dialogue pour y insérer une action malveillante. On peut par exemple citer Conficker qui poussait la technique jusqu'à aller récupérer dynamiquement la chaîne de caractères correspondant au message par défaut affiché lors de l'insertion d'une clé USB (sur les systèmes en Français : "Ouvrir le dossier pour afficher les fichiers"). Associé à l'icône par défaut des dossiers, ce texte faisait en sorte que le dialogue AutoPlay était plus que trompeur pour l'utilisateur qui, en cliquant sur cette première icône, exécutait le malware[9] en pensant simplement explorer le contenu de la clé. Microsoft, conscient du problème, a conçu Windows 7 pour ne plus afficher dans les fenêtres AutoPlay les tâches définies dans autorun.inf, sauf pour les CD et DVD (cette fonctionnalité a plus tard été publiée pour Windows XP et 2003 sous le correctif KB971029).*

3.1.1 Rappels des événements

Cette vulnérabilité a été découverte sous la forme d'une 0-day exploitée par Stuxnet. Un code d'exploitation a été publié dès le 18/07 sur le blog du Français Ivanlef0u[10].

Par la suite, alors que Stuxnet n'exploitait la vulnérabilité que pour se propager via les clés USB, la vulnérabilité se retrouve également exploitable via les partages SMB et WebDAV.

Microsoft a publié un avis officiel le 16/07[11], confirmant que toutes les versions de Windows sont impactées, et donnant les premières solutions de contournement (voir section 3.1.4). On notera d'ailleurs que d'autres versions de Windows non supportées sont également impactées, comme Windows 2000 et Windows XP avant SP3, et qu'aucun correctif ne sera donc publié pour ces systèmes.

Le bulletin Microsoft a été mis à jour par la suite afin d'indiquer que la vulnérabilité est également exploitable via les fichiers PIF ainsi que les documents supportant les raccourcis et les contrôles de navigateur embarqués, comme par exemple les documents Office. Le 30/07, Microsoft annonce qu'un correctif hors cycle sera publié le 02/08.

Le principe de la vulnérabilité est simple. Les raccourcis Windows (fichiers .lnk) peuvent pointer sur différents types de ressources. Lorsqu'un utilisateur crée un raccourci pointant

[9] http://cert.lexsi.com/weblog/index.php/2009/02/06/276-noms-de-domaine-de-conficker-downadup-a-et-b
[10] http://www.ivanlef0u.tuxfamily.org/?p=411
[11] http://www.microsoft.com/technet/security/advisory/2286198.mspx

vers un élément du panneau de configuration (fichier bibliothèque CPL), Windows ne va pas ajouter l'icône au fichier LNK, mais seulement une référence au fichier CPL ; l'icône sera dynamiquement chargée et affichée grâce au chargement de ce fichier. Ainsi, si un attaquant crée un fichier LNK de type "panneau de configuration" en précisant comme chemin vers l'élément une DLL malveillante, Windows chargera cette DLL pour tenter de récupérer son icône, exécutant ainsi sa fonction principale et infectant le système.

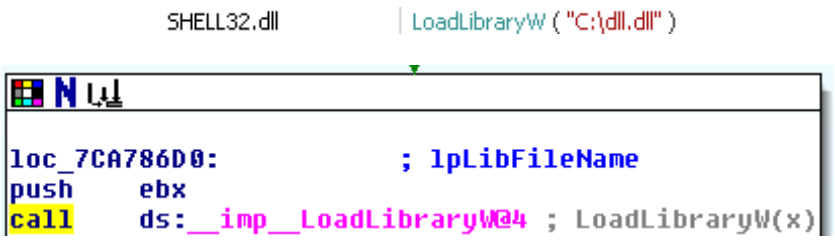
Comme indiqué précédemment, Stuxnet installe deux pilotes noyau dont le but est de camoufler les fichiers .lnk et ~WTR*.tmp en effectuant du filtrage NTFS :

Type	Name	Value
AttachedDevice	\FileSystem\Ntfs \Ntfs	mrxnet.sys (Windows NT NET Minirdr/Microsoft Corp...
AttachedDevice	\FileSystem\Fastfat \Fat	mrxnet.sys (Windows NT NET Minirdr/Microsoft Corp...

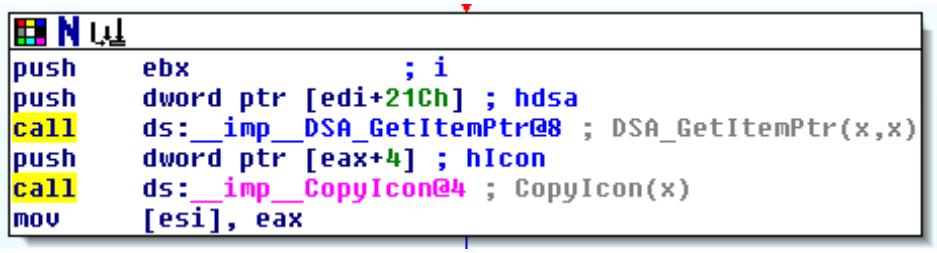
Ainsi, un utilisateur infecté ne verra pas les fichiers malveillants installés par le fichier .lnk spécialement formé. Les fichiers infectés sont copiés dans tous les périphériques de stockage (clés USB, partages réseaux, etc) afin d'augmenter la propagation du code malveillant. Le malware remonte ensuite des informations sur les sites www.mypremierfutbol.com et www.todaysfutbol.com comme les adresses IP, le nom d'hôte, la version de système ou la présence du logiciel Siemens Step 7. Ces sites font également office de C&C.

3.1.2 Analyse de la vulnérabilité et du correctif Microsoft

La vulnérabilité peut être retrouvée en traçant les appels Windows. Lors de l'exploitation de la vulnérabilité, on remarque que la DLL spécifiée dans le fichier LNK est chargée par un appel à **LoadLibrary()** :

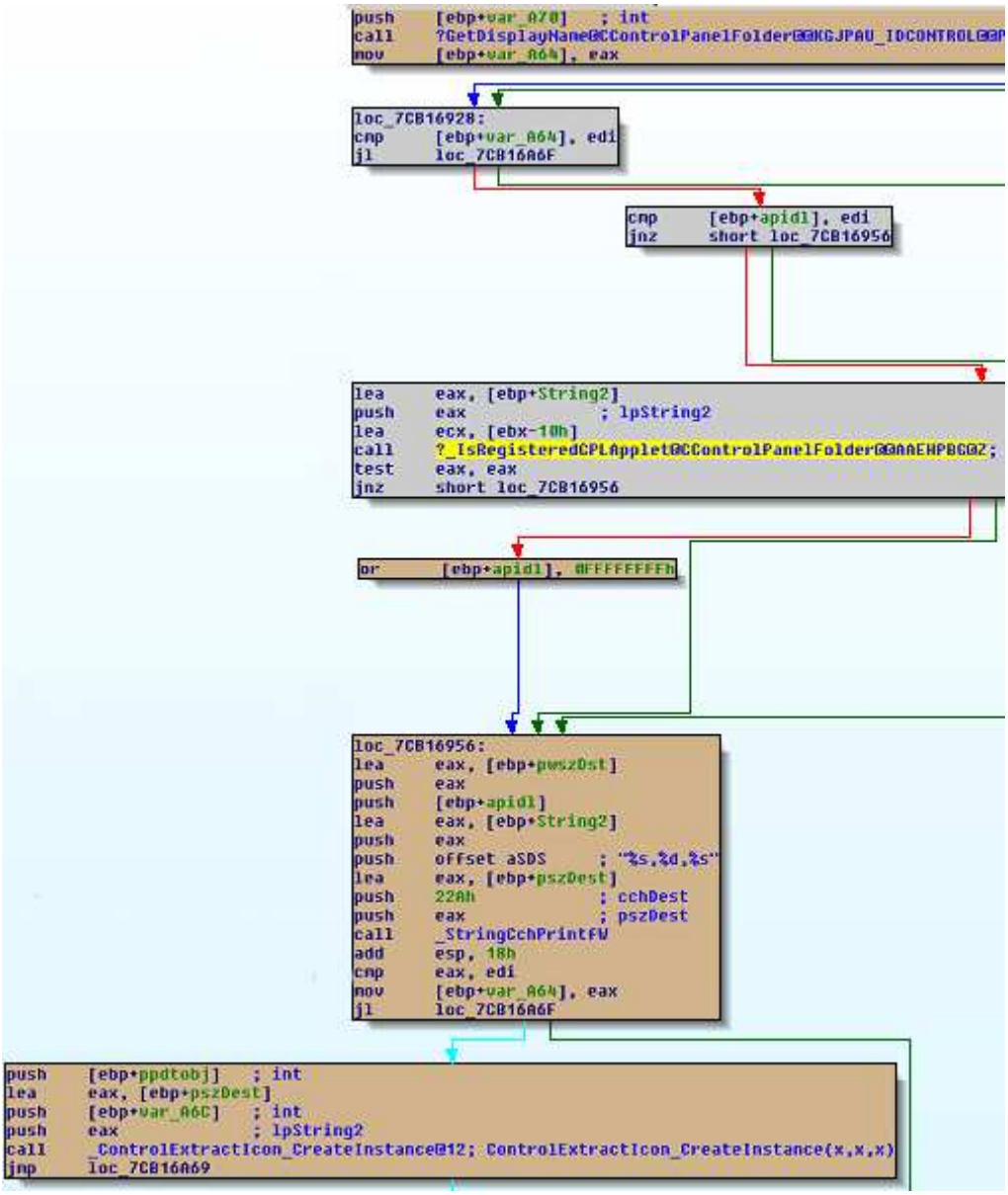


Cet appel est réalisé dans la bibliothèque shell32.dll, à l'adresse **_LoadCPLModule**+0x10d. En remontant dans les appels de fonctions, on tombe successivement dans les fonctions **CPL_LoadCPLModule()**, puis **CPL_LoadAndFindApplet()**, cette dernière étant chargée de récupérer l'icône :



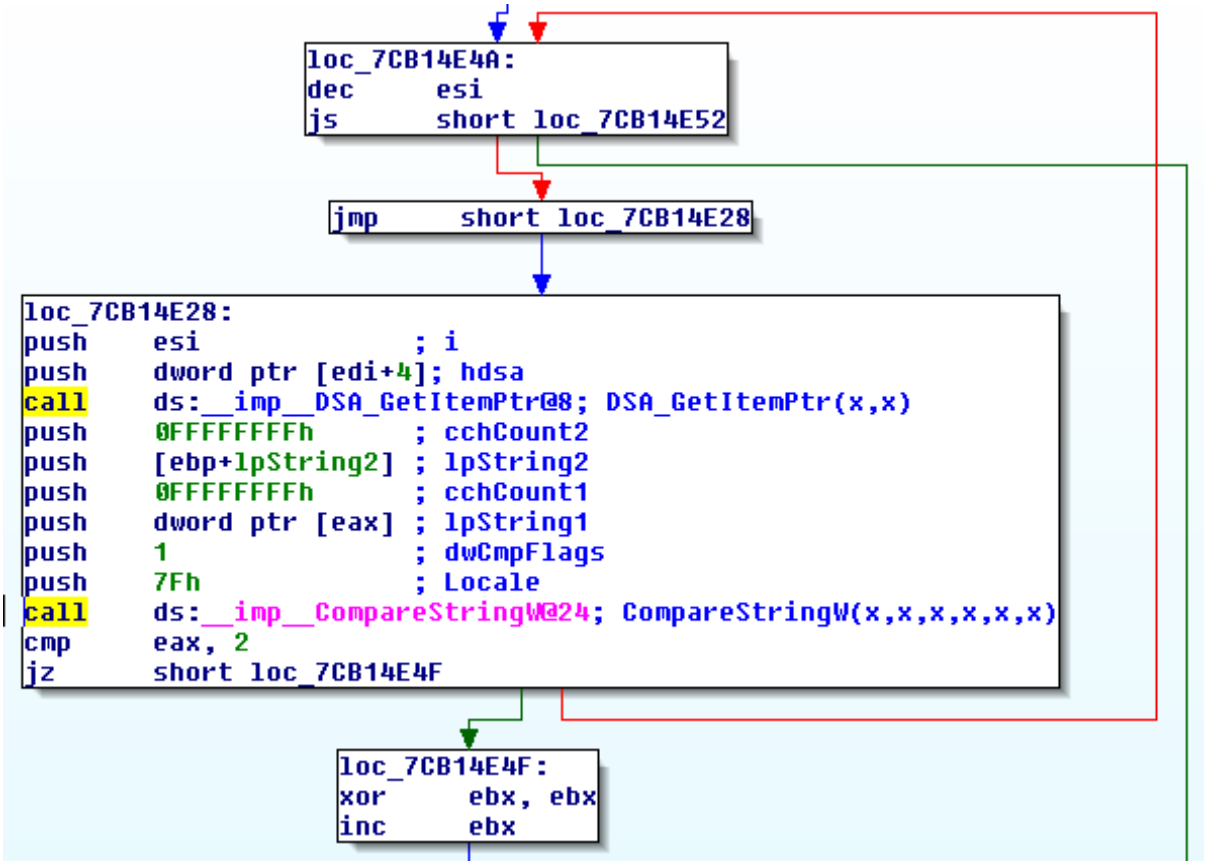
Observons maintenant la façon dont Microsoft l'a corrigée, par analyse différentielle de la bibliothèque shell32.dll pour Windows XP SP3 présent dans le correctif MS10-046 publié le 02/08/2010.

Plusieurs nouvelles fonctions ont été ajoutées à la version corrigée de la DLL ; sachant que la vulnérabilité est liée à la gestion des raccourcis vers des éléments du panneau de configuration (CPL), la nouvelle fonction **CControlPanelFolder::_IsRegisteredCPLApplet()** attire immédiatement notre attention. Or, il se trouve que la fonction **CControlPanelFolder::GetUIObjectOf()** a été modifiée pour se voir ajouter un nouveau bloc appelant cette fonction :



En bas de la capture, on note un appel à la fonction **_ControlExtractIcon_CreateInstance()**, chargée d'extraire l'icône, qui ne sera donc réalisé que si le code de retour de **_IsRegisteredCPLApplet()** est non-nul.

Si l'on regarde de plus près **_IsRegisteredCPLApplet()**, on observe qu'après avoir récupéré la listes des éléments du panneau de configuration enregistrés grâce à **CPLD_GetModules()**, la fonction itère sur ces éléments grâce à **DSA_GetItemPtr()** jusqu'à ce qu'une correspondance avec la DLL pointée par le raccourci soit trouvée par **CompareString()** (valeur de retour 2, soit CSTR_EQUAL, auquel cas la fonction **_IsRegisteredCPLApplet()** retourne 1), ou qu'il n'y ait plus d'éléments avec qui comparer (auquel cas elle retourne 0) :



Si l'on crée par exemple un raccourci CPL pointant vers C:\Windows\system32\zuaucpl.dll (au lieu du légitime wuaucpl.dll), on remarque bien que Windows compare le nom de notre DLL malveillante à la liste des éléments du panneau de configuration enregistrées :

```
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\Program Files\Fichiers communs\Microsoft Shared\Speech\sapi.cpl", -1, "C:\WINDO
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\wuaucpl.cpl", -1, "C:\WINDOWS\system32\wuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\Program Files\Fichiers communs\Microsoft Shared\Speech\sapi.cpl", -1, "C:\WINDO
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\wuaucpl.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\wscui.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\TweakUI.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\timedate.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\telephon.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\sysdm.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\powercfg.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\nwc.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\nusrmgr.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\netsetup.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\mmsys.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\main.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\joy.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\javacpl.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\inprops.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\intl.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\inetcpl.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\hdwwiz.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\firewall.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\desk.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\bthprops.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\appwiz.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
SHELL32.dll  CompareStringW ( 127, NORM_IGNORECASE, "C:\WINDOWS\system32\access.cpl", -1, "C:\WINDOWS\system32\zuaucpl.cpl", -1 )
```

Windows n'autorisera ainsi que les CPL légitimement enregistrés[12] à être chargés lors de la récupération de l'icône.

Cette mise à jour ajoute également le support de la valeur de registre **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers\IsAutorunForCDROMOnly** (sans pour autant la créer par défaut), permettant de désactiver l'AutoRun sur tous les supports à l'exception des CD et des DVD. Cette désactivation est le cas par défaut à partir de Windows 7[13] et Microsoft proposait jusqu'à présent le KB971029[14] pour l'appliquer aux versions antérieures de Windows.

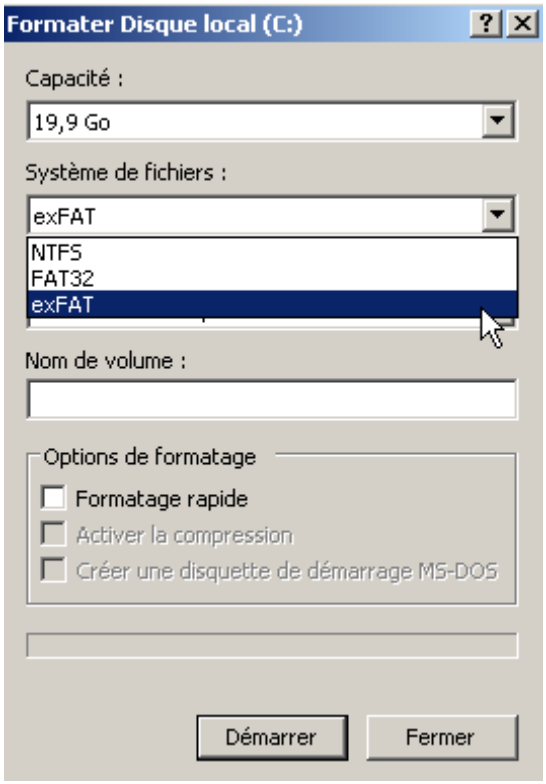
On trouve en effet un appel à une nouvelle fonction **_IsAutorunForCDROMOnly()** en tête des fonctions **CMountPoint::_ProcessAutoRunFile()** et **CContentTypeData::Init()** :

En bas de la fonction **CContentTypeData::Init()**, un nouveau test a été ajouté afin d'appeler ou non **AddRemovableOrFixedDiskAutorunINFHandler()**, en fonction du retour de **_IsAutorunForCDROMOnly()** (dans le cas de **CMountPoint::_ProcessAutoRunFile(),** il y a plusieurs vérifications au fil du code) :

La fonction **_IsAutorunForCDROMOnly()** récupère simplement la valeur depuis le registre :

Plus curieux, cette mise à jour modifie plusieurs fonctions (**InitializeFormatDlg()**, **BeginFormat()** et **FileSysChange()**) pour ajouter "exFAT" à la boîte de dialogue du formatage de disque :

[12] http://msdn.microsoft.com/en-us/library/cc144195(VS.85).aspx
[13] http://blogs.technet.com/b/srd/archive/2009/04/28/autorun-changes-in-windows-7.aspx
[14] http://support.microsoft.com/kb/971029



Problème : seule la boîte de dialogue a été modifiée ; les pilotes exFAT ne sont pas présents et le formatage ne sera donc pas possible en l'état... Le support de exFAT nécessite l'application d'une mise à jour distincte sous la forme du KB955704[15] qui comprend d'autres fichiers que shell32.dll.

En plus du correctif, cette nouvelle version de shell32.dll comprend donc deux mises à jour fonctionnelles (support pour la valeur permettant la désactivation complète de l'AutoRun hors CD et DVD, ainsi que support partiel du formatage exFAT), ce qui n'est, à notre connaissance, documenté nulle part (en dehors du fait que des mises à jour de shell32.dll ont été effectuées dans des KB publiés précédemment).

3.1.3 Exploitation par d'autres malwares

Suite à la médiatisation de l'affaire Stuxnet, d'autres malwares ont exploité la vulnérabilité LNK afin d'améliorer leur propagation :

- Dulkis/Vobfus, ver écrit en Visual Basic. Connu depuis 2009, il a été nommé par Microsoft selon le schéma **V**(isual Basic) + **obfus**cated[16] ;

[15] http://support.microsoft.com/kb/955704
[16] http://blogs.technet.com/b/mmpc/archive/2010/07/23/protection-for-new-malware-families-using-lnk-vulnerability.aspx

- Downloader.CJX qui exploite à la fois l'Autorun exactement à la manière de Conficker et cette vulnérabilité 0-day ;
- Chymine, un nouveau keylogger découvert par ESET[17]. Il est intéressant de noter que le code d'exploitation utilisé pour installer ce malware se connecte à un partage de fichiers SMB sur Internet, alors que Stuxnet copie les fichiers directement sur la clé USB ; cependant, il ne cherche plus à se propager une fois installé, ce qui en fait un cheval de Troie et non un ver ;
- Zeus/ZBot, le cheval de Troie bancaire bien connu. Cette variante s'est propagée par courriel semblant provenir de Security@microsoft.com, avec un fichier ZIP protégé par mot de passe en pièce jointe que l'utilisateur devait décompresser dans C:\[18] ;
- Sality, un infecteur de fichiers ayant fait parler de lui début 2010[19] ; un article dans MISC 48 lui a même été consacré.

Symantec[20] indique que la vulnérabilité LNK était déjà exploitée par le malware Zlob en novembre 2008, sans que cela n'ait été remarqué à l'époque.

A noter que les malwares n'ont pas tous exactement la même façon d'exploiter la vulnérabilité. Downloader.CJX l'exploite le plus simplement, en créant sur la clé USB infectée des fichiers LNK intégrant un chemin "en dur" vers une DLL malveillante préalablement déposée sur la clé. Comme le malware ne peut pas savoir à l'avance sous quel lecteur la clé sera montée sur les autres PC, il crée des raccourcis pour les lettres de lecteur allant de D: à L: :

```
sh-4.0$ strings -e l *.lnk|sort -u
 :D:\zzz.dl
 :E:\zzz.dl
 :F:\zzz.dl
 :G:\zzz.dl
 :H:\zzz.dl
 :I:\zzz.dl
 :J:\zzz.dl
 :K:\zzz.dl
 :L:\zzz.dl
```

La variante originale de Stuxnet utilise plusieurs raccourcis (pour fonctionner sur différentes versions de Windows) contenant chacun un chemin UNC pointant directement sur le périphérique USB, de type \\.\STORAGE#RemovableMedia#<id> et \\.\STORAGE#Volume#<id>, ce qui permet de s'affranchir de ce problème de lettre du lecteur.

[17] http://blog.eset.com/2010/07/22/new-malicious-lnks-here-we-go
[18] http://www.f-secure.com/weblog/archives/00001996.html
[19] https://cert.lexsi.com/weblog/index.php/fr/2010/03
[20] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

3.1.4 Outils et solutions de contournement

Dans son bulletin, Microsoft donne les solutions de contournement suivantes :

- Désactiver les icônes de tous les raccourcis, en supprimant ou renommant les clés **HKCR\lnkfile\shellex\IconHandler** (fichiers .lnk) et **HKCR\piffile\shellex\ IconHandler** (fichiers .pif). Cela bloque parfaitement toute exploitation de la vulnérabilité mais désactive l'affichage des icônes de tous les raccourcis, ce qui est difficilement déployable en entreprise. Malgré le Fix It publié par Microsoft[21], cette solution n'a sans doute pas eu beaucoup de succès en pratique ;
- Désactiver le client WebDAV (service WebClient activé par défaut). Cette solution bloque l'un des vecteurs d'exploitation : les partages WebDAV (HTTP ou HTTPS). Cette solution, bien qu'incomplète, ne s'est pas révélée inutile puisque ce vecteur a été utilisé par le code d'exploitation ajouté au framework Metasploit le 19/07 ; si on part du principe qu'un poste de travail en entreprise n'a pas accès à d'autres ports TCP que 80 et 443, elle bloque donc l'exploitation depuis Internet.

Les éditeurs antivirus ont été assez rapides à implémenter des signatures pour les codes d'exploitation et les malwares associés. Au 19/07, la détection par les antivirus de la Plateforme d'Analyse Antivirale du Cert-Lexsi[22] était la suivante :

Antivirus	Signature
Antivir	TR/Drop.Stuxnet.D
Avast	Win32:Trojan-gen
Bit Defender	Win32.Worm.Stuxnet.A
ClamAV	Trojan.Stuxnet
DrWeb	Trojan.Stuxnet.1
eTrust Antivirus	Win32/Stuxnet.A
F-Prot	NOT FOUND
F-Secure Anti-Virus	Trojan-Dropper:W32/Stuxnet.A Trojan-Dropper.Win32.Stuxnet.d
Ikarus	Trojan-Dropper.Win32.Stuxnet
Kaspersky Anti-Virus	Trojan-Dropper.Win32.Stuxnet.d
McAfee VirusScan	Stuxnet
Nod32	NOT FOUND
Norman Virus Control	NOT FOUND
Panda Anti-Virus	NOT FOUND
Sophos	Troj/Stuxnet-A
Symantec Command Line Scanner	W32.Temphid
Trend Micro VScan	TROJ_STUXNET.A
VBScan	Trojan.DR.Stuxnet.C
VirusBlokAda	Trojan-Spy.0485

[21] http://go.microsoft.com/?linkid=9738980
[22] https://www.lexsi.com/abonnes/p2a.php

Les solutions de contournement n'étant donc pas pleinement satisfaisantes, il y a fort à parier que la plupart des entreprises se sont contentées de ces détections et de celles des fichiers LNK malveillants, en attendant anxieusement le correctif officiel.

Par la suite, des solutions de contournements basées sur les fonctionnalités SRP (Règles de restriction logicielle) ou AppLocker (Windows 7 uniquement), permettant toutes deux de bloquer l'exécution de binaires non-sûrs, ont été décrites[23]. Leur efficacité ne fait pas de doute, mais on se heurte là aussi à des problématiques de déploiement, la plupart des entreprises préférant attendre le correctif officiel plutôt que de mettre en péril la production avec des solutions peu communes.

A noter que la désactivation de l'Autorun n'a jamais été une solution de contournement fiable ; elle permet cependant de nécessiter plus d'interaction utilisateur lors de l'insertion d'une clé USB.

Deux sociétés tierces, Sophos et G-Data, ont également publié des outils permettant de se protéger contre cette vulnérabilité en attendant le correctif officiel. Les deux outils fonctionnent sur le même principe : une DLL est injectée dans le processus explorer.exe (respectivement SophosLinkIconHandler32.dll pour Sophos et LnkCheck.dll pour G-Data) afin de surcharger les fonctions liées à l'affichage des icônes de raccourcis. Lorsqu'un raccourci malveillant est détecté, Sophos affiche un message d'erreur, alors que G-Data se contente d'afficher une icône en forme de raccourci. Ces outils n'ont pour but que de bloquer l'exécution automatique du code malveillant référencé par le raccourci ; si l'utilisateur décide de lui-même de lancer le malware, ils sont bien sûrs inefficaces et l'antivirus prend alors le relais.

L'outil de G-Data offre une protection efficace (les premières versions considéraient tout raccourci de type CPL comme malveillant, mais cela a été corrigé par la suite). En revanche, comme l'a mentionné H-Online[24], l'outil de Sophos considère comme inoffensif tout raccourci présent sur le disque C: ou tout raccourci dont la cible est déjà présente sur un disque local ; sa protection peut donc par exemple être contournée en incitant l'utilisateur à extraire une archive malveillante, comme l'a fait le malware Zeus.

Le 10/08, Microsoft a publié une mise à jour de l'Outil de suppression des logiciels malveillants (MSRT) qui détecte et supprime Stuxnet ainsi que les nouvelles variantes de Vobfus et Sality exploitant la vulnérabilité LNK.

3.2 Vulnérabilité dans le service Serveur (MS08-067, Ref. Lexsi 10828)

En plus de la fameuse vulnérabilité LNK présentée ci-dessus, Stuxnet exploite d'autres vulnérabilités. La première est la déjà connue MS08-067 exploitée entre autres par les malwares Gimmiv, Neeris, Arpoc, Wecorl et surtout

[23] https://cert.lexsi.com/weblog/index.php/2010/07/20/388-0-day-lnk-applocker-a-la-rescousse
[24] http://www.h-online.com/security/news/item/Anti-virus-vendors-offer-free-LNK-protection-Update-1046183.html

Conficker/Downadup[25]. Il s'agit d'une vulnérabilité de type débordement de tampon dans la pile, au niveau de la fonction **NetPathCanonicalize()** du service Serveur de Windows, permettant à un attaquant distant non authentifié (sauf sur Windows 2008 et Vista ou une authentification est nécessaire par défaut, à moins que la protection par mot de passe n'ait été explicitement désactivée) d'exécuter du code arbitraire avec les droits SYSTEM. L'exploitation de la vulnérabilité nécessite que le partage de fichiers et d'imprimante soit activé, mais ce sera généralement toujours le cas en entreprise.

Le correctif Microsoft est disponible depuis le 23/10/2008.

3.3 Vulnérabilité dans le spouleur (MS10-061, Ref. Lexsi 13972)

La troisième vulnérabilité exploitée par Stuxnet concerne le service Print Spooler de Windows qui ne vérifie pas suffisamment les permissions utilisateur lors de certaines requêtes RPC, permettant à un attaquant distant de créer des fichiers dans l'arborescence système si une imprimante est partagée, et donc d'exécuter du code avec des privilèges élevés (voir ci-dessous pour la méthode). Sur Windows XP, l'activation par défaut du compte Invité a pour conséquence que cette vulnérabilité peut être exploitée sans authentification. Microsoft a publié le correctif MS10-061 le 14/09/2010.

Contrairement à ce qui a pu être écrit sur certains sites, cette 0-day n'a pas été découverte avec Stuxnet car elle avait déjà été décrite dans le magasine hackin9 d'avril 2009[26].

A première vue, l'exploitation de cette vulnérabilité ne permet « que » de déposer un fichier arbitraire dans l'arborescence système. Comment donc l'exploiter afin d'exécuter du code arbitraire ? La solution passe par les fichiers MOF (Managed Object Format) qui peuvent inclure du VBScript ; Windows surveille le répertoire C:\Windows\system32\wbem\mof et tout fichier MOF qui y est déposé est automatiquement compilé et il sera possible de l'exécuter avec les privilèges SYSTEM[27] (plus de détails sont disponibles dans l'article Exploit Corner de MISC 53).

3.4 Vulnérabilités locales (MS10-073 et MS10-092, Ref. Lexsi 13974)

Deux autres 0-days sont exploitées par Stxunet, permettant à un attaquant local d'élever ses privilèges :

- Vulnérabilité liée au traitement d'un fichier "keyboard layout" spécialement formé (Windows 2000/XP/2003 seulement) ;

[25] http://cert.lexsi.com/weblog/index.php/2009/01/12/274-le-ver-conflicker-fait-des-ravages
[26] http://newsoft-tech.blogspot.com/2010/09/ms10-061-this-is-not-0day-you-are.html
[27] http://expertmiami.blogspot.com/2010/09/cyber-guerre-42e-edition-et-fichiers.html

- Vulnérabilité dans le planificateur de tâches (Windows Vista/2008 et 7/2008 R2 seulement).

Microsoft a publié le correctif MS10-073 pour la première vulnérabilité le 12/10 ; la seconde n'a été corrigée que le 14/12 par le correctif MS10-092.

Un code d'exploitation public est disponible dans le framework Metasploit pour la vulnérabilité affectant le planificateur de tâches depuis le 21/11.

4 Résumé des fonctionnalités du malware

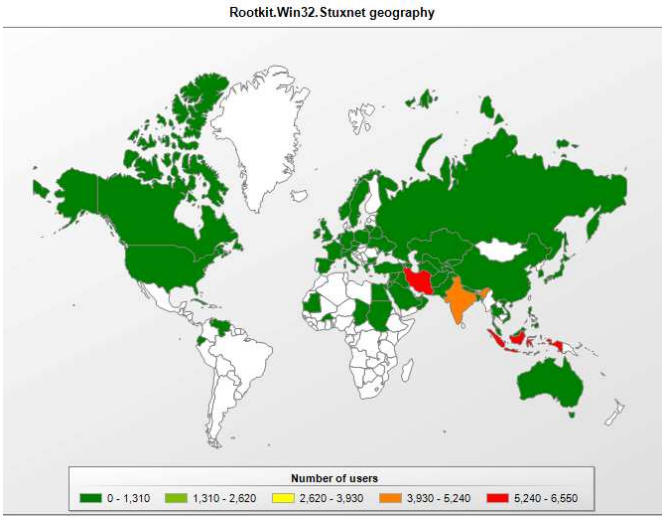
4.1 Fonctionnalités courantes

En plus de l'exploitation des vulnérabilités présentées dans la section 3, Stuxnet dispose des fonctionnalités suivantes, que l'on retrouve dans d'autres malwares :

- Connexion à des serveurs de contrôle afin de recevoir des mises à jour et envoyer des informations sur le système infecté ;
- Mise à jour sur le réseau local via un mécanisme de peer-to-peer ;
- Recopie dans tous les périphériques de stockage (clés USB, partages réseaux, etc) ;
- Propagation via les partages administratifs et exécution via une tâche planifiée (comme Conficker) ;
- Utilisation d'une rootkit noyau pour cacher ses fichiers malveillants ;
- Contournement des logiciels de sécurité, par exemple en appelant LoadLibrary() sur un fichier inexistant en ayant préalablement hooké Ntdll.dll pour effectivement charger une bibliothèque.

4.2 Attaques contre les systèmes SCADA

La première variante de Stuxnet s'est rapidement répandue en Iran (60% des infections), Indonésie et Inde, comme le montre la carte suivante[28] :

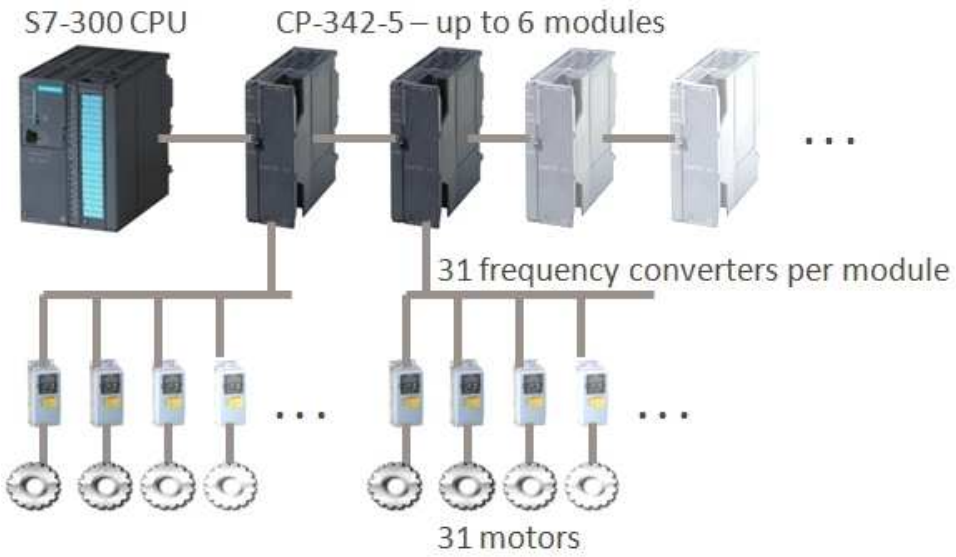


Source de l'image : Kaspersky

[28] http://www.securelist.com/en/blog/272/Myrtus_and_Guava_Episode_3

Selon Symantec, 100 000 machines auraient été infectées à la date du 29/09.

La spécificité de Stuxnet par rapport aux autres malwares connus est qu'il cible les systèmes SCADA (Supervisory Control And Data Acquisition) Siemens utilisés pour les infrastructures critiques comme les centrales énergétiques ou les transports. Symantec a pu déterminer que **le but du malware est de reprogrammer les PLC (Programmable Logic Controller) contrôlant certaines parties des systèmes industriels.** Pour cela, Stxunet remplace la bibliothèque s7otbxdx.dll du logiciel Siemens SIMATIC Step 7 (servant à programmer les PLC Simens) du poste Windows connecté au PLC et se place ainsi entre ce logiciel et le PLC, lui permettant de modifier les blocs de code à la volée sans que ces modifications ne soient visibles sur l'interface utilisateur. **Stuxnet agit donc comme une rootkit PLC** (la première du genre). La charge utile de Stuxnet est de reprogrammer les PLC des convertisseurs de fréquence fabriqués par les sociétés Fararo Paya (Iran) et Vacon (Finlande) seulement s'ils opèrent à une fréquence comprise entre 807 et 1210 Hz (ciblant ainsi précisément certains équipements non déterminés pour l'instant), **afin de faire tourner des moteurs alternativement très au-dessus ou très en-dessous de leur valeur nominale, dans un but de sabotage industriel** probablement contre l'Iran.



Source de l'image : Symantec

Symantec indique que des convertisseurs de ce type sont contrôlés à l'exportation aux Etats-Unis car ils peuvent par exemple être utilisés pour construire des centrifugeuses pour l'enrichissement d'uranium. Le 29/11, le président iranien a confirmé que plusieurs centrifugeuses de l'usine d'enrichissement d'uranium située à Natanz (centre de l'Iran) ont été "mises hors service par des logiciels installés sur les pièces électroniques"[29]. Outre l'Iran, il semble que la Corée du Nord utilise ce type de produits[30].

[29] http://www.lemonde.fr/technologies/article/2010/11/29/iran-plusieurs-centrifugeuses-affectees-par-un-virus-informatique_1446546_651865.html
[30] http://www.wired.com/dangerroom/2010/11/could-stuxnet-mess-with-north-koreas-new-uranium-plant/

Ces systèmes utilisent également une base de données WinCC dont les identifiants par défaut sont connus et ont été publiés sur certains forums dès 2008[31] ; Stuxnet utilise ces identifiants afin d'exécuter du code SQL afin de lancer des commandes permettant d'infecter le système. Suite à la découverte du malware Stuxnet, Siemens a publié un document officiel afin d'informer ses clients sur le problème[32] mais ne préconise pas le changement du mot de passe car cela pourrait empêcher ces systèmes de fonctionner correctement[33]....

De plus, Stuxnet infecte les projets Step 7 afin d'automatiser l'exécution du malware lors de l'ouverture du projet (fichiers .s7p).

Des informations techniques détaillées sur la rootkit PLC peuvent être trouvées dans le dossier Symantec concernant Stuxnet[34] (« Modifying PLCs », page 32). ESET a également publié un document sur Stuxnet[35].

[31] http://www.net-security.org/malware_news.php?id=1408

[32] http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&objid=43876783&caller=view

[33] http://www.pcworld.com/businesscenter/article/201442/after_worm_siemens_says_dont_change_passwords.html

[34] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[35] http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

5 Conclusion

De nombreux observateurs s'accordent sur le fait que l'attaque dont Stuxnet est l'outil central est de très haut niveau et que celui-ci a probablement été développé par un état.

Le malware Stuxnet aura été remarquable pour plusieurs raisons :

- Il exploite cinq vulnérabilités dont quatre 0-days (dont une déjà connue) ;
- Il utilise des pilotes noyaux signés avec un certificat volé ;
- Il cible des infrastructures SCADA très précises utilisées pour les systèmes critiques comme les usines, l'énergie ou les transports, dans un but de sabotage industriel.