



```
for(e=n;s<i;c++){attitude();}
```

Sur environnement Microsoft Windows

# Il était une fois... les investigations forensic !

## Pourquoi une investigation ?

- ▶ Doutes de malveillance interne
- ▶ Corruption de client, serveur, défacement de site. . .
- ▶ Identification des processus de malveillance
- ▶ Moyens de correction
- ▶ . . .

# Il était une fois... les investigations forensic !

## Sources d'investigations numériques :

- ▶ L'état instantané du système (mémoire, processus, sockets, fichiers ouverts. . . )
- ▶ Le système de fichiers (FAT, NTFS)
- ▶ Les journaux d'audit (Evt, Evtx et parfois log)
- ▶ La base de registre
- ▶ ...

# Systeme de fichiers

- ▶ **Les interactions** : dates d'accès, modification, création...  
Informations modifiables à partir d'un accès en écriture.  
Peu fiables en cas de modification de l'heure système.  
Limitées aux derniers accès, dernières modifications...
- ▶ **Les restrictions d'accès** : propriétaire, ACL, Bitlocker...  
Inutiles en cas de démarrage à partir d'un autre système d'exploitation.
- ▶ **Les attributs** : caché, protégé système, compressé, chiffré...
- ▶ **Les types de fichiers** : répertoires, fichiers, ADS (NTFS Alternative Data Stream)...

# Système de fichiers : Modifier les dates en C

```
HANDLE hFile = CreateFile(" fichier", GENERIC_READ|GENERIC_WRITE,
                        NULL, OPEN_EXISTING, FILE_ATTRIBUTE_NORMAL, NULL);
if (hFile != INVALID_HANDLE_VALUE)
{
    //Nouvelle date : 13 Mars 2012 08:30:00.00
    SYSTEMTIME sysTime;
    sysTime.wDay           = 13;
    sysTime.wMonth        = 03;
    sysTime.wYear         = 2012;

    sysTime.wHour         = 8;
    sysTime.wMinute       = 30;
    sysTime.wSecond       = 0;
    sysTime.wMilliseconds = 0;

    //Conversion de la date pour le fichier
    FILETIME fileWriteTime, locTime;
    SystemTimeToFileTime(&sysTime, &locTime);
    LocalFileTimeToFileTime(&locTime, &fileWriteTime);

    //Appliquer au fichier
    SetFileTime(hFile,
                NULL, /*CreationTime*/
                NULL, /*LastAccessTime*/
                &fileWriteTime /*LastWriteTime*/);
}
CloseHandle(hFile);
```

# Système de fichiers : Outils - Windows

- ▶ McAfee/Foundstone Forensic Toolkit : en ligne de commande, il gère en plus les ACL (ACE+SID) et exporte en texte brut.

<http://www.mcafee.com/us/downloads/free-tools/>

- ▶ Streams (Windows Sysinternals) : recherche de fichiers ADS.

<http://technet.microsoft.com/en-us/sysinternals/bb897440.aspx>

- ▶ Dislocker (HSC) : lecture de partition bitlocker sous Linux.

<http://www.hsc.fr/ressources/outils/dislocker/>

- ▶ Suites AccessData (payant) : système de fichiers, mémoire. . .

<http://accessdata.com/products/computer-forensics>

# Les journaux d'audit : Formats Evt/Evtx

## Evt (< Vista)

Enregistrements stockés par ordre chronologique

ID + source d'un évènement = description et format de l'enregistrement

Plusieurs niveaux d'état/criticité

Dates d'émission et d'écriture de l'enregistrement (soumis à l'heure système)

Emplacement par défaut :  
C:\Windows\system32\config\

Format de fichier assez simple à exploiter sans les API Windows (séquentiel)

## Evtx (≥ Vista)

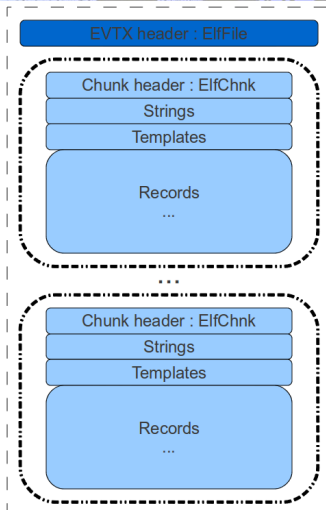
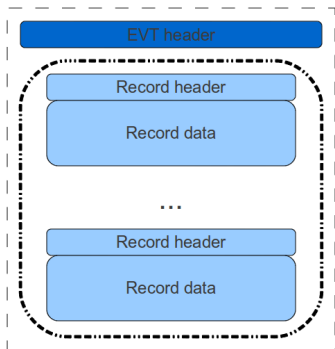
Ordre chronologique par groupe

Emplacement par défaut :  
C:\Windows\system32\winevt\logs\

Format de fichier assez complexe à exploiter sans les API Windows (BinXML)

Nécessité d'activer des règles d'audit pour journaliser...

# Les journaux d'audit : Formats Evt/Evtx





# Les journaux d'audit : Identifiants intéressants

ID	Source	OS	Description
512/513	Security	< Vista	Windows start/stop
528/538			User Logon/Logoff
520			The system time was changed
517			The security log was cleared
4608/4609	Microsoft-Windows-Security-Auditing	≥ Vista	Windows start/stop
4624/4634			User Logon/Logoff
4616			The system time was changed
1102			The security log was cleared

# Les journaux d'audit : Outils

- ▶ Evtx Parser : script PERL de conversion Evtx vers XML

<http://computer.forensikblog.de/en/>

- ▶ TZWorks Windows Event Log Viewer : lecteur Evtx avec visualisation binaire

[http://www.tzworks.net/download\\_links.php](http://www.tzworks.net/download_links.php)

- ▶ Microsoft wevtutil (à partir de Vista) : conversion Evt vers Evtx

`wevtutil export-log source.evt target.evtx /lf`

# La base de registre : Présentation

Contient un grand nombre de données :

- ▶ Hardware (données non statiques)
- ▶ Système : bootkey, GPO et licences. . .
- ▶ Configuration : logiciels, mises à jour, réseau, services et drivers. . .
- ▶ Utilisateurs : liste locale des groupes, utilisateurs, hash des mots de passe
- ▶ Historiques utilisateurs : MRU, MUICache, UserAssist. . .
- ▶ Divers : supports externes connectés (USB), applications au démarrage. . .

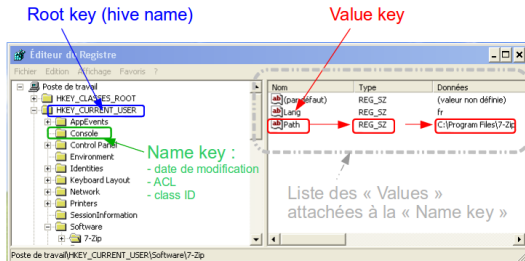
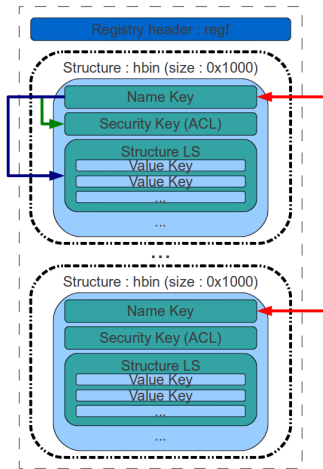
**Une mine d'or pour les analyses forensic !**

# La base de registre : Présentation

Et...

- ▶ Le format binaire n'a presque pas évolué, seule la structure a évolué
- ▶ Le format binaire est un peu documenté
- ▶ Les droits appliqués par défaut sont peu restrictifs
- ▶ Droits difficiles à modifier : architecture peu documentée
- ▶ L'édition hors ligne est possible en cas de disque non chiffré
- ▶ Aucun blocage des API n'existe en GPO (hors ACL), seul Regedit peut être bloqué par une clé de registre (modifiable par tous les utilisateurs)

# La base de registre : Le format



# La base de registre : Les données

- ▶ **Applications au démarrage :** (HKEY\_LOCAL\_MACHINE et HKEY\_CURRENT\_USER)  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\, RunOnce, RunOnceEx  
HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Startup\, Logon, Shutdown, Logoff  
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Load\, Run, AppSetup, Shell
- ▶ **Services et drivers :** HKLM\SYSTEM\CurrentControlSet\Services\
- ▶ **Logiciels et mises à jour installés :**  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\  
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\Packages\  
HKLM\SOFTWARE\Microsoft\Updates\
- ▶ **Supports externes déjà connectés :** HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR\

# La base de registre : Les données (MRU)

## ▶ MRU (Most Recently Use):

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\, RecentDocs, StreamMRU, ComputerDescriptions, Map Network Drive MRU, ComDlg32\LastVisitedMRU, ComDlg32\OpenSaveMRU

HKCU\SOFTWARE\Microsoft\Search Assistant\ACMrU\

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Applets\\*\Recent File List\

HKCU\SOFTWARE\Microsoft\Office\\*\\*\Recent File List\

Éditeur du Registre

Poste de travail\HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
a	REG_SZ	regedit\1
b	REG_SZ	cmd\1
c	REG_SZ	gpedit.msc\1
d	REG_SZ	reg\1
e	REG_SZ	regedit HKEY_LOCAL_MACHINE\SOFTWARE\7-Zip\1
f	REG_SZ	runas\1 751

Exécuter

Entrez le nom d'un programme, dossier, document ou d'une ressource Internet, et Windows l'ouvrira pour vous.

Ouvrir : regedit

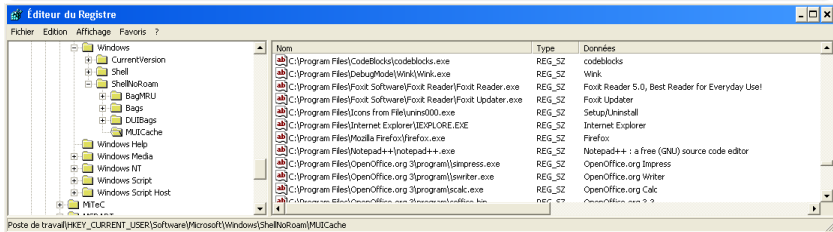
- regedit /?
- cmd
- regedit HKEY\_LOCAL\_MACHINE\SOFTWARE\7-Zip
- reg
- gpedit.msc

# La base de registre : Les données (MUICache)

## ► MUICache (Applications déjà exécutées) :

HKCU\SOFTWARE\Microsoft\Windows\ShellNoRoam\MUICache\

HKCU\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\MUICache\



The screenshot shows the Windows Registry Editor window titled "Éditeur du Registre". The left pane shows the tree structure expanded to "Poste de travail\HKEY\_CURRENT\_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache". The right pane displays a list of registry values:

Nom	Type	Données
C:\Program Files\CodeBlocks\codeblocks.exe	REG_SZ	codeblocks
C:\Program Files\DebugMode\Wink\Wink.exe	REG_SZ	Wink
C:\Program Files\Foxit Software\Foxit Reader\Foxit Reader.exe	REG_SZ	Foxit Reader 5.0, Best Reader for Everyday Use!
C:\Program Files\Foxit Software\Foxit Reader\Foxit Updater.exe	REG_SZ	Foxit Updater
C:\Program Files\Icons from File\Unins000.exe	REG_SZ	Setup/Uninstall
C:\Program Files\Internet Explorer\IEXPLORE.EXE	REG_SZ	Internet Explorer
C:\Program Files\Mozilla Firefox\firefox.exe	REG_SZ	Firefox
C:\Program Files\Notepad++\notepad++.exe	REG_SZ	Notepad++ : a free (GNU) source code editor
C:\Program Files\OpenOffice.org 3\program\smpress.exe	REG_SZ	OpenOffice.org Impress
C:\Program Files\OpenOffice.org 3\program\swriter.exe	REG_SZ	OpenOffice.org Writer
C:\Program Files\OpenOffice.org 3\program\scalc.exe	REG_SZ	OpenOffice.org Calc
C:\Program Files\OpenOffice.org 3\program\soffice.bin	REG_SZ	OpenOffice.org 3



# La base de registre : Les données (UserAssist)

## ▶ UserAssist (Applications exécutées, codées en ROT13) :

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\\*

Éditeur du Registre

Fichier Edition Affichage Favoris ?

Streams  
StuckRects2  
tips  
TrayNotify  
User Shell Folders  
UserAssist  
    {5E6AB780-7743-11CF-A12B-00AA004AE837}  
        Count  
    {75048700-EF1F-11D0-9888-006097DEACF9}  
        Count  
VisuaEffects  
Workgroup\Crawler  
Ext  
Group Policy  
grpConv  
Internet  
Internet Settings  
Policies

Nom	Type	Données
HRZR_EHACNGU:P:JVAQB3JF ertqvgr.rkr	REG_BIN...	1a 00 00 00 83 00 00 10 a0 ba 74 c 7 9e cc 01
HRZR_EHACNGU:P:JVAQB3JF ifgrz32 ABGRONQ.RKR	REG_BIN...	17 00 00 00 4a 00 00 00 40 b8 5f 9c c0 95 cc 01
HRZR_EHACNGU:P:JVAQB3JF ifgrz32 ehaay32.rkr	REG_BIN...	19 00 00 00 06 00 00 00 14 51 57 59 9a cc 01
HRZR_EHACNGU:P:JVAQB3JF ifgrz32 ert.rkr	REG_BIN...	11 00 00 00 06 00 00 00 30 e5 08 3c 1b 80 cc 01
HRZR_EHACNGU:P:JVAQB3JF ifgrz32 hncqte.rkr	REG_BIN...	0f 00 00 00 06 00 00 10 68 97 1e 34 75 cc 01
HRZR_EHACNGU:P:JVAQB3JF ifgrz32 pnyp.rkr	REG_BIN...	13 00 00 00 3a 00 00 00 b0 2a 8a 99 33 87 cc 01
HRZR_EHACNGU:P:JVAQB3JF ifgrz32 pza.rkr	REG_BIN...	18 00 00 00 24 00 00 00 70 75 d5 a6 c8 98 cc 01
HRZR_EHACNGU:P:JVAQB3JF ifgrz32 zfnwag.rkr	REG_BIN...	12 00 00 00 0a 00 00 00 60 41 ec a9 19 81 cc 01
HRZR_EHACNGU:P:JVAQB3JF ifgrz32 zfrkvp.rkr	REG_BIN...	11 00 00 00 06 00 00 20 cf 68 95 2e 7a cc 01
HRZR_EHACNGU:P:JVAQB3JF ifgrz32 zsp.rkr	REG_BIN...	0e 00 00 07 00 00 00 e0 71 c5 eb 46 74 cc 01
HRZR_EHACNGU:P:\Qbphzraof naq Frogvatf\avpb\Ohermh\{P} Y...	REG_BIN...	01 00 00 00 06 00 00 50 b6 2a 31 4a 58 cc 01
HRZR_EHACNGU:P:\Qbphzraof naq Frogvatf\avpb\Ohermh\Abhi...	REG_BIN...	11 00 00 00 06 00 00 60 d5 45 d4 56 79 cc 01
HRZR_EHACNGU:P:\Qbphzraof naq Frogvatf\avpb\Ohermh\EGP...	REG_BIN...	0d 00 00 00 08 00 00 20 at b8 74 4a 72 cc 01
HRZR_EHACNGU:P:\Qbphzraof naq Frogvatf\avpb\Ohermh\EGP...	REG_BIN...	0d 00 00 00 06 00 00 60 2c 91 54 06 73 cc 01
HRZR_EHACNGU:P:\Qbphzraof naq Frogvatf\avpb\Ohermh\EGP...	REG_BIN...	0d 00 00 00 06 00 00 80 bc 5d 4f 1b 73 cc 01

Poste de travail\REY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}

Path	Use count	Last GUID update	User
I UEME_RUNPATH.C:\WINDOWS\regedit.exe	0x00000083	2011/11/09/11:04:50	nico...
I UEME_RUNPATH.C:\WINDOWS\system32\notepad.exe	0x0000004a	2011/10/28/23:22:16	nico...
I UEME_RUNPATH.C:\WINDOWS\system32\calc.exe	0x0000003a	2011/10/10/10:57:36	nico...
I UEME_RUNPATH.C:\WINDOWS\system32\cmd.exe	0x00000024	2011/11/01/19:56:56	nico...
I UEME_RUNPATH.C:\WINDOWS\system32\mmc.exe	0x00000007	2011/09/16/08:55:48	nico...
I UEME_RUNPATH.C:\WINDOWS\system32\mspaint.exe	0x0000000a	2011/10/02/16:36:22	nico...
I UEME_RUNPATH.C:\WINDOWS\system32\reg.exe	0x00000006	2011/10/01/10:18:14	nico...
I UEME_RUNPATH.C:\WINDOWS\system32\rundll32.exe	0x00000006	2011/11/03/19:47:25	nico...
I UEME_RUNPATH.C:\WINDOWS\system32\wupdmgr.exe	0x00000006	2011/09/17/13:19:33	nico...

# La base de registre : Outils - Windows

## Extracteurs/Éditeurs de fichiers de registre brut :

- ▶ MiTec Windows Registry Recovery : <http://www.mitec.cz>
- ▶ TZWorks Yet Another Registry Utility :  
[http://www.tzworks.net/download\\_links.php](http://www.tzworks.net/download_links.php)
- ▶ Digital Forensics Framework : <http://www.digital-forensic.org>
- ▶ Regviewer : <http://sourceforge.net/projects/regviewer/>
- ▶ Registry decoder : <http://code.google.com/p/registrydecoder/>

## **Constat** : Après plusieurs années d'investigation...

- ▶ **Peu d'outil libre de corrélation de données** : système de fichiers, journaux d'audit, base de registre et données spécifiques
- ▶ **Peu d'outils d'extraction/analyse forensic globale de machine** (et souvent payants)
- ▶ **Résultats souvent trop limités**
- ▶ Finalement, beaucoup de temps dépensé pour des résultats perfectibles

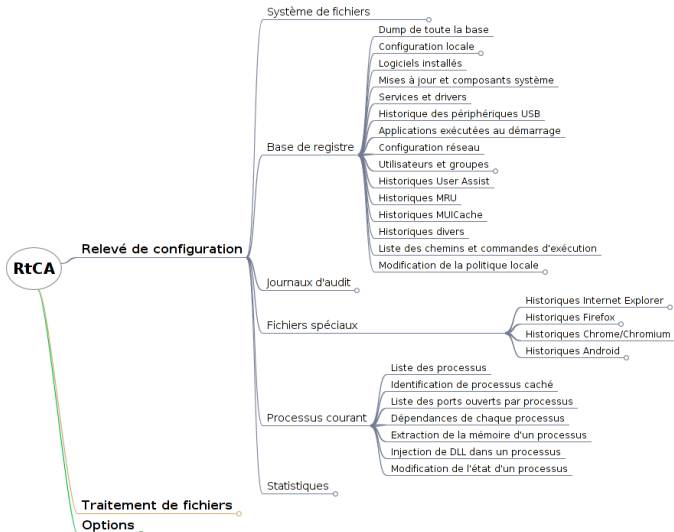
# Constat Après plusieurs années d'analyses Forensic...

## Création d'une boîte à outils d'extraction de configuration et d'analyse forensic : RtCA

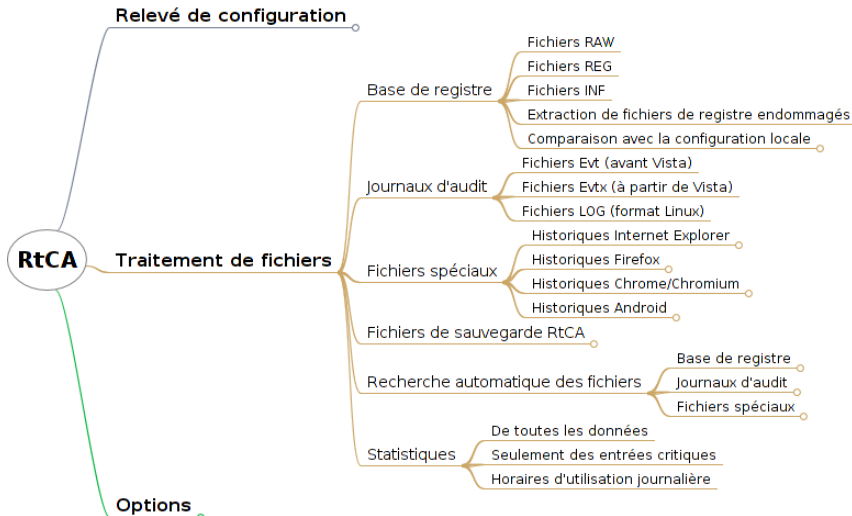
- ▶ Projet libre sous licence GPLv3
- ▶ Codé en C win32/64 compatible XP/2003/2008/7/8/Wine
- ▶ Extraction/Traitement des fichiers, des journaux d'audit, de la base de registre et certains applicatifs (navigateurs, Android...)
- ▶ Première publication *testing* en octobre 2011, encore beaucoup de travail...

<http://omni-a.blogspot.com/2011/10/rtca-v01-outil-daide-aux-analyses.html>

# RtCA : Fonctionnement



# RtCA : Fonctionnement



# RtCA : Aperçu

## Accès rapide aux informations : (outil de relevé de configuration)

RtCA v0.2.76 - <http://code.google.com/p/omnia-projects/>

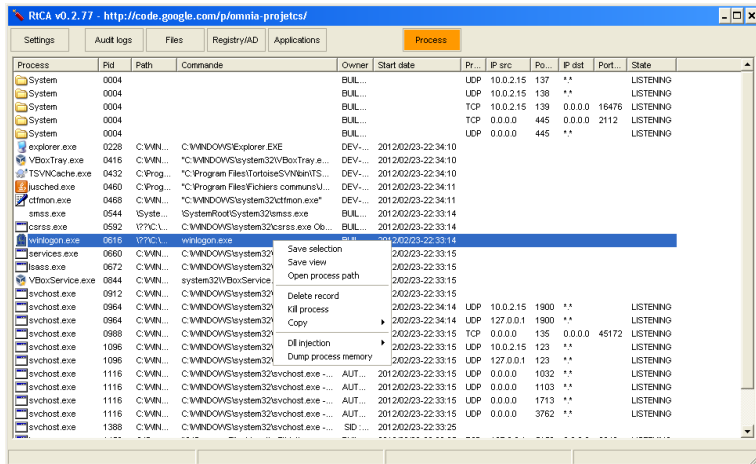
Settings Audit logs Files **Registry** Applications State Process

File	Key	Value	Data	Description	Parent key update
	HKEY...	ProductName	Microsoft Windows XP	(Settings) Operating System	2012/02/06-20:2...
	HKEY...	CSD/Version	Service Pack 3	(Settings) Service Pack	2012/02/06-20:2...
	HKEY...	SystemRoot	C:\WINDOWS	(Settings) System path	2012/02/06-20:2...
	HKEY...	DigitalProductId		(Serial) MS product serial	2012/02/06-20:2...
	HKEY...	AppInit_DLLs		(malware) DLL load in GUI Windows	2011/08/08-19:3...
	HKEY...	Debugger	ntsd -d	(attack vector) Use for redirect application	2011/08/08-19:3...
	HKEY...	Autorun		(malware) Command to execute with all cmd com...	2011/08/08-19:3...
	HKEY...	NoDriveTypeAutoRun	<NO VALUE>	(malware) Autorun usb/CDROM/... 0x01: disable	2012/01/04-15:5...
	HKEY...	Autorun	<NO VALUE>	(malware) Autorun CDROM, 0x00: disable	2012/02/06-20:2...
	HKEY...	RestrictNullSessAccess	<NO VALUE>	(attack vector) Null session, 0x01: Disable	2012/02/06-20:2...
	HKEY...	dontdisplaylastusername	<NO VALUE>	(authentication) 0x01: Do not display last usernam...	2012/02/06-20:2...
	HKEY...	enableplaintextpassword	<NO VALUE>	(authentication) 0x00: Disable send unencrypted ...	2012/02/06-20:2...
	HKEY...	dontdisplaylastusername	<NO VALUE>	(authentication) 0x01: Do not display last usernam...	2011/08/08-17:3...
	HKEY...	enableplaintextpassword	00000000	(authentication) 0x00: Disable send unencrypted ...	2011/08/08-17:3...
	HKEY...	RestrictNullSessAccess	<NO VALUE>	(attack vector) Null session, 0x01: Disable	2011/08/08-17:3...
	HKEY...	RestrictAnonymousSAM	00000001	(attack vector) Anonymous connexion for SAM e...	
	HKEY...	RestrictAnonymous	00000000	(attack vector) Anonymous connexion, 0x01: Dis...	
	HKEY...	LmCompatibilityLevel	00000000	(location) Authentication method 0x00: only ...	
	HKEY...	NoLmHash	00000000	(location) 0x01: Disable LM HASH	
	HKEY...	auditbaseobjects	00000000	(audit) the access of global system objects...	
	HKEY...	fulprivilegeauditing	00000000	(audit) use of Backup and Restore privileg...	
	HKEY...	everyoneincludesanonymous	00000000	(application) Permissions "everyone" are appl...	
	HKEY...	DontDisplayLastUserName	00000000	(application) Dtsplay last user login, 0x01: Disab...	2012/01/04-16:0...
	HKEY...	EnableLUA	<NO VALUE>	(application) 0x01: Disable UIAC (User Account Con...	2012/01/04-16:0...
	HKEY...	DisableRegistryTools	00000000	(application) Disable use of windows registry ...	2012/01/04-16:0...
	HKEY...	disablecad	<NO VALUE>	(application) 0x01: Enable CTRL+ALT+DEL requirem...	2012/02/06-20:2...
	HKEY...	legalnoticefile	<NO VALUE>	(application) Message title for user attempting ...	2011/08/08-19:3...
	HKEY...	legalnoticecaption	<NO VALUE>	(application) Message for user attempting to l...	2011/08/08-19:3...
	HKEY...	ScreenSaveActive	<NO VALUE>	(Saver) Enable screensaver, 0x01: Enable	2011/12/10-21:4...

load 633 events

# RtCA : Aperçu

## État des processus :



RtCA v0.2.77 - <http://code.google.com/p/omnia-projets/>

Settings | Audit logs | Files | Registry/AD | Applications | **Process**

Process	Pid	Path	Commande	Owner	Start date	Pr...	IP src	Po...	P dist	Port...	State
System	0004			BUIL...			UDP 10.0.2.15	137	**		LISTENING
System	0004			BUIL...			UDP 10.0.2.15	138	**		LISTENING
System	0004			BUIL...			TCP 10.0.2.15	139	0.0.0.0	16476	LISTENING
System	0004			BUIL...			TCP 0.0.0.0	445	0.0.0.0	2112	LISTENING
System	0004			BUIL...			UDP 0.0.0.0	445	**		LISTENING
explorer.exe	0228	C:\WIN...	C:\WINDOWS\Explorer.EXE	DEV-...	2012/02/23-22:34:10						
YBoxTray.exe	0416	C:\WIN...	"C:\WINDOWS\system32\YBoxTray.e...	DEV-...	2012/02/23-22:34:10						
TSVNCache.exe	0432	C:\Prog...	"C:\Program Files\TorloiseSYN\TS...	DEV-...	2012/02/23-22:34:10						
tschost.exe	0460	C:\Prog...	"C:\Program Files\Fichiers communs\U...	DEV-...	2012/02/23-22:34:11						
ctfmon.exe	0468	C:\WIN...	"C:\WINDOWS\system32\ctfmon.exe"	DEV-...	2012/02/23-22:34:11						
smss.exe	0544	\Syste...	\SystemRoot\System32\smss.exe	BUIL...	2012/02/23-22:33:14						
csrss.exe	0592	?77C:\...	C:\WINDOWS\system32\csrss.exe Ob...	BUIL...	2012/02/23-22:33:14						
winlogon.exe	0616	?77C:\...	winlogon.exe		2012/02/23-22:33:14						
services.exe	0660	C:\WIN...	C:\WINDOWS\system32\services.exe		2012/23-22:33:15						
lsass.exe	0672	C:\WIN...	C:\WINDOWS\system32\lsass.exe		2012/23-22:33:15						
YBoxService.exe	0844	C:\WIN...	system32\YBoxService.exe		2012/23-22:33:15						
svchost.exe	0912	C:\WIN...	C:\WINDOWS\system32\svchost.exe		2012/23-22:33:15						
svchost.exe	0964	C:\WIN...	C:\WINDOWS\system32\svchost.exe		2012/23-22:34:14	UDP	10.0.2.15	1900	**		LISTENING
svchost.exe	0964	C:\WIN...	C:\WINDOWS\system32\svchost.exe		2012/23-22:34:14	UDP	127.0.0.1	1900	**		LISTENING
svchost.exe	0988	C:\WIN...	C:\WINDOWS\system32\svchost.exe		2012/23-22:33:15	TCP	0.0.0.0	135	0.0.0.0	45172	LISTENING
svchost.exe	1095	C:\WIN...	C:\WINDOWS\system32\svchost.exe		2012/23-22:33:15	UDP	10.0.2.15	123	**		LISTENING
svchost.exe	1096	C:\WIN...	C:\WINDOWS\system32\svchost.exe		2012/23-22:33:15	UDP	127.0.0.1	123	**		LISTENING
svchost.exe	1116	C:\WIN...	C:\WINDOWS\system32\svchost.exe	AUT...	2012/02/23-22:33:15	UDP	0.0.0.0	1032	**		LISTENING
svchost.exe	1116	C:\WIN...	C:\WINDOWS\system32\svchost.exe	AUT...	2012/02/23-22:33:15	UDP	0.0.0.0	1103	**		LISTENING
svchost.exe	1116	C:\WIN...	C:\WINDOWS\system32\svchost.exe	AUT...	2012/02/23-22:33:15	UDP	0.0.0.0	1713	**		LISTENING
svchost.exe	1116	C:\WIN...	C:\WINDOWS\system32\svchost.exe	AUT...	2012/02/23-22:33:15	UDP	0.0.0.0	3762	**		LISTENING
svchost.exe	1388	C:\WIN...	C:\WINDOWS\system32\svchost.exe	SID...	2012/02/23-22:33:25						

Context menu for winlogon.exe:

- Save selection
- Save view
- Open process path
- Delete record
- Kill process
- Copy
- Dll injection
- Dump process memory



# RtCA : Aperçu

## Corrélation de données :

RtCA v0.2.76 - <http://code.google.com/p/omnia-projets/>

Settings Audit logs Files Registry/AD Applications **State** Process

Date	Source	Description	User/ACL
2012/01/15-10:51:03	Audit logs	[INFORMATION] Service Control Manager : 07036 (Status servic...	
2012/01/15-10:51:04	Audit logs	[INFORMATION] Service Control Manager : 07036 (Status servic...	
2012/01/15-11:39:48	Registry	[Key update] Data from : UserAssist ; UEME_LUOTOOLBAR:0x1123	nico SID :S-1-5-21-160698084
2012/01/15-12:58:40	Registry	[Key update] Data from : UserAssist ; UEME_RUNPATH:C:Progr...	nico SID :S-1-5-21-160698084
2012/01/15-12:58:40	Registry	[Key update] Data from : UserAssist ; UEME_RUNPIDL:%csid2%	nico SID :S-1-5-21-160698084
2012/01/15-13:20:23	Registry	[Key update] Data from : UserAssist ; UEME_RUNPATH.Z:Intern...	nico SID :S-1-5-21-160698084
2012/01/15-13:41:40	Registry	[Key update] Data from : UserAssist ; UEME_RUNPATH.Z:Intern...	nico SID :S-1-5-21-160698084
2012/01/15-14:31:48	Audit logs	[INFORMATION] Tcpip : 04201 (New network connection) DEV-...	
2012/01/20-17:23:14	Audit logs	[INFORMATION] BROWSER : 08033 (The browser has forced a...	
2012/01/20-17:23:14	Audit logs	[ERROR] Dhcp : 01000 (New IP address) DEV-XP 08002703726...	
2012/01/20-17:23:14	Audit logs	[WARNING] Dhcp : 01003 (Error to renew address) DEV-XP 080...	
2012/01/20-17:23:37	Audit logs	[INFORMATION] W32Time : 00035 (Time service synchronised) ...	
2012/01/20-19:40:44	Registry	[Key update] Data from : UserAssist ; UEME_RUNPATH:Mozilla F...	nico SID :S-1-5-21-160698084
2012/01/20-20:08:24	Registry	[Key update] Data from : Software ; Index Dat Spy 2.1.0	
2012/01/20-20:53:18	Registry	[Key update] Data from : Software ; Index.dat Analyzer v2.5 2.5	
2012/01/20-21:06:57	Registry	[Key update] Data from : UserAssist ; UEME_RUNPATH:C:Docu...	nico SID :S-1-5-21-160698084
2012/01/21-00:55:48	Registry	[Key update] Data from : UserAssist ; UEME_RUNPATH.Z:RTCA...	nico SID :S-1-5-21-160698084
2012/01/21-10:05:15	Audit logs	[INFORMATION] Tcpip : 04201 (New network connection) DEV-...	
2012/01/21-10:15:33	Audit logs	[WARNING] W32Time : 00036 (Time service not synchronised) ...	
2012/01/21-10:21:27	Registry	[Key update] Data from : UserAssist ; UEME_RUNPATH.Z:RTCA...	nico SID :S-1-5-21-160698084
2012/01/21-10:35:24	Registry	[Key update] Data from : UserAssist ; UEME_RUNPATH.Z:RTCA...	nico SID :S-1-5-21-160698084
2012/01/21-10:35:28	Registry	[Key update] Data from : UserAssist ; UEME_RUNPATH.Z:RTCA...	nico SID :S-1-5-21-160698084
2012/01/21-10:35:34	Registry	[Key update] Data from : UserAssist ; UEME_RUNPATH.Z:RTCA...	nico SID :S-1-5-21-160698084
2012/01/21-10:42:40	Registry	[Key update] Data from : UserAssist ; UEME_RUNPIDL:%csid2%	nico SID :S-1-5-21-160698084
2012/01/21-10:42:40	Registry	[Key update] Data from : UserAssist ; UEME_RUNPIDL:%csid2%	nico SID :S-1-5-21-160698084
2012/01/21-10:42:40	Registry	[Key update] Data from : UserAssist ; UEME_RUNPATH:C:WIND...	nico SID :S-1-5-21-160698084
2012/01/21-12:04:12	Audit logs	[INFORMATION] Tcpip : 04201 (New network connection) DEV-...	
2012/01/21-13:20:09	Reolstrv	[Key update] Data from : UserAssist ; UEME_RUNPATH.Z:RTCA...	nico SID :S-1-5-21-160698084

All

load 633 events

# Références

- ▶ **SANS digital forensics :**  
<http://computer-forensics.sans.org/>
- ▶ **Andreas Schuster :**  
<http://computer.forensikblog.de/en/>
- ▶ **Windows NT Registry File (REGF) format specification :**  
<http://sourceforge.net/projects/libregf/files/Documentation/>
- ▶ **Revers of SAM registry :**  
<http://www.beginningtoseethelight.org/ntsecurity/>
- ▶ **NTFS Alternate Streams :**  
<http://www.flexhex.com/docs/articles/alternate-streams.phtml>

# Des questions ?

Merci d'être resté éveillé jusqu'au bout !

- ▶ **Contact** : `nicolas.hanteville(at)devoteam.com`
- ▶ **RtCA** : `http://code.google.com/p/omnia-projetcs/`