

Dans le cadre de

SECURIDAY 2010

Et sous le thème de

Computer Forensics Investigation



VOUS PRÉSENTE L'ATELIER :

Analyse des Malwares

Chef Atelier : **Hamdi Tbourbi (RT4)**

- Asma DHAYA (RT5)
- Salmen HITANA (RT4)
- Malek DRIDI (RT3)



1) Introduction :

Les malwares sont des programmes malveillants qui sont développés dans le but de nuire à un système informatique.

Le terme malware est donc un terme générique qui définit différentes catégories de logiciels malveillants :

❖ **Les virus :**

Un virus est un bout de programme qui s'attache à un programme légitime ou à un exécutable pour exécuter une fonction spécifique sur l'ordinateur cible et affecter son fonctionnement. Ils peuvent se répandre à travers Internet, les CD, les clés USB...

❖ **Les vers (worm) :**

Ce sont des programmes qui exploitent une vulnérabilité sur l'hôte cible pour s'installer. Contrairement au virus, le ver est autonome et peut s'installer sans se rattacher à un autre programme. Une fois installé, il se réplique sur d'autres hôtes en se propageant via le réseau. Le ver exécute des activités malveillantes tel que la dégradation des performances réseau et les dénis de service (DOS).

❖ **Les trojan (chevaux de Troie) :**

Le trojan est un programme innocent en apparence dissimilé dans un programme saint ou porté par un virus ou un vers, il exploite les privilèges de l'utilisateur qui l'exécute pour ouvrir des portes dérobées, causer des dommages, etc...

❖ **Les exploits :**

Ils permettent d'exploiter une faille de sécurité d'un [système d'exploitation](#) ou d'un [logiciel](#) dans le but, de prendre le [contrôle à distance](#) de la machine ciblée ou d'y installer des malware.

❖ **[rootkits](#) :**

C'est un ensemble de programmes qui sont chargés de dissimuler l'activité nuisible du malware.



❖ Les keyloggers :

Ce malware permettent d'enregistrer toutes les touches que la victime presse au clavier et peut donc obtenir mots de passe, conversations en ligne voire même des numéros de carte bancaires, et puis le les renvoyer au pirate.

❖ Les portes dérobées (backdoor) :

Une porte dérobée est un moyen qui permet l'accès distant à un ordinateur cible ,pour exécuter des actions nuisibles prévues par ce programme.

❖ Les composeurs (dialers) :

Ces programmes prennent le contrôle du modem téléphonique et établit une nouvelle connexion à Internet en composant un numéro de téléphone surfacturé. Les composeurs sont inopérants sur les une connexion haut débit (ADSL...).

Différents types de «Sandbox»:

On peut réaliser tout seul un environnement d'analyse dynamique de malwares(SANDBOX) dans une machine virtuelle isolée des réseaux mais on risque toujours d'être contaminé soit par des malwares intelligents soit en faisant des manipulations risquées. Une des solutions qui s'offre à nous est d'utiliser des "Sandbox Online...

Machine virtuelle :

VMware Workstation ACE Edition 6.0.2

Dans nos tests on a choisi de travailler sur des machines virtuelles pour les raisons suivantes :

- Sécurité : les machines virtuelles peuvent être connectées par un réseau virtuel totalement indépendant de tout réseau opérationnel, sans risque d'infecter d'autres machines.
- Rapidité et efficacité : une machine virtuelle peut être stoppée, restaurée et redémarrée en quelques secondes.
- Les machines virtuelles peuvent être facilement copiées, dupliquées et modifiées pour constituer une bibliothèque de toutes les versions d'un système d'exploitation ou d'une application.



Sandboxes en ligne :

CWSandbox :

flexible, évolutif, système entièrement automatisé pour la surveillance et les rapports sur le comportement des échantillons suspects. CWSandbox est un outil d'analyse malware grande, surtout pour les "première vue" analyse.

Submit a file to Sunbelt's CWSandbox on-line malware analyzer

Enter your email address and click "Browse" to find the file you want to analyze.
To submit the sample, click "Submit sample for analysis".
Within a short time, the analysis of the file you submitted will be sent to your email.

HTML Results Text Results

Your email address:

File to upload: (< 12288 KB) Aucun fichier choisi

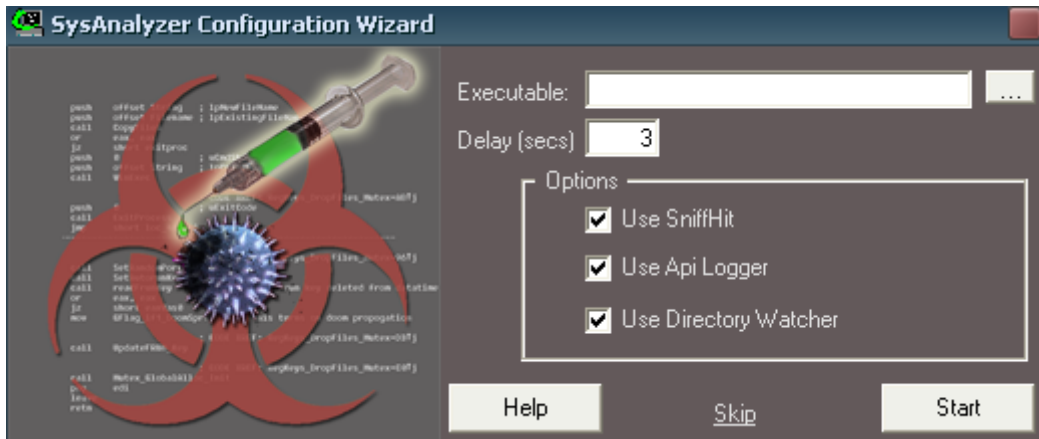
Comment: < 255 chars



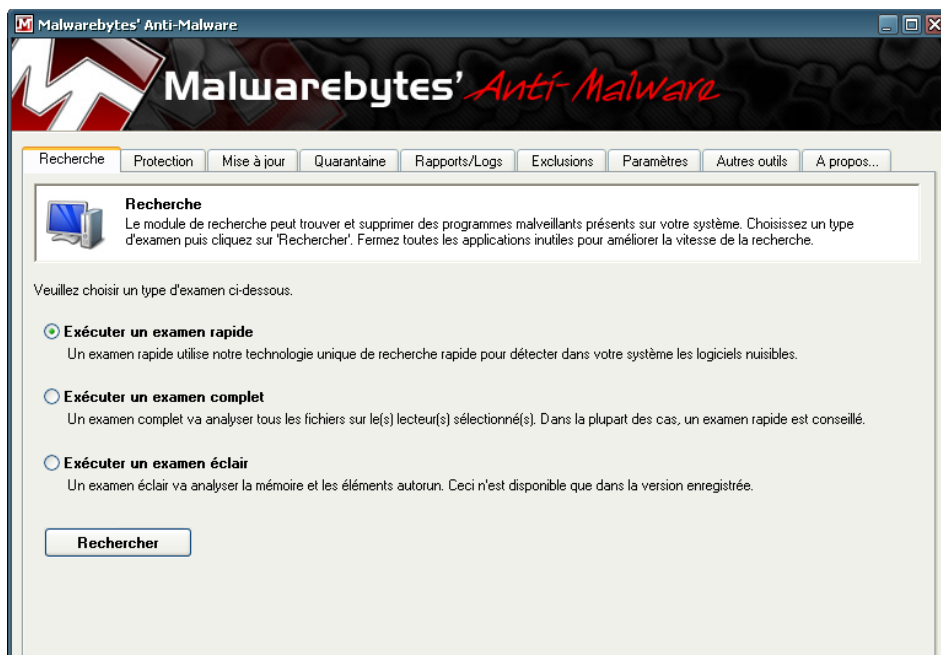
Visit the Sunbelt CWSandbox product page for more info on our malware analysis tools.

virusTotal :

Virustotal est un **service qui analyse les fichiers suspects** et facilite la détection rapide des virus, vers, chevaux de Troie et toutes sortes de malwares détectés par les moteurs antivirus.



1.2 MalwareBytes Anti-Malware:



MalwareByte's Anti-Malware permet de supprimer tous les malwares (Trojan, Backdoor, Spyware, Rogue etc..). Il est simple d'utilisation et efficace.

La version freeware de MalwareByte's Anti-Malware ne possède pas de gardien pour protéger des intrusions, elle permet de scanner et supprimer les infections.



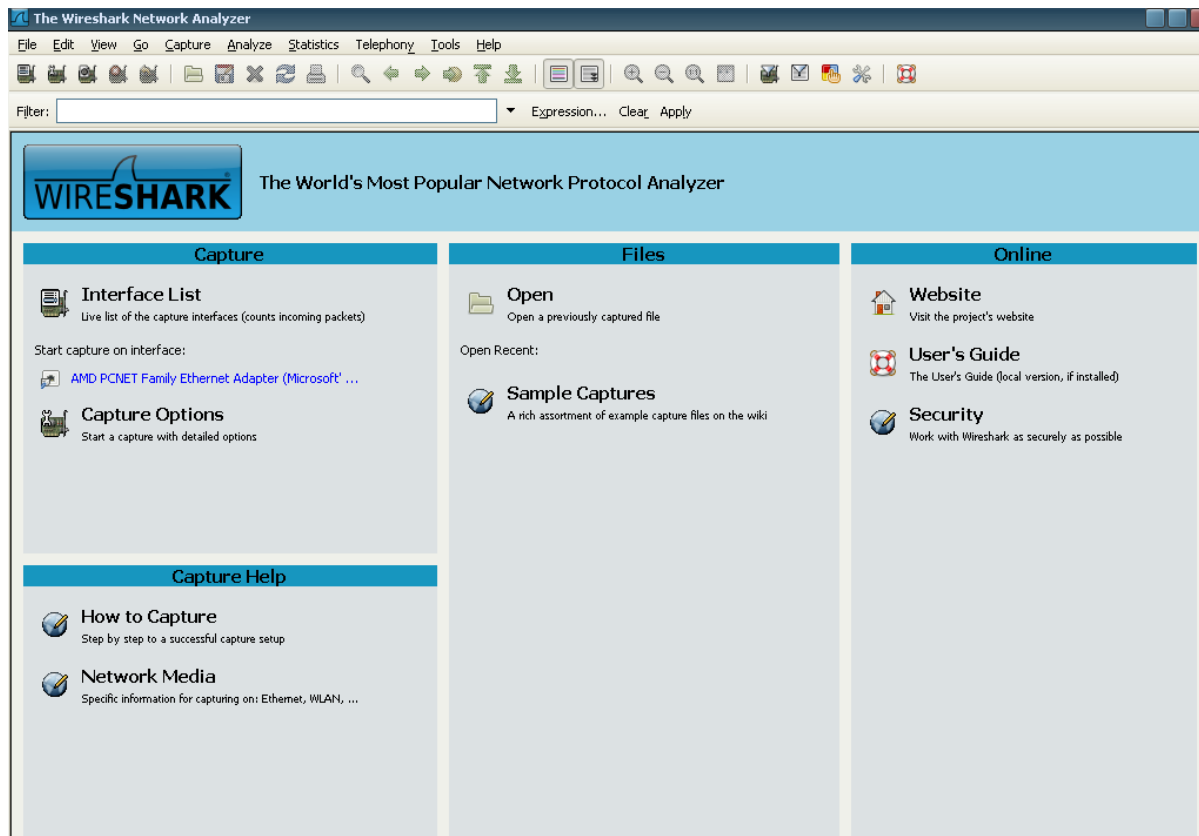
1.3 Wireshark:

Wireshark est l'analyseur réseau le plus populaire du monde. Cet outil extrêmement puissant fournit des informations sur des protocoles réseaux et applicatifs à partir de données capturées sur un réseau.

Comme un grand nombre de programmes, Wireshark utilise la librairie réseau pcap pour capturer les paquets.

La force de Wireshark vient de:

- sa facilité d'installation.
- sa simplicité d'utilisation de son interface graphique.
- son très grand nombre de fonctionnalités.

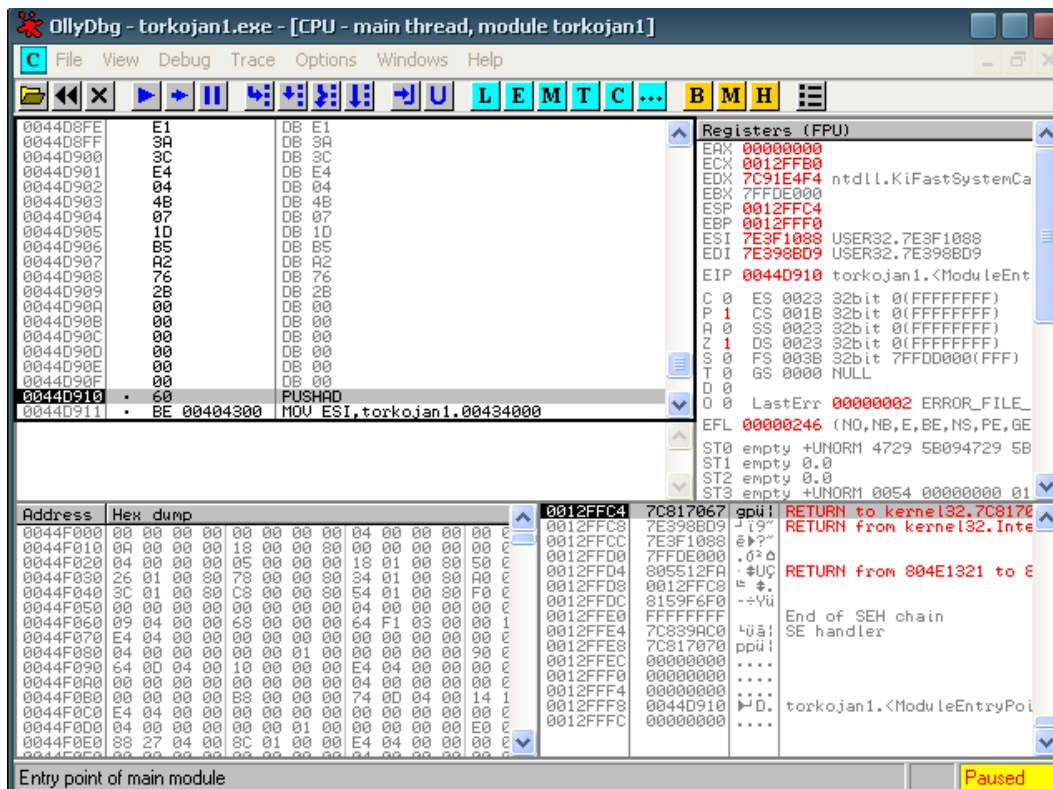




2.2-Analyses statique(binaire) :

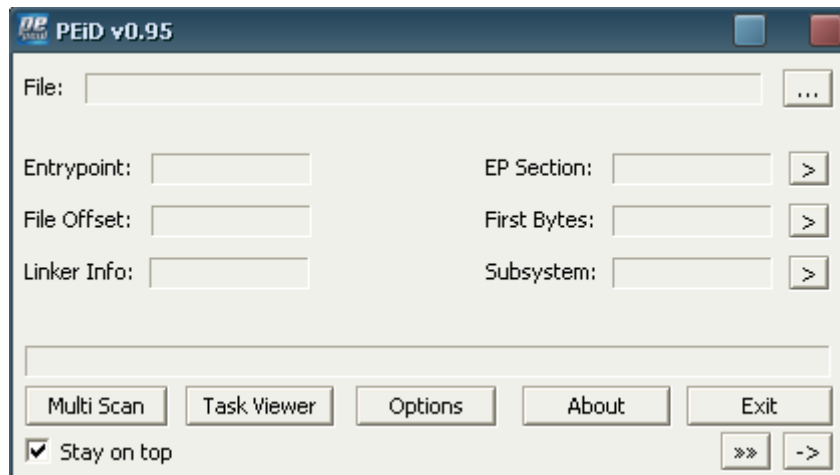
1.1 OllyDbg:

OllyDbg est un niveau assembleur 32-bit analyse débogueur pour Microsoft Windows. L'accent mis sur l'analyse de code binaire, il est particulièrement utile dans les cas où la source n'est pas disponible. Il prévoit le contenu des registres, reconnaît les procédures, les appels de l'API, les commutateurs, les tables, les constantes et les cordes, localise routines à partir des fichiers objet et des bibliothèques, permet des étiquettes et des commentaires dans le code désassemblé, écrit correctifs à fichier exécutable et plus.





1.2 PEiD:



3) Malwares :

3.1-Collecte des malwares :

*Honeypote

Un honeypot (en français pot de miel) est un [ordinateur](#) ou un [programme](#) volontairement vulnérable destiné à attirer et à piéger les [pirates informatiques](#).

Un honeypot permet d'émuler des services sur une machine afin de simuler le véritable fonctionnement d'une machine de production. Ce système assure ainsi la surveillance du réseau par la collecte et le traitement des informations.

SECURINETS



Club de la sécurité informatique
INSAT

SURF **IDS** **INTRUSION DETECTION SYSTEM**

Thursday 15 Apr 2010 01:37

Contact Logout About Manual

Login

Username:

Password:

Username: testuser
Password: testuser

Login

SURFids version: 3.00 | <http://ids.surfnet.nl> SURFids Demo Environment

3.2-Création des malwares

*Turkojan v4.0



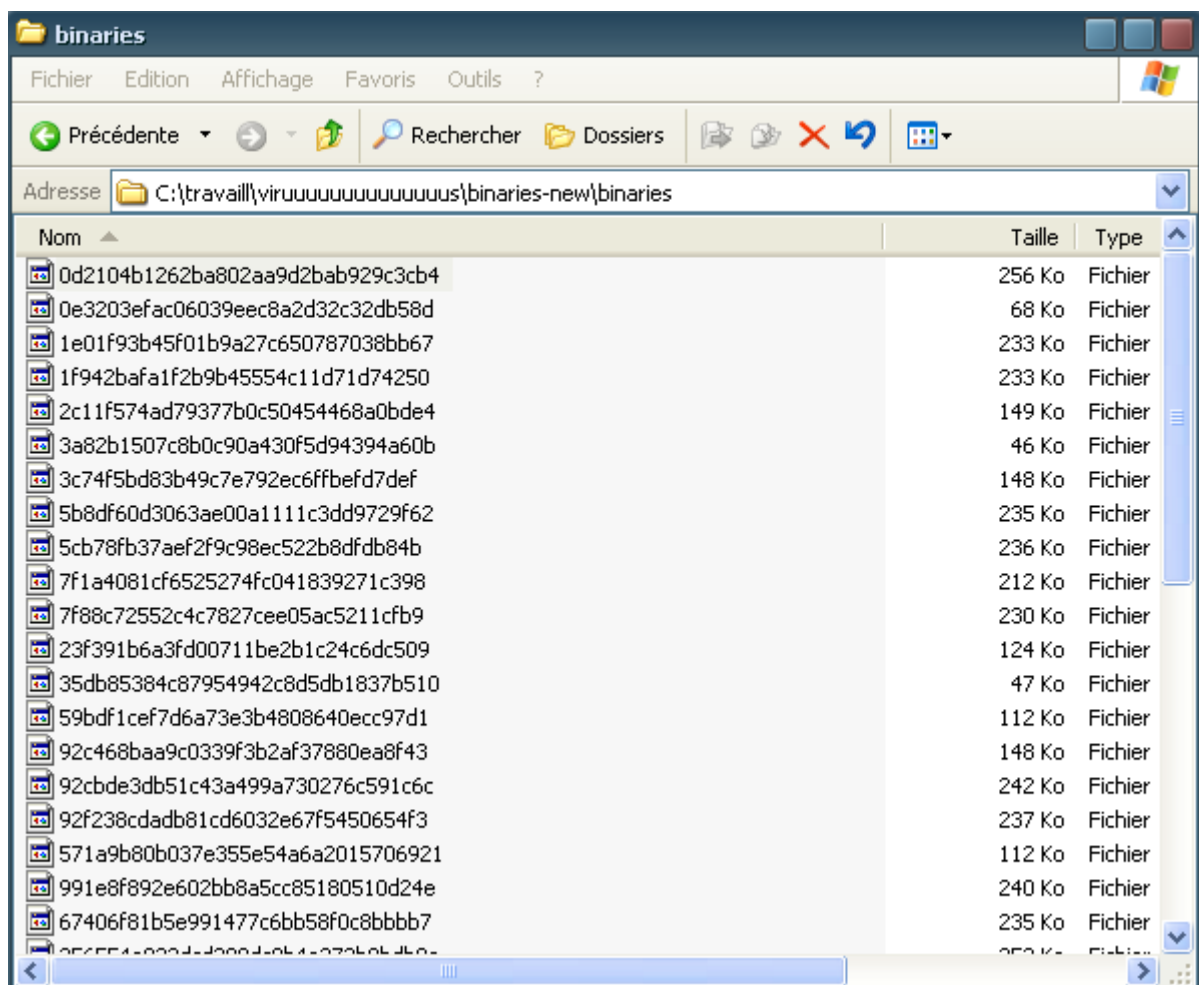
Ce logiciel espion est une plaie. D'abord parce qu'il peut se diffuser vite et bien. Son "ogive" tactique : un serveur caché dans la machine d'une personne piégée, qui ne dépasse pas les 100 kilos. Ensuite, il peut : Voler la connexion, regarder par la webcam, écouter via un micro branché, exploiter les mails, retrouver les mots de passe, intercepter les informations et messages MSN, bloquer les sites web (le pirate peut empêcher de visiter les sites offrant des analyses antivirales en ligne ou autres mises à jour d'antivirus, NDLR).



Cet espioniciel permet aussi aux pirates de créer un serveur chat, en gros l'ordinateur de la victime se transforme en lieu de discussions ou de revente de CB, de films ou des plus grave. Une trentaine d'autres options ont été incluses dans ce programme qui, pour le moment, reste très discret **face aux logiciels de sécurité.**

4) Scénario :

A-Fichier binaires collecté a partir du honypote :



SECURINETS



Club de la sécurité informatique
INSAT

-->Analyse dynamique par Sandbox en ligne « Virustotal »

VirusTotal - Mozilla Firefox

http://www.virustotal.com/compacto.html

VIRUS TOTAL

Fichier vmup85.exe_ reçu le 2010.04.10 14:41:25 (UTC)

Antivirus	Version	Dernière mise à jour	Résultat
a-squared	4.5.0.50	2010.04.10	Virus.Win32.Flot!IK
AhnLab-V3	5.0.0.2	2010.04.10	-
AntiVir	7.10.6.55	2010.04.09	TR/Drop.Tofsee.H.1
Antiy-AVL	2.0.3.7	2010.04.09	-
Authentium	5.2.0.5	2010.04.10	-
Avast	4.8.1351.0	2010.04.10	Win32:Flot
Avast5	5.0.332.0	2010.04.10	Win32:Flot
AVG	9.0.0.787	2010.04.10	-
BitDefender	7.2	2010.04.10	Trojan.Dropper.Tofsee.H
CAT-QuickHeal	10.00	2010.04.10	-
ClamAV	0.96.0.3-git	2010.04.10	-
Comodo	4556	2010.04.10	-
DrWeb	5.0.2.03300	2010.04.10	BackDoor.IRC.Bot.283
eSafe	7.0.17.0	2010.04.08	-
eTrust-Vet	35.2.7418	2010.04.09	-
F-Prot	4.5.1.85	2010.04.10	-
F-Secure	9.0.15370.0	2010.04.10	Trojan.Dropper.Tofsee.H
Fortinet	4.0.14.0	2010.04.10	-
GData	19	2010.04.10	Trojan.Dropper.Tofsee.H
Ikarus	T3.1.1.80.0	2010.04.10	Virus.Win32.Flot
Jiangmin	13.0.900	2010.04.10	-
Kaspersky	7.0.0.125	2010.04.10	-
McAfee-GW-Edition	6.8.5	2010.04.09	Trojan.Drop.Tofsee.H.1
Microsoft	1.5605	2010.04.10	-
NOD32	5015	2010.04.10	Win32/AutoRun.IRCBot.DZ
Norman	6.04.11	2010.04.10	-
nProtect	2009.1.8.0	2010.04.06	Trojan.Dropper.Tofsee.H
Panda	10.0.2.2	2010.04.10	Generic Trojan
PCTools	7.0.3.5	2010.04.10	-
Prevx	3.0	2010.04.10	High Risk Cloaked Malware

SECURINETS



Club de la sécurité informatique
INSAT

Création du serveur :



Backdor « securinets » crée :

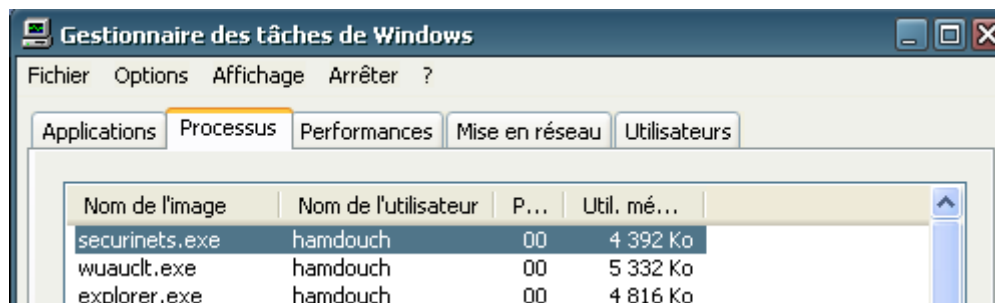
SECURINETS



Club de la sécurité informatique
INSAT



Backdor « securinets » est bien installé :



Connexion établie entre Backdor « securinets » et le serveur :

SECURINETS



Club de la sécurité informatique
INSAT

Turkojan Client v4.0 [Gold Edition] - Bug Fixed [Online :1] _ X

Alien Technology
TURKOJAN 4 *Turkey*
www.cigicigi.com

English Editor Settings About Order Port : 15963 Stop

passwords
accessories
settings manager
manage keyboard
extra
communication
chat with server
send message
manage files
commands
server properties
system information
fun manager
contact us
local tools

Send Fake Error Messages

Message Icon
[ANY]    

Message Buttons
 OK Yes,No,Cancel
 OK,Cancel Retry,Cancel
 Yes,No Abort,Retry,Ignore

Message Title : Error
Message : Subsystem is down
Use '!' charecter to send multiline message

Test Message Send Message

Connection ID :	IP Address :	Computer Name :	OS :
 securinets	192.168.1.74/192.168.1.74	7AMIDOU	WinXP

Lost connection! Status : Started

ANALYSE DE BACKDOR :

Analyse avec wirechark :

SECURINETS



Club de la sécurité informatique
INSAT

No.	Time	Source	Destination	Protocol	Info
51	16.065825	192.168.1.70	192.168.1.74	TCP	[TC
52	16.065874	192.168.1.74	192.168.1.70	TCP	fpo
54	19.983010	192.168.1.74	192.168.1.70	TCP	fpo
57	20.232621	192.168.1.70	192.168.1.74	TCP	159
58	20.232672	192.168.1.70	192.168.1.74	TCP	[TC
59	23.217771	192.168.1.70	192.168.1.74	TCP	159
60	23.217844	192.168.1.70	192.168.1.74	TCP	[TC
61	23.217892	192.168.1.74	192.168.1.70	TCP	fpo
62	23.220956	192.168.1.74	192.168.1.70	TCP	fpo
63	23.546893	192.168.1.70	192.168.1.74	TCP	159
64	23.546950	192.168.1.70	192.168.1.74	TCP	[TC
65	24.964863	192.168.1.74	192.168.1.70	TCP	fpo
66	25.167149	192.168.1.70	192.168.1.74	TCP	159
67	25.167233	192.168.1.70	192.168.1.74	TCP	[TC
68	29.974604	192.168.1.74	192.168.1.70	TCP	fpo
69	30.195837	192.168.1.70	192.168.1.74	TCP	159
70	30.195915	192.168.1.70	192.168.1.74	TCP	[TC

Frame 1 (63 bytes on wire, 63 bytes captured)
Ethernet II, Src: vmware_bf:33:43 (00:0c:29:bf:33:43), Dst: GemtekTe_55:c2:3f (00:21:00:...)
Internet Protocol, Src: 192.168.1.74 (192.168.1.74), Dst: 192.168.1.70 (192.168.1.70)
Transmission Control Protocol, Src Port: fpo-fps (1066), Dst Port: 15963 (15963) Seq: 1

```
0000 00 21 00 55 c2 3f 00 0c 29 bf 33 43 08 00 45 00  .!.U.?..).3C..E.  
0010 00 31 0c 45 40 00 80 06 6a a1 c0 a8 01 4a c0 a8  .1.E@...j....J..  
0020 01 46 04 2a 3e 5b e0 66 5e 38 f3 99 cd 30 50 18  .F.*>[.f ^8...0P.  
0030 44 66 47 68 00 00 42 41 47 4c 41 4e 54 49 3f    DfGh..BA GLANTI?
```

-->On voit ici que le backdoor qui a l'adresse 192.168.1.74 échange des données avec notre serveur 1.70

Analyse avec malwareBytes :

Malwarebytes' Anti-Malware

Recherche Protection Mise à jour Quarantaine Rapports/Logs Exclusions Paramètres Autres outils À propos...

Recherche
Malwarebytes' Anti-Malware examine en ce moment votre système. Veuillez attendre la fin de l'examen.

Recherche d'infections dans les éléments du système de fichiers.
Élément(s) analysé(s): 3008
Élément(s) infecté(s): 0

Type d'examen: Examen rapide
Temps écoulé: 2 minute(s), 10 seconde(s)

En cours d'analyse:
C:\WINDOWS\system32\svsp.ini

Suspendre l'examen Abandonner l'examen

Acheter Enregistrer Quitter

SECURINETS



Club de la sécurité informatique
INSAT

Malwarebytes' Anti-Malware

Recherche Protection Mise à jour Quarantaine Rapports/Logs Exclusions Paramètres Autres outils A propos...

Recherche
Ci-dessous se trouve une liste des programmes malveillants trouvés sur votre système. Fermez toutes les applications inutiles pour garantir la réussite de la suppression des menaces.

<input type="checkbox"/>	Vendeur	Catégorie	Elément	Autre	Action effectuée
<input checked="" type="checkbox"/>	Malware.Pack...	File	C:\Documents and Settings\hamdouch\Local...		No action taken.
<input checked="" type="checkbox"/>	Malware.Pack...	File	C:\Documents and Settings\hamdouch\Local...		No action taken.
<input checked="" type="checkbox"/>	Malware.Pack...	File	C:\Documents and Settings\hamdouch\Local...		No action taken.
<input checked="" type="checkbox"/>	Trojan.I.Stole....	File	C:\WINDOWS\system32\AntiWPA.dll		No action taken.
<input checked="" type="checkbox"/>	Trojan.I.Stole....	Memory Module	C:\WINDOWS\system32\AntiWPA.dll		No action taken.
<input checked="" type="checkbox"/>	Hijack.Control...	Registry Value	HKEY_CURRENT_USER\SOFTWARE\Micr...	Value: forceclas...	No action taken.
<input checked="" type="checkbox"/>	Hijack.Help	Registry Data	HKEY_CURRENT_USER\SOFTWARE\Micr...	Bad: (1) Good: (0)	No action taken.

Supprimer la sélection Ignorer Enregistrer le rapport Menu principal

Acheter Enregistrer Quitter

-->On voit qu'il detecte notre trojan....

SECURINETS



Club de la sécurité informatique
INSAT

Rapport généré :

```
1 Malwarebytes' Anti-Malware 1.45
2 www.malwarebytes.org
3
4 Version de la base de données: 3985
5
6 Windows 5.1.2600 Service Pack 3
7 Internet Explorer 7.0.5730.13
8
9 15/04/2010 22:40:33
10 mbam-log-2010-04-15 (22-40-33).txt
11
12 Type d'examen: Examen rapide
13 Élément(s) analysé(s): 98032
14 Temps écoulé: 4 minute(s), 15 seconde(s)
15
16 Processus mémoire infecté(s): 0
17 Module(s) mémoire infecté(s): 1
18 Clé(s) du Registre infectée(s): 0
19 Valeur(s) du Registre infectée(s): 1
20 Élément(s) de données du Registre infecté(s): 1
21 Dossier(s) infecté(s): 0
22 Fichier(s) infecté(s): 4
23
24 Processus mémoire infecté(s):
25 (Aucun élément nuisible détecté)
26
27 Module(s) mémoire infecté(s):
28 C:\WINDOWS\system32\AntiWPA.dll (Trojan.I.Stole.Windows) -> No action taken.
29
```

Analyse avec SysAnlyser :

sniff_hit
Network Interfaces: 192.168.1.74
HTTP Ports: 80
Copy Clear Unique IPs

SysAnalyzer
Pid: 2012

PID	Par...	User
1384	svchost.exe	AUTORITE NT:SYSTEM
1748	wuauclt.exe	7AMIDOU:hamdouch
2012	securinets.exe	7AMIDOU:hamdouch
1524	Capture.exe	7AMIDOU:hamdouch
468	Capture.exe	7AMIDOU:hamdouch
1544	wireshark.exe	7AMIDOU:hamdouch
1436	dumpcap.exe	7AMIDOU:hamdouch
932	Capture.exe	7AMIDOU:hamdouch
296	sysAnalyzer.exe	7AMIDOU:hamdouch
1996	sniff_hit.exe	7AMIDOU:hamdouch
1372	proc_analyzer.e...	7AMIDOU:hamdouch

Loaded Exploit Signatures

- Bagle Backdoor Exploitation 1
- Bagle Backdoor Exploitation 2
- DameWare Mini Remote Control Buffer Overflow
- RPC DCOM Exploit MS03-026
- LSASS exploit - MS04-011
- Microsoft Workstation Vulnerability
- MyDoom Backdoor Exploitation
- IIS 5.0 WebDAV Exploit

Analyze PID
Running Processes Open P...

report.
Data Report Tools



Rapport généré :

```
List Data
Copy Save
File: securinets.exe
Size: 110592 Bytes
MD5: AE7203DA3446D5D9C8E38D788087FEC5
Packer: File not found C:\IDEFENSE\SysAnalyzer\peid.exe

File Properties: CompanyName
FileDescription
FileVersion
InternalName
LegalCopyright
OriginalFilename
ProductName
ProductVersion

Exploit Signatures:
-----
Scanning for 19 signatures
Scan Complete: 320Kb in 0,031 seconds
Urls
-----
```

5) Conclusion :

Les malware sont des outils utilisés par les pirates pour contrôler d'une façon illégale les activités d'une victime ou encore pour nuire ou paralyser le fonctionnement de son poste de travail.

Ces activités peuvent être s si les autorités réussissent à découvrir l'identité du pirate, de ce fait il est fortement recommandé de ne pas utiliser de tels outils mais seulement apprendre à s'en protéger.