DEPLOIEMENT
WINDOWS SERVER 2003 / XP

Siège social de
Renault Europe Automobiles
(R E A)

```
; Script d'installation AutoIT pour les clients Symantec Antivirus Corporate Edition.
; Pierre ROYER - Renault Europe Automobiles, juin 2004.

$Dossier = @TempDir

FileInstall ("GRC.DAT", $Dossier & "\GRC.DAT")
FileInstall ("GRC.REG", $Dossier & "\GRC.REG")

AutoItSetOption ("SendKeyDelay", 2)
Sleep (150)

Run ("runas /noprofile /user:interactmig c:\windows\system32\cmd.exe", "")
Sleep (300)

Send ("1@dminAV{ENTER}")
Sleep (300)

Send ("copy " & $Dossier & "\GRC.DAT "& CHR (34) &"D:\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5\"& CHR (34) &" /Y")
Sleep (250)
Send ("{ENTER}")
Sleep (300)

Send ("regedit /s " & $Dossier & "\GRC.REG")
Sleep (250)
Send ("{ENTER}")
Sleep (300)

Send ("net stop "& CHR (34) &"Symantec AntiVirus Client"& CHR (34))
Sleep (250)

Send ("{ENTER}")
Sleep (300)

Send ("net start "& CHR (34) &"Symantec AntiVirus Client"& CHR (34))
Sleep (250)

Send ("{ENTER}")
Sleep (300)

FileDelete($Dossier & "\GRC.*")
;send ("DEL " & $Dossier & "\GRC.*{ENTER}")
Sleep (250)

Send ("exit{ENTER}")
```

REMERCIEMENTS

Mes remerciements s'adressent à toutes les personnes qui ont contribué à l'élaboration de ce projet.

Pour la qualité de l'enseignement et du contenu de la formation d'administrateur réseau et systèmes, je tiens à remercier toute l'équipe des enseignants.

Je remercie tout particulièrement Madame Spathis pour m'avoir fait confiance, et pour m'avoir admis au sein de la formation de cette session 2003-2004.

Je veux également exprimer ma gratitude à l'équipe informatique de Renault Europe Automobiles, dans laquelle j'ai effectué mon stage de trois mois. Un grand merci notamment à Jean-Louis Ghiglione, Chef du Service Exploitation et Infrastructures Techniques, qui m'a accueilli dans son service.

De même, je suis reconnaissant envers les autres stagiaires, avec lesquels j'ai pu échanger des informations utiles à l'enrichissement de mes connaissances informatiques.

* * * * *

SOMMAIRE

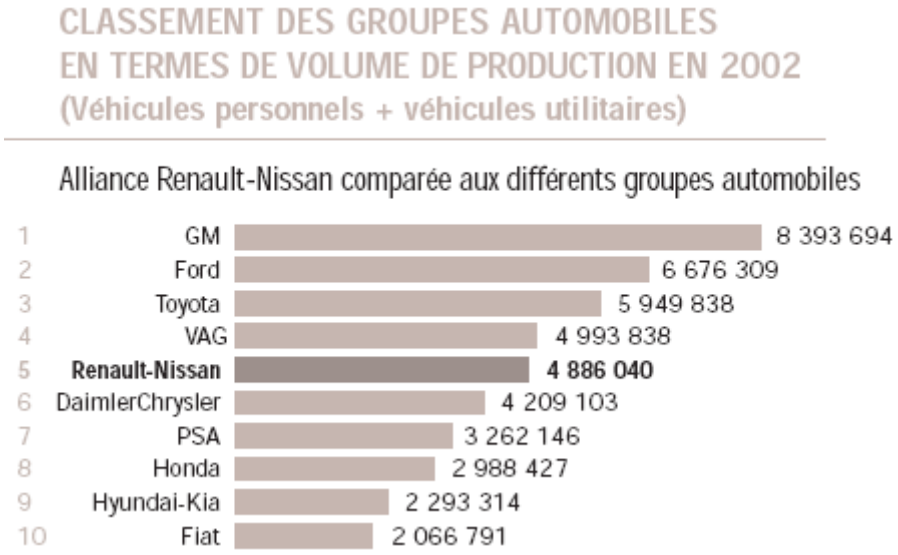
PRESENTATION DE RENAULT EUROPE AUTOMOBILES

Renault Europe Automobile est la filiale de distribution du groupe Renault. Créée en 2001, elle unifie l'ensemble du réseau de distribution propre de Renault en Europe, et assure la gestion et l'animation de ses filiales de ventes. Avec 14 609 personnes, 290 500 véhicules neufs et 230 500 véhicules d'occasion sont vendus sur ses 250 sites (dont 23 pour Nissan) en France et Europe.

Parmi les autres services propres à l'automobile, on peut aussi signaler :
- la vente de pièces de rechanges (730 157 K€ de chiffre d'affaire).
- l'entretien des véhicules en ateliers: carrosserie et mécanique (196 449 K€ de chiffre d'affaire).
- la vente de services associés : financement, assurances, location…

Avec 11,1% de part de marché, R.E.A. est le premier Groupe de distribution automobile en Europe, et s'est implanté dans douze pays : l'Allemagne, l'Autriche, la Belgique, l'Espagne, la France, la Grande-Bretagne, la Hongrie, l'Italie, le Luxembourg, les Pays-Bas, le Portugal, et la Suisse.

Depuis le 27 mars 1999, une alliance entre Renault et Nissan voit le jour, et la production automobile représente près de 9 % du marché mondial.



En septembre 1999, le groupe Renault a pris le contrôle du constructeur Dacia, qui occupe près de 45% de part de marché en Roumanie. Avec l'acquisition de Samsung Motors, Renault s'implante en Corée du sud, deuxième marché d'Asie.

* * * * *

PREAMBULE

Les enjeux pour R.E.A. sont de centraliser et maîtriser l'administration de ses 10 000 postes de travail répartis dans ses établissements en Europe. Pour parvenir à ces fins, un système informatique stable est en train d'être déployé. Il doit entre autre permettre de :

- réduire le temps d'indisponibilité des postes.
- centraliser, uniformiser, et contrôler la configuration des postes clients.
- sécuriser les données entre les différents utilisateurs.
- remonter les informations critiques par mail (alertes).
- réutiliser les applications existantes.
- permettre l'hébergement des futures applications spécifiques REA.
- maîtriser et optimiser les achats informatiques pour ces entités.
- réutiliser la topologie existante.

Afin de pouvoir bénéficier de toutes ces fonctionnalités, des serveurs ainsi que des postes clients doivent être déployés et paramétrés. Il devient alors nécessaire de mettre en place une méthode d'installation et de configuration commune et rapide pour les serveurs, et pour les quelques 5 000 postes clients répartis sur 140 établissements.

Le projet de déploiement est démarré depuis plusieurs mois, et beaucoup de compétences sont nécessaires pour un tel projet. Le service informatique s'est vu augmenté en personnel (prestataires de services), et j'ai intégré cette phase importante de déploiement alors qu'elle était déjà amorcée. Je connaissais le service informatique avant le commencement de ma formation à Jussieu, car j'avais effectué un remplacement de l'administrateur réseau du siège pendant un mois. Or, je me suis retrouvé dans un contexte de travail bien différent. Il fallait que je me réintègre dans un environnement connu, en prenant en compte les nouvelles orientations.

Pour faciliter ce déploiement, une méthode simple, commune et malléable pour l'installation des ordinateurs doit être mise en place. Mais avec un peu de recul, on se rend vite compte de la complexité d'une telle méthode pour des postes clients de configuration différentes, des besoins particuliers pour chaque utilisateur, et des spécificités des serveurs.

De plus, il devient important de mettre en place un système de gestion de définition de virus, afin de protéger tous les postes de R.E.A. Le choix de l'antivirus à été décidé, mais il faut mettre en place la meilleure stratégie afin de sécuriser et protéger au mieux les ordinateurs.

Mon stage consistait à participer à certaines installations, et en particulier la mise en place d'une protection antivirale à plusieurs niveaux. Il fallait que je commence par connaître le produit Symantec, pour ensuite consacrer mon temps à définir quelle était la méthode la mieux adaptée pour le déploiement sur la future topologie de R.E.A.

* * * * *

LE SYSTEME D'INFORMATION

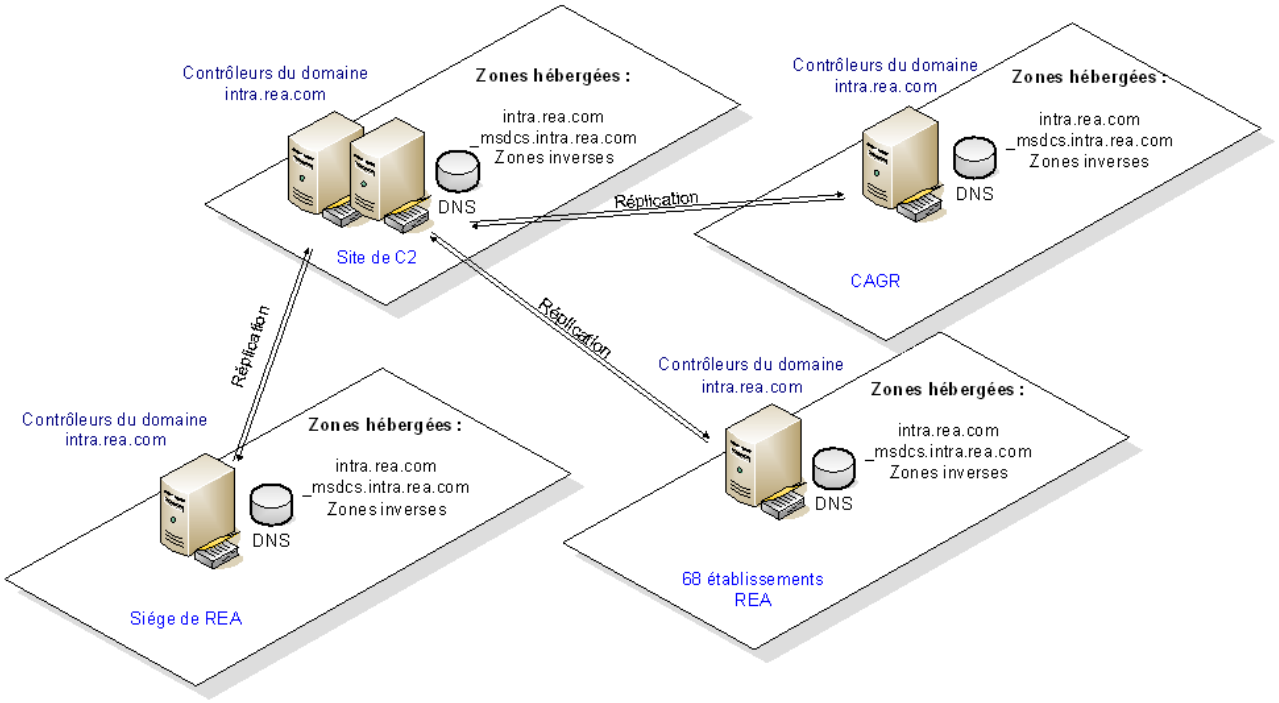
I) Architecture physique

Une architecture centralisée à domaine unique (Intra.rea.com) est répliquée à partir d'un serveur tête de pont (Bridgehead) sur les différents contrôleurs de domaine via Active Directory.

Chaque contrôleur de domaine permet l'authentification des utilisateurs, afin de pouvoir accéder à des données partagées et à des applications hébergées par l'infrastructure. De même, ces serveurs sont synchronisés en se connectant sur un serveur de temps sur internet.

Un service DNS sert à la réplication d'Active Directory, et à la localisation des contrôleurs de domaine lors des phases d'authentification des postes clients. Une délégation de zones est réalisée au sein des serveurs DNS de C2 afin de déléguer la zone intra.rea.com aux serveurs DNS hébergés à C2, au siège de REA et au CAGR.

Répartition des contrôleurs de domaines :
2 contrôleurs de domaine sur le site de C2.
1 contrôleur siège de REA.
2 contrôleurs au CAGR (Centre de service Administratif et de Gestion du Réseau).
68 contrôleurs **à déployer** pour chacun des établissements français.



L'ensemble de ces contrôleurs fait partie d'un arbre, et partagent un espace de nommage commun. Une forêt est un ensemble de domaines qui ne sont pas sous-domaines les un des autres, mais qui sont liés par une relation de confiance bidirectionnelle transitive.

Dans une forêt, il y a au moins cinq rôles FSMO (Flexible Single Master Operations - également appelés *rôles maître des opérations*) qui sont attribués à un ou plusieurs contrôleurs de domaine. Deux rôles FSMO ont autorité sur la forêt et trois existent dans chaque domaine :

Rôles dans une forêt :

Le **contrôleur de schéma** contrôle toutes les mises à jour et les modifications apportées au schéma (définition formelle de tous les types d'objets d'active Directory). Ces modifications sont ensuite répliquées sur tous les contrôleurs de domaine de la forêt.

Le **maître de nom de domaine** contrôle l'ajout ou la suppression de domaines dans la forêt.

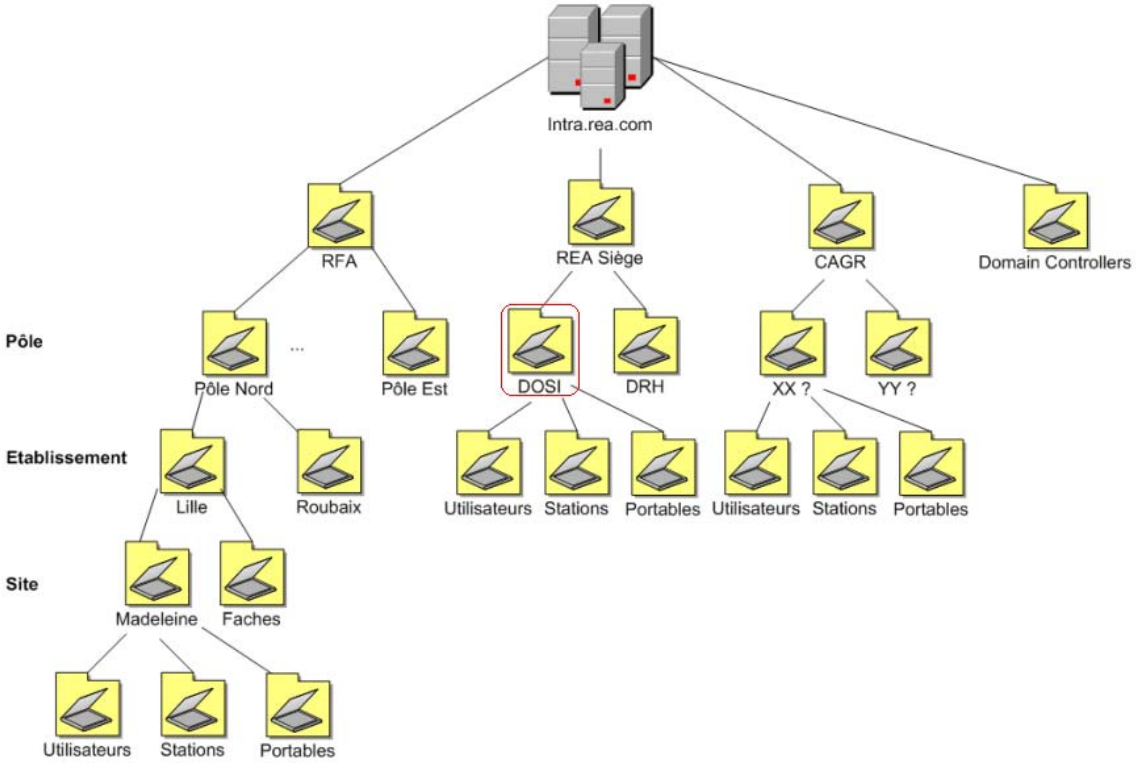
Rôles dans les domaines :

Le **maître d'infrastructure** est responsable de la mise à jour des références des objets de son domaine vers les objets d'autres domaines.

Le **maître RID** (Relative Identifier) est responsable pour un domaine particulier de délivrer des fourchettes d'identifiants de sécurité (SID) aux autres contrôleurs de domaine, et assure le déplacement d'objets entre ces domaines.

L'**émulateur PDC** (Primary Domain Controler) permet de maintenir une compatibilité descendante avec les versions antérieures de Windows (contrôleurs de domaine NT 4.0, postes de travail)

Les sites de REA sont regroupés en OU (Unités d'Organisation).



II) Moyens humains

Chaque établissement de R.E.A. a un correspondant pour l'organisation et les systèmes informatiques (COSI). Un groupe d'établissement constitue un Pôle. Il y a pour chaque pôle un COSI Pôle.

Les COSI sont des employés qui, en plus de leurs fonctions premières, gèrent aussi l'informatique locale des établissements dont ils dépendent. Ils doivent avoir les connaissances nécessaires pour gérer les comptes utilisateurs ainsi que les ressources informatiques partagées. Certaines notions de réseau informatique leur sont utiles pour pouvoir intervenir au niveau des switchs et des routeurs.

Les COSI doivent de même indiquer les besoins en fournitures directement sur l'extranet. Si ces commandes sont validées, elles sont ventilées automatiquement entre les différents fournisseurs, et les différents intervenants sont alertés par des e-mails automatisés et sécurisés.

Les COSI pôle occupent quant à eux la totalité de leur temps de travail à l'informatique. Ils interviennent pour une gestion plus globale sur plusieurs établissements.

Au sein du siège de R.E.A., j'étais intégré à la « DOSI » (Direction de l'Organisation et des Systèmes d'information) pendant la durée de mon stage.

Voici l'équipe avec laquelle j'ai partagé mon trimestre :

Nom	Fonction	Employeur
Abderrahim Hraiba	Responsable micro et réseaux	Prestataire
David Valéro	Support technique au déploiement Windows XP	Prestataire
David Dziesietnik	Coordinateur de projet	Prestataire
Faissel Bessioud	Pilote de domaine technique central	REA
Hugues Salomon	Chargé de projet télécom.	Prestataire
Jean-Louis Ghiglione	Responsable exploitation et infrastructures techniques	REA
Mickael Bataille	Support technique	Prestataire
Nathalie S-D-D	Gestionnaire parc	REA
Patrick Lecuyot	Exploitation et infrastructures techniques systèmes	REA
Pierre Bolot	Gestionnaire parc	REA
Steve Passerotte	Administrateur sécurité, réseaux et données REA	REA
Renaud Rayez	Chef de projet	Prestataire

Comme nous pouvons le constater, le service informatique est constitué autant de personnes internes à R.E.A. que de prestataires externes. Certains des prestataires de services ont intégré notre structure depuis quelques années, d'autres uniquement pour le déploiement.

* * * * *

METHODE DE DEPLOIEMENT

Pour mettre en œuvre une solution intégrant ces paramètres, une solution basée sur des clients Windows XP, des clients légers Windows XP Embedded, et des serveurs Windows 2003 a été retenue.

La quantité des postes à installer est répartie de la façon suivante :

Matériel	Type	Quantité
P.C.	Serveurs	68
P.C.	Desktop (D530)	1 632
P.C.	Laptop	77
Clients légers	NeoWare	1 331
Upgrade	Divers	1 854
Total		**4 962**

L'installation des 5 000 ordinateurs doit être la plus simple et la plus rapide possible. Pour parvenir à ce résultat, une image de base a été créée spécialement pour les postes clients, et une autre pour les serveurs. Ces images sont faites avec sysprep et ghost, pour être déployées sur cédérom, et contiennent les derniers correctifs windows. Une disquette est aussi utilisée pour permettre l'automatisation des paramètres réseau (utilisation de la commande NETSH INTERFACE IP). L'image de cette disquette est générée par DsImage, un outil opensource (http://osplus.sourceforge.net/).

La procédure commune pour l'installation des P.C. est la suivante :

1. Modification des scripts de la disquette pour sysprep.
2. Démarrage de l'ordinateur en bootant sur le premier cédérom du système d'exploitation Windows généré avec Ghost.
3. La copie des partitions système et données commence ; insérer le deuxième cédérom à la fin du premier, pour finaliser cette copie.
4. Redémarrage du système sur la disquette ; SYSPREP prend le relais afin d'automatiser l'installation.

Avant de s'étendre sur l'ensemble des affaires R.E.A, la phase de déploiement a commencé sur deux sites de test (Mantes la jolie et St-Denis) et un site pilote (Orléans).

I) Les clients XP

Un jeu de cédéroms sert à l'installation des systèmes d'exploitation XP. Il doit contenir les dernières versions des pilotes de périphériques des postes déployés parmi les configurations suivantes :

Modèle Machine	Type	Mémoire (Mo)	Taille Disque (Go)	Processeur
HP EVO D530	Desktop	512	40	P4 2,4 GHz
HP EVO D510	Desktop	256	40	P4 2,0 GHz
HP VL420	Desktop	256	20	P4 1,6 GHz
HP EVO N610C	Laptop	256	20	P4m 1,7 GHz
Toshiba SP6000	Laptop	128 + ajout 128 prévu	20	Celeron 1,06 GHz
Toshiba Tecra S1	Laptop	512	40	Centrino 1,4 GHz

Un deuxième jeu de cédérom sera utilisé pour l'installation de programmes additionnels, qui sont paramétrés de manière homogène pour s'intégrer à l'infrastructure réseau. Parmi les applications utilisées, nous avons :

- Office 2000
- un webmail
- un logiciel pour la location de voitures (Renault Rent).
- une gestion des achats/ventes/stocks hébergée par un système unix.
- des logiciels spécifiques vendeurs.
- des applications spécifiques intranet.
- et d'autres applications métier…

L'installation de des différents programmes est automatisée, et se fait par l'intermédiaire d'un simple menu en mode commande. Cependant, malgré une installation simplifiée, il a fallu trouver des moyens pour générer certaines actions automatiques dans windows, pour masquer les mots de passe d'administration des scripts, pour insérer des délais entre les installations de pilotes de périphériques…

En effet, l'installation d'applications telles que « acrobat reader » nécessite une intervention humaine pour spécifier et valider les options dans les menus d'installation. De plus, les mots de passe d'administration ne sont pas divulgués pour les paramétrages et les installations. Enfin, un délai est souvent nécessaire pour que les installations de périphériques ne se fassent pas en parallèle, ce qui cause des problèmes.

Pour palier à ces problèmes, homogénéiser les postes, et accélérer les installations, nous avons utilisé un outil de mémorisation des touches clavier, et des clics de souris. Le programme **AutoIT** (http://www.hiddensoft.com/AutoIt/) permet d'enregistrer les actions effectuées lors d'une installation modèle, de compiler ces enregistrements dans un fichier autonome crypté, et de simuler ces séquences pour les installations futures.

Ce programme permet également de temporiser ces installations, afin qu'elles ne s'exécutent pas toutes en même temps.

II) Les clients XP Embedded

Parallèlement, 1 300 terminaux légers sont également déployés. Leur utilisation limitée permet uniquement l'accès à un applicatif spécifique Renault, à un navigateur web pour l'intranet, et éventuellement à l'édition de factures.

Le matériel utilisé se présente sous la forme d'un boîtier de taille réduite sans disque dur, avec les prises nécessaires pour brancher les périphériques. Le modèle retenu est un Neoware EON ; NeoWare occupant la deuxième place mondiale du marché des terminaux légers.

Le système d'exploitation est réduit au strict minimum, et compressé dans une mémoire flash de 256 Mo. Cette mémoire est en écriture lors de l'installation du système, et en lecture seule une fois l'O.S. transféré. Au moment du démarrage du système, celui-ci est décompressé à la volée.

Windows XP embedded permet de démarrer sur ce type de mémoire, sans avoir à utiliser de fichier d'échange.

Les avantages de ce type de client léger sont multiples :

- ils sont peu onéreux, et peu encombrants.
- l'installation de ces postes peut s'effectuer en parallèle via un hub ou un switch.
- pour redescendre l'image du système sur les clients, l'opération ne prend qu'une dizaine de minutes en 100 Mb.
- il n'y a aucun risque de propagation de virus, si la mémoire est verrouillée.
- le système d'exploitation reste inchangé une fois installé, ce qui garantie une grande fiabilité dans le temps.
- la maintenance après installation est nulle, tant au niveau du système et des applications, qu'au niveau du matériel (boîtiers dépourvus de disque dur, lecteur de disquette, CD-Rom, et ventilateur).
- les ressources matérielles recommandées sont modestes, et un processeur à 500 Mhz équipé de 256 Mo de RAM suffisent.

III) Les contrôleurs de domaine

Les caractéristiques des serveurs permettant ces services sont les suivantes :

Composants	Type	Quantité
Système	Windows 2003 Server	1
Processeur	2,8 Ghz	2
Mémoire vive	DDR 400	1 Go
Disques	Serial ATA	2 de 80 Go
Contrôleur disques	RAID 1	1
Carte réseau	Gigabit	2
Unité de sauvegarde	Externe SCSI	1 x 40/80 Go

Active Directory est un annuaire, les informations qu'il contient sont enregistrées dans une base de donnée, modélisée sous la forme d'un seul fichier (%systemroot%\NTDS\ntds.dit). L'extension de ce fichier (DIT), signifie Directory Information Tree. Cette base de données est basée sur la base ESE (Extensible Storage Engine), créée à l'origine pour Microsoft Exchange Server. Elle peut stocker plusieurs millions d'objets, et atteindre une taille maximale théorique de 70To.

La structure de l'annuaire de R.E.A. est amenée à évoluer au cours du temps. Une sauvegarde quotidienne sur chaque serveur est planifiée, pour le système et les données. Pour limiter les éventuelles surcharges des disques, un quota de 500 Mo est mis en place pour chaque dossier utilisateur.

IV) Qualipark

Renault Europe Automobiles utilise une solution logicielle pour inventorier ses ordinateurs, ses imprimantes, ainsi que les applications, les licences achetées, déployées et disponibles.

Qualiparc Asset Management est une puissante application permettant d'avoir une vision globale et une gestion centralisée du parc informatique en temps réel.

QP Discovery est un module de Qualipark, et permet d'inventorier les équipements et logiciels. La collecte de ces informations s'effectue automatiquement au travers le réseau et récupère les informations techniques, matérielles et logicielles des postes de travail. Le processus d'inventaire, invisible pour les utilisateurs, est déployé sur tous les postes et est réalisé au démarrage des stations. Son utilisation peut de même être planifiée.

Discovery dispose d'un "requêteur" pour consulter et classer les informations collectées afin de simplifier chaque recherche. Ces informations sont centralisées sur une base de donnée Oracle 8i.

La mise en œuvre et le fonctionnement de Qualipark peuvent être totalement centralisés en environnement Windows NT/2000/XP.

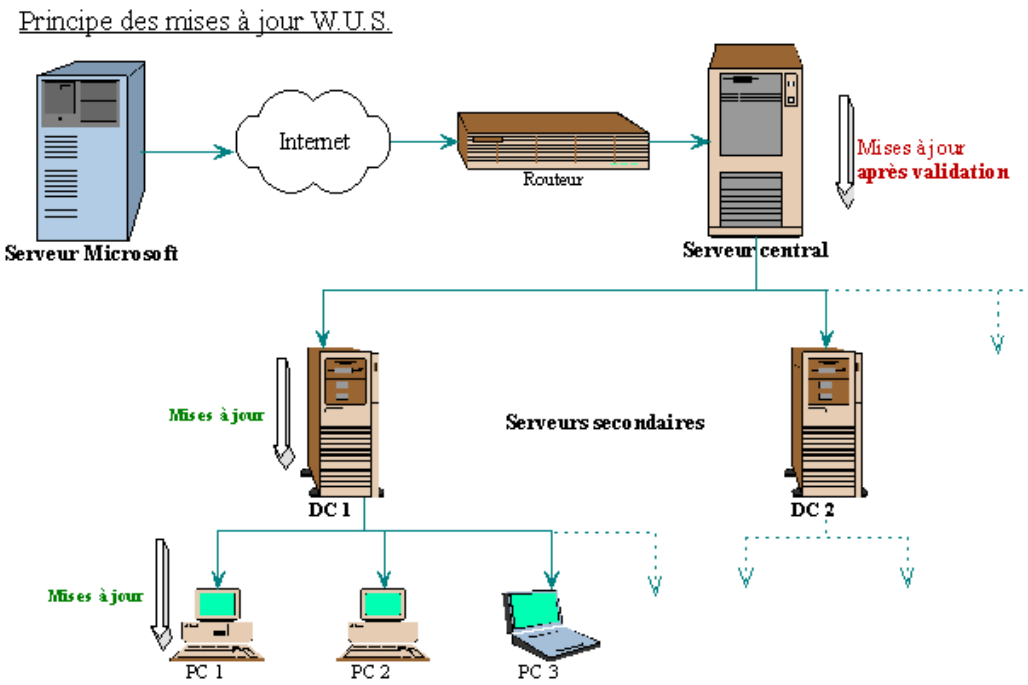
L'avantage d'un tel outil est de pouvoir suivre et contrôler les différentes évolutions des postes de travail. Il peut aussi être utilisé pour surveiller les logiciels installés afin de gérer les licences ou prévenir les risques.

V) Les mises à jour

Afin de sécuriser les ordinateurs, une solution de déploiement des patchs de sécurité est à l'étude. Les mises à jour critiques ne peuvent être installées par les utilisateurs, car elles requièrent un droit d'administrateur sur les P.C.

Une solution Microsoft, baptisée W.U.S. (Windows Update Services) permet le téléchargement des dernières mises à jour à partir du site Windows Update, et l'installation de ces patchs, suite à l'approbation et la validation de l'administrateur.

Voici un schéma de mise en œuvre du principe de validation et de déploiement des patchs :



Nous avons testé la version précédente de WUS (S.U.S. SP1), afin de comprendre la philosophie d'administration. Dans les semaines qui vont suivre, il est prévu d'installer ce principe de mise à jour pour l'ensemble des postes de R.E.A.

Concernant les autres mises à jour, j'avais la charge de tester le système antivirus Symantec Antivirus Corporate Edition.

* * * * *

DEPLOIEMENT ANTIVIRUS

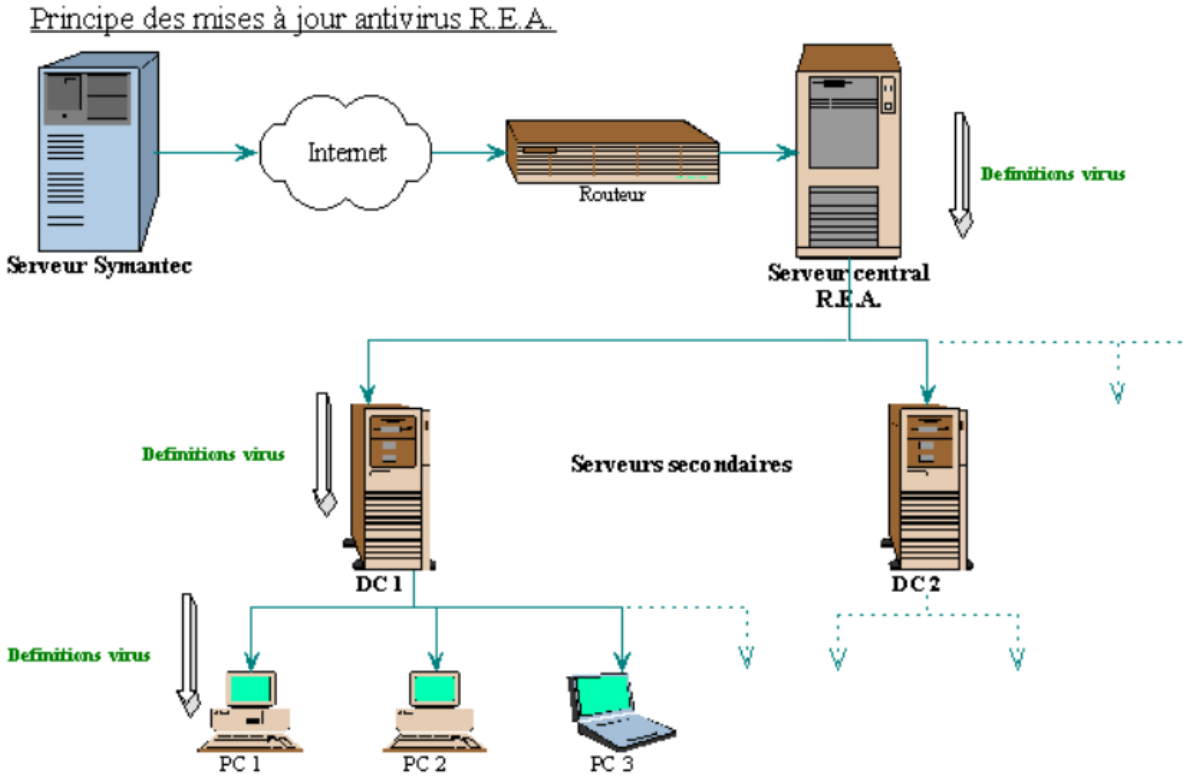
I) L'existant

Les ordinateurs ont été livrés avec la version Symantec Corporate Edition. Cette version antivirale assure :

- une solution complète pour protéger tous les niveaux du réseau (serveurs, passerelles de messagerie, et postes de travail).
- une gestion centralisée facilitant l'installation et l'administration.
- une gestion de groupes logiques pour les postes de travail et les serveurs.
- une mise à jour automatique des définitions de virus.
- la mise à jour les définitions de virus et les améliorations de moteur sans avoir à redémarrer le serveur.
- la possibilité de créé, modifier et déployer des paquets d'installation msi.
- une optimisation de la bande passante du réseau, grâce à une distribution paramétrable des définitions de virus par technologie « push ».

II) Les objectifs

Le principe adopté est d'utiliser un serveur primaire pour télécharger les mises à jour (premier niveau). Ce serveur mettrait à jour les autres contrôleurs de domaines distants (niveau 2), qui eux-mêmes assureraient les redescentes des nouvelles définitions sur les postes clients (niveau 3).



Les mises à jour sont programmables, et le serveur primaire est paramétré pour chercher les mises à jour à 6h le matin (après les sauvegardes). Les serveurs secondaires, quant à eux, vont chercher ces mises à jour une demi-heure plus tard. Les postes clients se mettent à jour lors de la connexion au réseau.

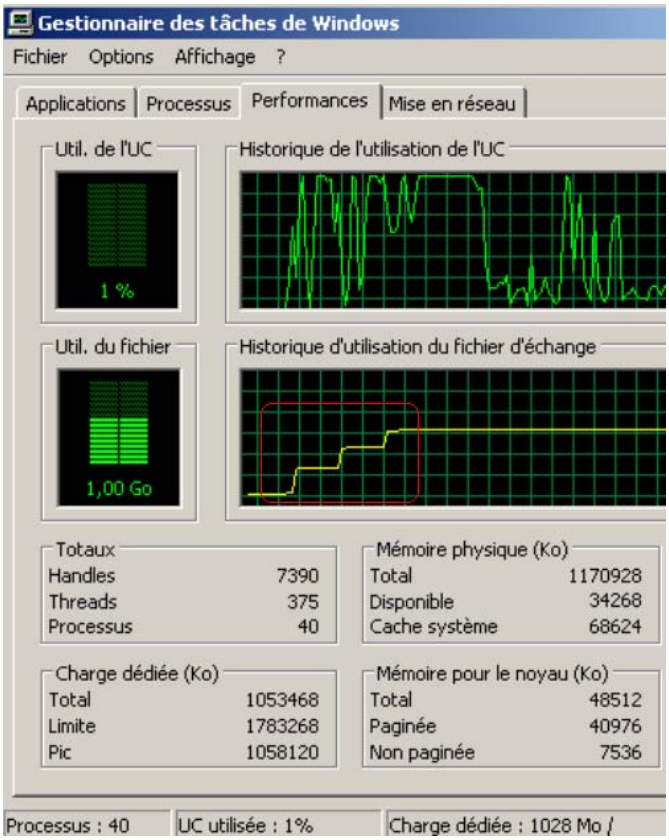
III) Le réseau virtuel

Symantec antivirus corporate edition s'avère être l'outil minimum pour protéger un parc informatique. En pratique, une installation telle qui a été effectué chez R.E.A. est compliquée, car les méthodes d'installation sont diverses, et certaines ne sont pas fonctionnelles.

Une des tâches que je devais effectuer était de définir une procédure d'installation pour le serveur principal, les 70 contrôleurs de domaines, et les postes clients.

Afin de ne pas tester ces différentes méthodes d'installation et de configuration dans l'environnement existant, j'ai utilisé un poste avec windows XP avec 1,2 Go de mémoire vive, et VmWare GSX Server 3.0. Les machines virtuelles que j'ai installées sont un serveur windows 2003 maître, un serveur windows 2003 secondaire, et un client windows XP pro.

Cet environnement de test fut idéal, car il ne nécessite pas d'ordinateur supplémentaire, et il permet de s'isoler du réseau réel. Par contre, l'ordinateur hôte à besoin d'un processeur rapide et d'une quantité de mémoire vive disponible importante. En effet, chacune des trois machines est configurées avec 256 Mo, et l'hôte fonctionne avec lui aussi 256 Mo. Nous pouvons voir ci-dessous l'occupation par palier du fichier d 'échange, quand les trois machines virtuelles sont démarrées.



La première méthode que j'ai testée fut d'installer le serveur principal, de créer des packages MSI pour les serveurs secondaires, et les postes clients.

Cette méthode fonctionnait bien dans le réseau virtuel, mais dans l'environnement de R.E.A. les mises à jour n'étaient pas redescendues par le serveur principal (méthode PUSH).

J'ai de ce fait cherché une autre solution, et je me suis rendu compte qu'un fichier de configuration permettait aux postes clients de se connecter aux serveurs, avec les paramètres adéquats. La méthode finalement utilisée pour déployer les clients antivirus consiste à copier ce fichier dans un dossier d'installation de Symantec.

Afin de mettre ce fichier sur les postes clients, nous aurions pu ajouter une commande de copie au script de login des utilisateurs. Or certains ordinateurs portables ne font pas partie du domaine, et d'autres ont une installation qui diffère (l'antivirus est installé soit sur le lecteur C, soit sur le D). C'est pourquoi nous avons demandé à chaque COSI de placer ce fichier sur chaque ordinateur. De ce fait, cela nous permettait aussi d'être sûr qu'aucun poste ne soit oublié.

Pour faciliter la tâche des COSI, j'ai utilisé le programme AutoIT (voir page 9). Le script qui a été créé permet de :

- extraire le fichier de configuration GRC.DAT et GRC.REG.
- ouvrir une console sous le profil administrateur avec RUNAS.
- copier le fichier GRC.DAT dans un dossier accessible uniquement par un administrateur (\Documents and Settings\All Users\...).
- arrêter et redémarrer le service antivirus pour intégrer les paramètres du fichier GRC.DAT.
- fusionner le fichier GRC.REG dans la base de registre.
- effacer les fichiers extraits.
- quitter la console.

SCRIPT D'INSTALLATION CLIENTS ANTIVIRUS

```
; AutoIt Version: 3.0
;
; Script d'installation des paramétrages Symantec Antivirus pour les postes clients.
; Renault Europe Automobiles - Juin 2004

; Définition du dossier temporaire
$Dossier=@TempDir

; Extraction des fichiers de configuration dans le dossier temporaire
FileInstall ("GRC.DAT",$Dossier & "\GRC.DAT")
FileInstall ("GRC.REG",$Dossier & "\GRC.REG")

; Délai clavier
AutoItSetOption ("SendKeyDelay",2)
Sleep(150)

; On lance une console en mode admin
Run("RunAs /noprofile /user:INTRAREA\Admin C:\WINDOWS\SYSTEM32\CMD.EXE", "", )
Sleep(500)

; Mot de passe admin crypté après compilation de script
Send("@dminAV{ENTER}")
Sleep(500)
```

```
...


; Copie GRC.DAT dans le dossier Symantec
Send("COPY " & $Dossier & "\GRC.DAT" & CHR(34) & "D:\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus Corporate Edition\7.5\" & CHR(34) & "\Y")
Sleep(250)
Send("{ENTER}")
Sleep(250)

; Fusionne GRC.REG dans la base de registres
Send("REGEDIT /s " & $Dossier & "\GRC.REG")
Sleep(250)
Send("{ENTER}")
Sleep(250)

; Arrêt du service antivirus
Send("NET STOP " & CHR(34) & “Symantec AntiVirus Client" & CHR(34))
Sleep(250)
Send("{ENTER}")
Sleep(250)

; Redémarrage du service antivirus pour intégration du GRC.DAT
Send("NET START " & CHR(34) & “Symantec AntiVirus Client" & CHR(34))
Sleep(250)
Send("{ENTER}")
Sleep(250)

; Suppression des fichiers temporaires de configuration
FileDelete ($Dossier & "\GRC.*")
Sleep(250)

; Fermeture de la console
Send("EXIT{ENTER}")
Sleep(300)
```

Les avantages d’un tel script sont multiples. Un seul double clic suffit pour effectuer les actions nécessaires pour la mise en place des paramétrages corrects, sans avoir besoin de donner les droits d’administration. Seules quelques petites secondes suffisent pour cette opération, et il est ensuite aisé de vérifier si le poste client pointe sur le bon serveur (à partir de la console serveur). Après quelques essais concluants, c’est cette méthode qui a été utilisée pour installer les machines de production.

Pour le déploiement du réseau R.E.A. j’ai rédigé une procédure d’installation complète et validée (voir annexe de ce présent rapport, *Méthode d’installation de Norton Antivirus Corporate Edition 8.1*).

* * * * *

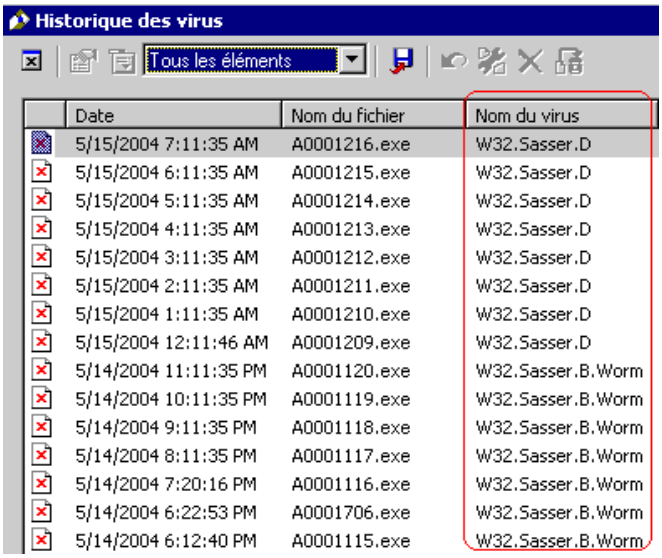
ADMINISTRATION
DES SERVEURS ANTIVIRUS

I) Journal d'un serveur

L'administration des serveurs implique une surveillance minutieuse des journaux d'activité de ces derniers. Toutes les informations concernant les infections des postes clients et des serveurs sont centralisées sur le serveur central. Nous pouvons ainsi visualiser l'état d'un groupe d'ordinateurs, comme illustré ci-dessous :

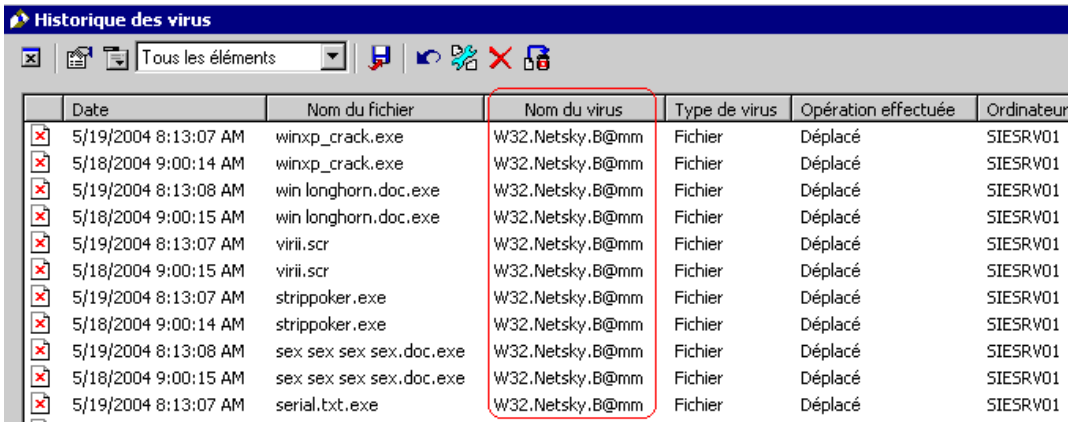
Client	Utilisateur	Groupe	Etat
MAS2NET1	a197548	MASNET	Virus détecté !
MAS2NET4	a386399	MASNET	Hors ligne
MASNET12	a961612	MASNET	Virus détecté !
MASNET14	mig	MASNET	Virus détecté !
MASNET15	a975592 (déconnecté)	MASNET	Virus détecté !
MASNET16	User	MASNET	Virus détecté !
MASNET17	a398873	MASNET	Virus détecté !
MASNET18	a972725	MASNET	Virus détecté !
MASNET19	a392829	MASNET	Virus détecté !
MASNET20	comptainterim	MASNET	Virus détecté !
MASNET21	a963358	MASNET	
MASNET23	a391972	MASNET	Virus détecté !
MASNET24	a387097	MASNET	Virus détecté !
MASNET25	a395780	MASNET	Virus détecté !
MASNET26	a972576	MASNET	Virus détecté !
MASNET27	a386935	MASNET	Hors ligne
MASNET28	a964460	MASNET	Virus détecté !
MASNET2	a389993	MASNET	Virus détecté !
MASNET30	a976864	MASNET	Virus détecté !
MASNET31	a378458	MASNET	Virus détecté !
MASNET32	a378458	MASNET	Virus détecté !
MASNET35	a381766	MASNET	Hors ligne
MASNET39	a853541	MASNET	Virus détecté !
MASNET3	a974129	MASNET	Virus détecté !
MASNET40	a392027	MASNET	Virus détecté !
MASNET43	a389969	MASNET	Virus détecté !
MASNET44	a961783	MASNET	Virus détecté !
MASNET45	a379481	MASNET	Virus détecté !
MASNET46	a963258	MASNET	Virus détecté !
MASNET47	a966209	MASNET	Virus détecté !
MASNET48	a856170	MASNET	Virus détecté !

De même, il est possible d'isoler les informations d'un seul serveur, afin de pouvoir prendre les mesures nécessaires en cas d'infection. En effet, chaque serveur peut être victime d'une contamination spécifique. Par exemple un premier serveur peut être principalement infecté par le virus Sasser.



Date	Nom du fichier	Nom du virus
5/15/2004 7:11:35 AM	A0001216.exe	W32.Sasser.D
5/15/2004 6:11:35 AM	A0001215.exe	W32.Sasser.D
5/15/2004 5:11:35 AM	A0001214.exe	W32.Sasser.D
5/15/2004 4:11:35 AM	A0001213.exe	W32.Sasser.D
5/15/2004 3:11:35 AM	A0001212.exe	W32.Sasser.D
5/15/2004 2:11:35 AM	A0001211.exe	W32.Sasser.D
5/15/2004 1:11:35 AM	A0001210.exe	W32.Sasser.D
5/15/2004 12:11:46 AM	A0001209.exe	W32.Sasser.D
5/14/2004 11:11:35 PM	A0001120.exe	W32.Sasser.B.Worm
5/14/2004 10:11:35 PM	A0001119.exe	W32.Sasser.B.Worm
5/14/2004 9:11:35 PM	A0001118.exe	W32.Sasser.B.Worm
5/14/2004 8:11:35 PM	A0001117.exe	W32.Sasser.B.Worm
5/14/2004 7:20:16 PM	A0001116.exe	W32.Sasser.B.Worm
5/14/2004 6:22:53 PM	A0001706.exe	W32.Sasser.B.Worm
5/14/2004 6:12:40 PM	A0001115.exe	W32.Sasser.B.Worm

Alors qu'un autre serveur peut lui avoir été touché par le virus Netsky…



Date	Nom du fichier	Nom du virus	Type de virus	Opération effectuée	Ordinateur
5/19/2004 8:13:07 AM	winxp_crack.exe	W32.Netsky.B@mm	Fichier	Déplacé	SIESRV01
5/18/2004 9:00:14 AM	winxp_crack.exe	W32.Netsky.B@mm	Fichier	Déplacé	SIESRV01
5/19/2004 8:13:08 AM	win longhorn.doc.exe	W32.Netsky.B@mm	Fichier	Déplacé	SIESRV01
5/18/2004 9:00:15 AM	win longhorn.doc.exe	W32.Netsky.B@mm	Fichier	Déplacé	SIESRV01
5/19/2004 8:13:07 AM	virii.scr	W32.Netsky.B@mm	Fichier	Déplacé	SIESRV01
5/18/2004 9:00:15 AM	virii.scr	W32.Netsky.B@mm	Fichier	Déplacé	SIESRV01
5/19/2004 8:13:07 AM	strippoker.exe	W32.Netsky.B@mm	Fichier	Déplacé	SIESRV01
5/18/2004 9:00:14 AM	strippoker.exe	W32.Netsky.B@mm	Fichier	Déplacé	SIESRV01
5/19/2004 8:13:08 AM	sex sex sex sex.doc.exe	W32.Netsky.B@mm	Fichier	Déplacé	SIESRV01
5/18/2004 9:00:15 AM	sex sex sex sex.doc.exe	W32.Netsky.B@mm	Fichier	Déplacé	SIESRV01
5/19/2004 8:13:07 AM	serial.txt.exe	W32.Netsky.B@mm	Fichier	Déplacé	SIESRV01

Et pour un troisième exemple, il est possible d'avoir d'autres familles de virus et vers en touts genres !

Date	Nom du fichier	Nom du virus
5/17/2004 5:07:51 PM	Q666777.exe	Download.Trojan
5/17/2004 5:07:51 PM	ai02776.vcf.scr	W32.Bugbear.B@mm
5/17/2004 5:07:51 PM	ai02776.vcf.scr	W32.Bugbear.B@mm
5/17/2004 5:07:50 PM	ai02776.vcf.scr	W32.Bugbear.B@mm
5/17/2004 5:07:50 PM	ai02776.vcf.scr	W32.Bugbear.B@mm
5/17/2004 5:07:50 PM	ai02776.vcf.scr	W32.Bugbear.B@mm
5/17/2004 5:07:50 PM	juqfgg.zip	W32.Mydoom.A@mm
5/17/2004 5:07:50 PM	juqfgg.zip	W32.Mydoom.A@mm
5/17/2004 5:07:50 PM	readme.zip	W32.Mydoom.A@mm
5/17/2004 5:07:49 PM	ai02776.vcf.scr	W32.Bugbear.B@mm
5/17/2004 5:07:50 PM	juqfgg.pif	W32.Mydoom.A@mm
5/17/2004 5:07:50 PM	juqfgg.pif	W32.Mydoom.A@mm
5/17/2004 5:07:50 PM	readme.t…	W32.Mydoom.A@mm
5/17/2004 4:41:39 PM	avserve2.exe	W32.Sasser.B.Worm
5/17/2004 4:41:39 PM	9045_up.exe	W32.Sasser.B.Worm
5/17/2004 4:41:39 PM	7129_up.exe	W32.Sasser.B.Worm

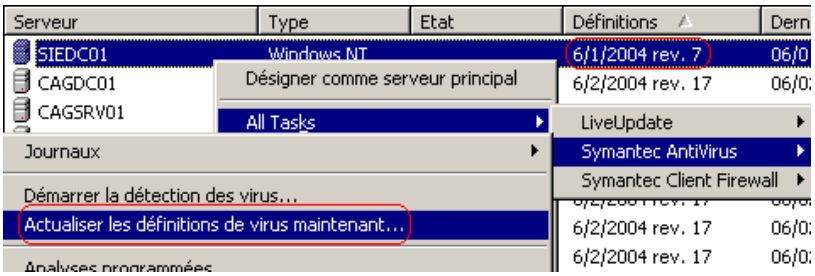
Pour chaque type de virus, il existe une parade à mettre en oeuvre en cas d'infection. Concernant le virus Sasser, la méthode ci-dessous est recommandée par Symantec :

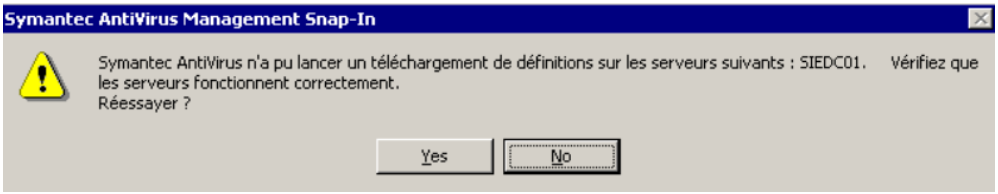
Si votre PC est infecté :

5. Commencez par faire un petit Ctrl+Alt+Del pour ouvrir le gestionnaire de taches.
6. Cliquez sur l'onglet processus, puis terminez le processus avserve.exe ainsi que tout processus portant un nom composé de 5 chiffres suivi de _up.exe (exemple : 74354_up.exe). Cela doit éviter les redémarrages intempestifs durant la désinfection.
7. Installez le patch de sécurité qui va bien, via Windows update ou en manuel.
8. Téléchargez l'outil de suppression de Sasser de Symantec.
9. Fermez tous les programmes en cours.
10. Déconnectez-vous d'Internet.
11. Désactivez le système de restauration de Windows XP.
12. Lancez l'utilitaire FXSasser.exe que vous avez téléchargé. Cet outil supprime les fichiers W32.sasser, et nettoie la base des registres.

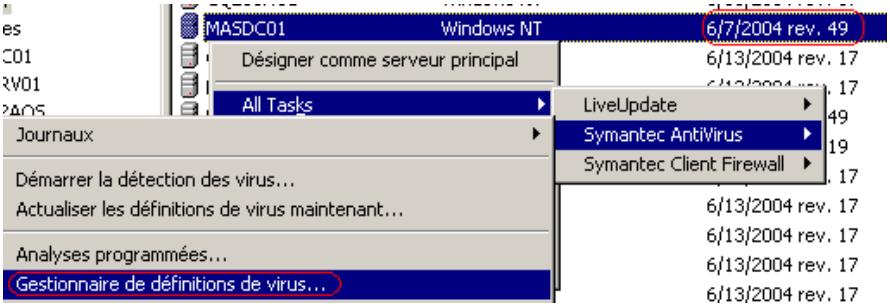
II) Problèmes rencontrés

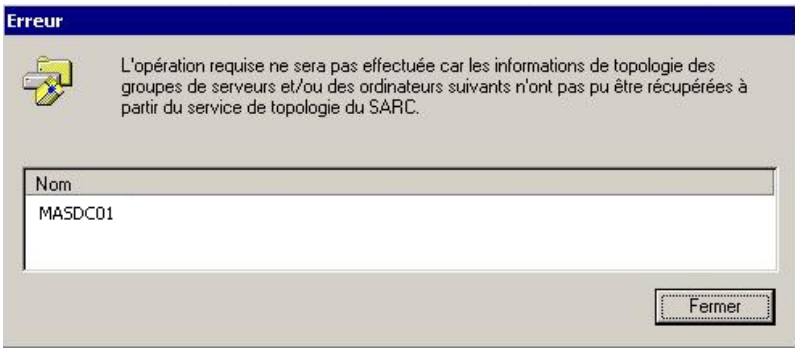
Pendant le début de la période de test, il était fréquent que les serveurs installés avec windows 2003 ne transmettent pas les mises à jour automatiquement.





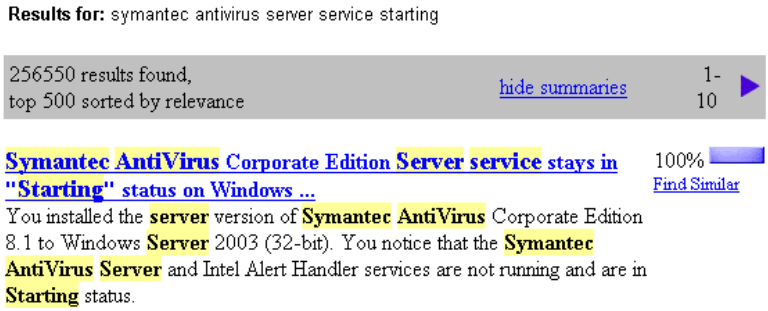
Il semblait qu'un problème de communication entre les ordinateurs subsistait, sans pour autant avoir de message d'erreur sur la console.





Ce n'était jamais tous les serveurs en même temps qui bloquaient, mais un de temps en temps, de façon aléatoire. Nous nous sommes rendu compte que les serveurs concernés avaient subi un redémarrage à chaud. En se rendant dans la liste des services du système d'exploitation, on s'est aperçu que le service « Symantec Antivirus Server » était en cours de démarrage, mais qu'il ne démarrait jamais !

Le problème est connu de Symantec, et la solution est expliquée sur le site de l'éditeur.



Pour remédier au problème, il faut installer une nouvelle version de pilote. La procédure est expliquée ci-dessous :

Procédure de mise à jour du pilote Symantec

Situation :
You installed the server version of Symantec AntiVirus Corporate Edition 8.1 to Windows Server 2003 (32-bit). You notice that the Symantec AntiVirus Server and Intel Alert Handler services are not running and are in "Starting" status.

Solution :
Most often this issue has been reported with Symantec AntiVirus Server 8.1 build 825 and 8.1.1 build 314 installed on Windows 2003 (32-bit) Server. Symantec is investigating this problem to determine a solution. This document will be updated when new information or a solution is available.

Temporary workaround

The following workaround has resolved this issue in some situations:

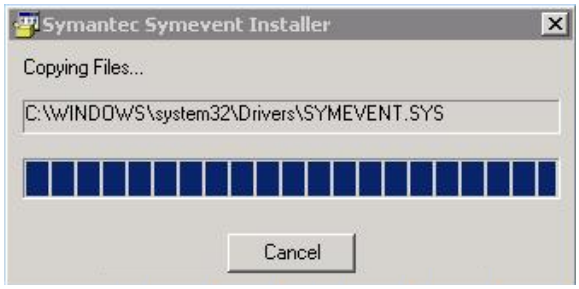
1. Uninstall Symantec AntiVirus Server and AMS Server.
2. Install the latest Windows critical updates and security patches using Windows Update.
3. Reinstall the Symantec AntiVirus Server and AMS Server.
4. Restart the computer.
5. Install the latest Symevent drivers (see the next section).

Note: Alternately, designate a different server, uninstall the server and AMS Server, and install the client version on that computer.

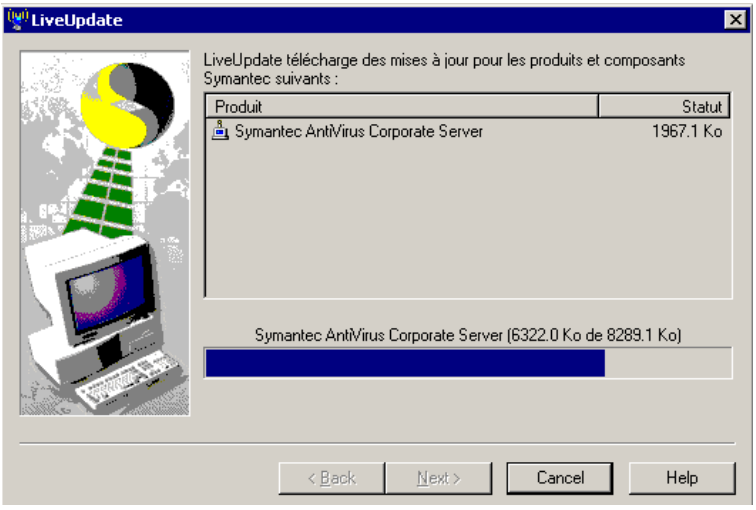
To install the latest Symevent drivers

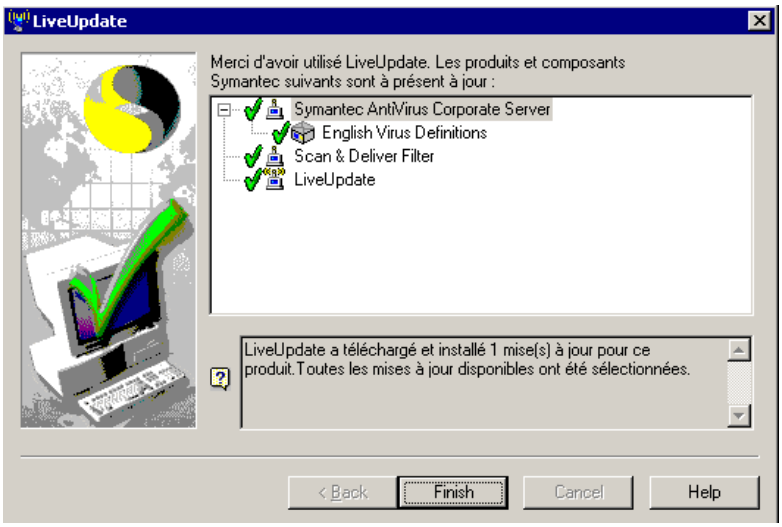
1. Download the Symevent installer, Sevinst.exe, from the Symevent download page.
2. On the Windows taskbar, click Start > Run.
3. Click Browse to locate the Sevinst.exe file that you downloaded.
4. In the Open box, type NAVNT after the existing command line.
   For example, if you downloaded the Sevinst.exe file to C:\Temp, the command line should be:
   C:\Temp\Sevinst.exe NAVNT
5. Click OK.
6. Restart the computer.

La mise à jour du pilote se fait rapidement et sans problèmes particuliers, comme en témoignent les captures d'écran suivantes :



Au terme de cette mise à jour, le service Symantec démarre enfin, et les mises à jour s'effectuent normalement.





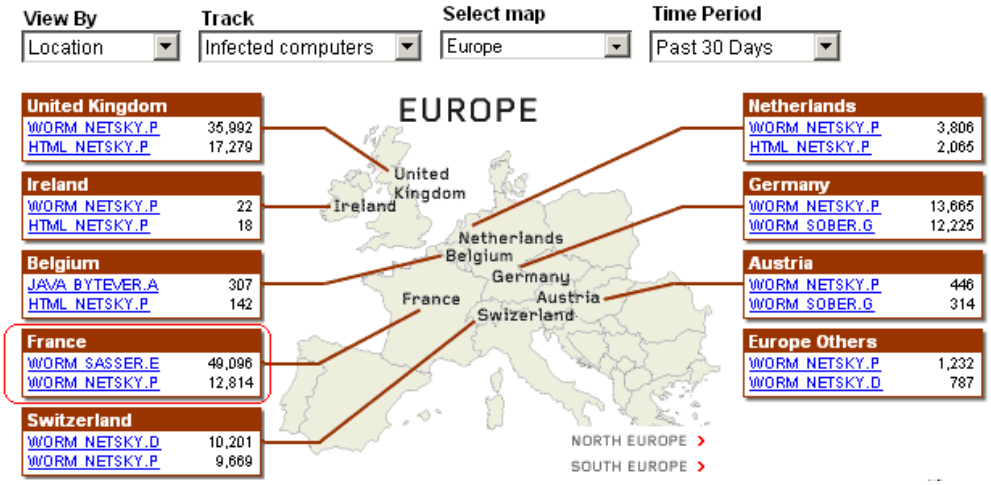
Nous nous rendons compte qu'un outil aussi important et vital dans une société qu'un antivirus peut avoir des bugs. En cas de blocage, il est impératif d'intervenir rapidement afin de sécuriser l'ensemble des ordinateurs. C'est d'ailleurs l'un des principaux rôles de tout administrateur système.

* * * * *

SURVEILLANCE DES POSTES CLIENTS

Les ordinateurs destinés aux utilisateurs sont très vulnérables. Ils le sont d'autant plus en fonction des habitudes de chacun. En effet, il y a des comportements dangereux, comme le fait d'ouvrir une pièce jointe d'un mail dont on ne connaît pas l'expéditeur, échanger des disquettes, visiter des sites internet peu fréquentables… Les ordinateurs portables sont aussi un moyen privilégié de détourner les systèmes de sécurité existants dans les entreprises.

En consultant la carte des postes vérolés en Europe depuis un mois, on se rend compte que la France détient la palme d'or, avec près de 50 000 infections pour le virus Sasser, et près de 13 000 infections pour Netsky.



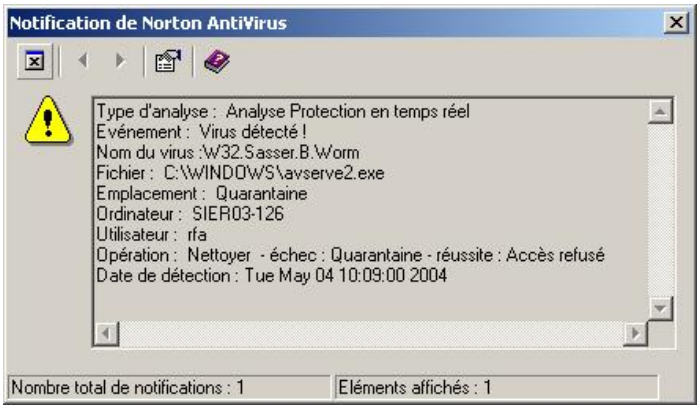
© Trend micro

Le réseau R.E.A. n'a pas échappé à cette propagation rapide et en masse de ces virus. Voici ce que j'ai pu constater lors de mon stage…

I) Le virus Sasser

Lors de la première phase de déploiement, R.E.A. fut victime du virus Sasser. Un lundi 3 mai 2004, à la première heure, presque la totalité des postes furent vérolés. En effet, aucune protection n'a été mise en place (le pare-feu de windows n'est pas actif par défaut), et les directives préconisant la déconnexion physique au réseau n'ont pas été suivies dans tous les établissements.

Le programme antivirus n'était pas capable de nettoyer le fichier infecté avec les définitions de la semaine précédente. Tout ce qu'il pouvait faire était de le placer en quarantaine.

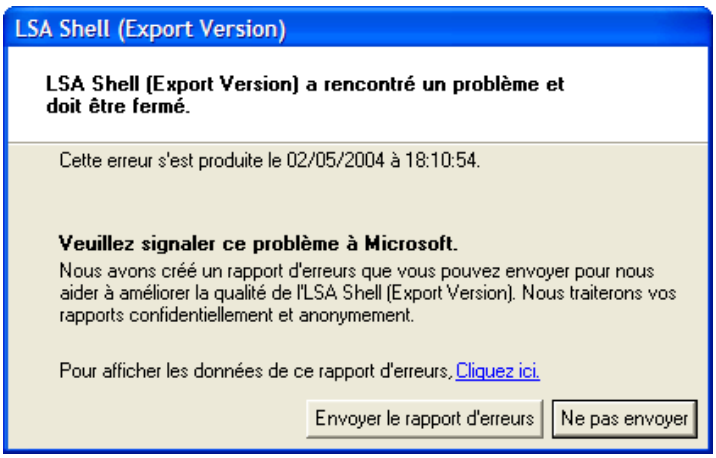


Le ver Sasser qui réussi à s'exécuter sur un ordinateur non protégé se copie sur %Windir%\Avserve2.exe, et dans le répertoire système sous un nom variable xxxx_up.exe. Il s'auto-installe à chaque démarrage de la machine après avoir ajouté la valeur "avserve2.exe"="%Windir%\avserve2.exe" à la clé de registre HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.

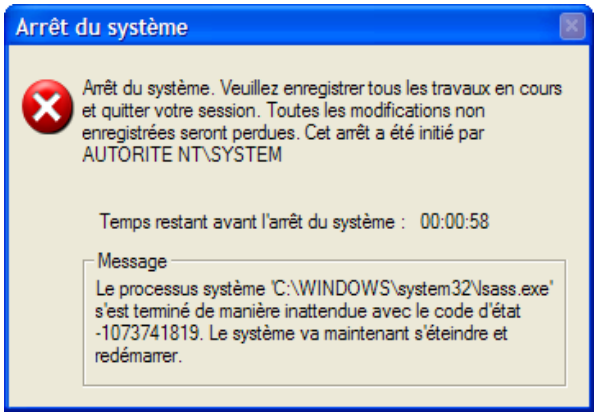
De plus, il utilise l'API "AbortSystemShutdown" afin d'empêcher les tentatives d'arrêt ou de redémarrage de l'ordinateur.

Afin de se propager sur d'autres hôtes, il démarre un serveur FTP sur le port TCP 5554, et tente de se connecter à des adresses IP générées de façon aléatoire sur le port TCP 445 (utilisé par windows pour les échanges de fichiers par le protocole SMB). Cela a eu comme effet de saturer la charge processeur des machines, car pas moins de 128 processus sont actifs pour chercher des adresses IP disponibles.

Ce virus provoque un dépassement de mémoire tampon dans LSASRV.DLL, une DLL du service Lsass.exe (**L**ocal **S**ecurity **A**uthority **S**ubsystem **S**ervice) des systèmes windows XP, 2000, et 2003. Cette vulnérabilité a été annoncée le 13/04/04 par Microsoft, et deux semaines plus tard cette faille a été exploitée.

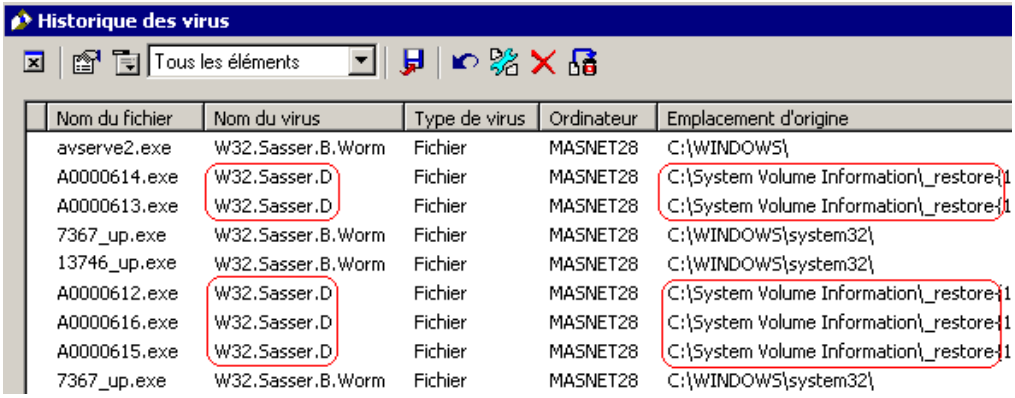


Parmi les autres effets néfastes, le virus redémarre après une minute les postes infectés. Le compte à rebours commence à l'apparition de la fenêtre suivante :



Il fallait appliquer d'urgence les mises à jour du service LSASS et Symantec, afin que les utilisateurs puissent à nouveau exploiter les ressources partagées, et travailler sans fermetures intempestives de leurs postes.

En attendant les mises à jour des ordinateurs, il est possible de désactiver le ver en arrêtant son service (avserve.exe ou avserve2.exe, selon la version du virus). Il est aussi efficace d'activer le pare-feu de windows. Une fois les mises à jour effectuées, un nettoyage de l'ordinateur concerné s'imposait. Un outil permet d'éliminer les fichiers vérolés en scannant les fichiers et la base de registre. Toutefois, il faut désactiver la restauration du système avant de l'utiliser, afin qu'il soit possible d'accéder au dossier système des points de restauration. En effet, nous pouvons constater ci-dessous que la version D de ce ver se trouve à l'emplacement C:\System Volume Information\.



Nom du fichier	Nom du virus	Type de virus	Ordinateur	Emplacement d'origine
avserve2.exe	W32.Sasser.B.Worm	Fichier	MASNET28	C:\WINDOWS\
A0000614.exe	W32.Sasser.D	Fichier	MASNET28	C:\System Volume Information_restore{1
A0000613.exe	W32.Sasser.D	Fichier	MASNET28	C:\System Volume Information_restore{1
7367_up.exe	W32.Sasser.B.Worm	Fichier	MASNET28	C:\WINDOWS\system32\
13746_up.exe	W32.Sasser.B.Worm	Fichier	MASNET28	C:\WINDOWS\system32\
A0000612.exe	W32.Sasser.D	Fichier	MASNET28	C:\System Volume Information_restore{1
A0000616.exe	W32.Sasser.D	Fichier	MASNET28	C:\System Volume Information_restore{1
A0000615.exe	W32.Sasser.D	Fichier	MASNET28	C:\System Volume Information_restore{1
7367_up.exe	W32.Sasser.B.Worm	Fichier	MASNET28	C:\WINDOWS\system32\

Après un nettoyage, nous pouvons avoir un compte-rendu des opérations effectuées :

SASSER.LOG

```
C:\System Volume Information: (not scanned)
C:\WINDOWS\system32\11489_up.exe: (deleted)


C:\System Volume Information: (not scanned)
C:\WINDOWS\system32\11489_up.exe: (deleted)
C:\WINDOWS\system32\12696_up.exe: (deleted)
C:\WINDOWS\system32\13746_up.exe: (deleted)
.
.
C:\WINDOWS\system32\8121_up.exe: (deleted)
C:\WINDOWS\system32\9497_up.exe: (deleted)

W32.Sasser.Worm has been successfully removed from your computer!

Here is the report:
The total number of the scanned files: 28635
The number of deleted files: 98
The number of viral processes terminated: 1
The number of registry entries fixed: 1
```

Si une connexion est établie sur un ordinateur, le ver envoie un shellcode à cet ordinateur, ce qui peut provoquer l'exécution d'un shell distant sur le port TCP 9996.

Le ver utilise alors le shell pour pousser l'ordinateur à se reconnecter au serveur FTP sur le port 5554 et récupérer une copie du ver. Cette copie portera un nom composé de quatre ou cinq chiffres suivis de _up.exe (par ex. : 74354_up.exe).

Nous nous sommes trouvés face à un virus qui a pu se déployer très rapidement, sans aucune action de la part des utilisateurs. En effet, contrairement à la majorité des vers qui se propagent via l'ouverture des pièces jointes des courriers électroniques, celui-ci ne demande qu'une connexion internet pour s'installer.

II) Le ver Netsky

Ce virus est capable de se propager par mail, de la version 95 de windows jusqu'à la dernière version XP. Il s'est aussi propagé très rapidement dans nos locaux.

- Cas de la version B

Après ouverture de la pièce jointe du mail, il se copie comme %Windir%\services.exe. Afin de s'auto démarrer, il ajoute la valeur "service" = "%Windir%\services.exe -serv" dans la clé : HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Ensuite, il essaie de se diffuser dans les dossiers partagés nommés "Share" ou "Sharing". Pour finir, il recherche les adresses mail qui se situent dans les fichiers de l'ordinateur infecté, afin de se propager grâce à son propre moteur SMTP.

Remarques :

- le virus peut usurper l'adresse de la personne infectée pour se propager, ce qui peut « endormir les soupçon » du destinataire.
- le seul avantage de ce vert est qu'il désactive l'exécution des virus Mydoom.A@mm, Mydoom.B@mm, et Mimail.T@mm. !

La méthode de propagation est malheureusement très efficace, mais nous pouvons constater qu'une autre variante de Netsky est encore plus dangereuse :

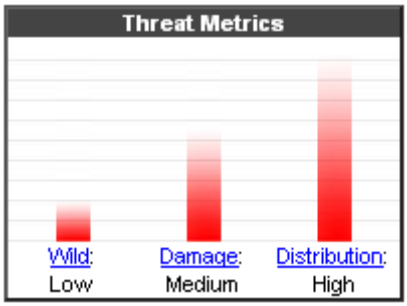
- Cas de la version X

- le nom du service lancé par le virus est « FirewallSvr », ce qui laisse supposer que l'ordinateur est protégé quand on regarde le gestionnaire de tâches.
- Il vérifie le domaine principal d'Internet (TLD) de l'adresse électronique trouvée, et adapte la langue à l'objet, au message, et au nom de la pièce jointe en conséquence.

Exemple :

Domaine principal	**.fr**	**.no**
Objet	Re: document	Re: dokumentet
Message	Veuillez lire le document	Behage lese dokumentet
Pièce jointe	document.pif	dokumentet.pif

Cette variante de virus est encore plus intelligente car elle s'adapte en fonction de l'adresse mail du destinataire, et donc de sa langue natale. Les soupçons d'un message électronique malveillant sont d'autant plus diminués. Comme nous pouvons le constater ci-dessous, ce virus ne cause pas trop de dégats, mais il se répend très rapidement.



© Symantec

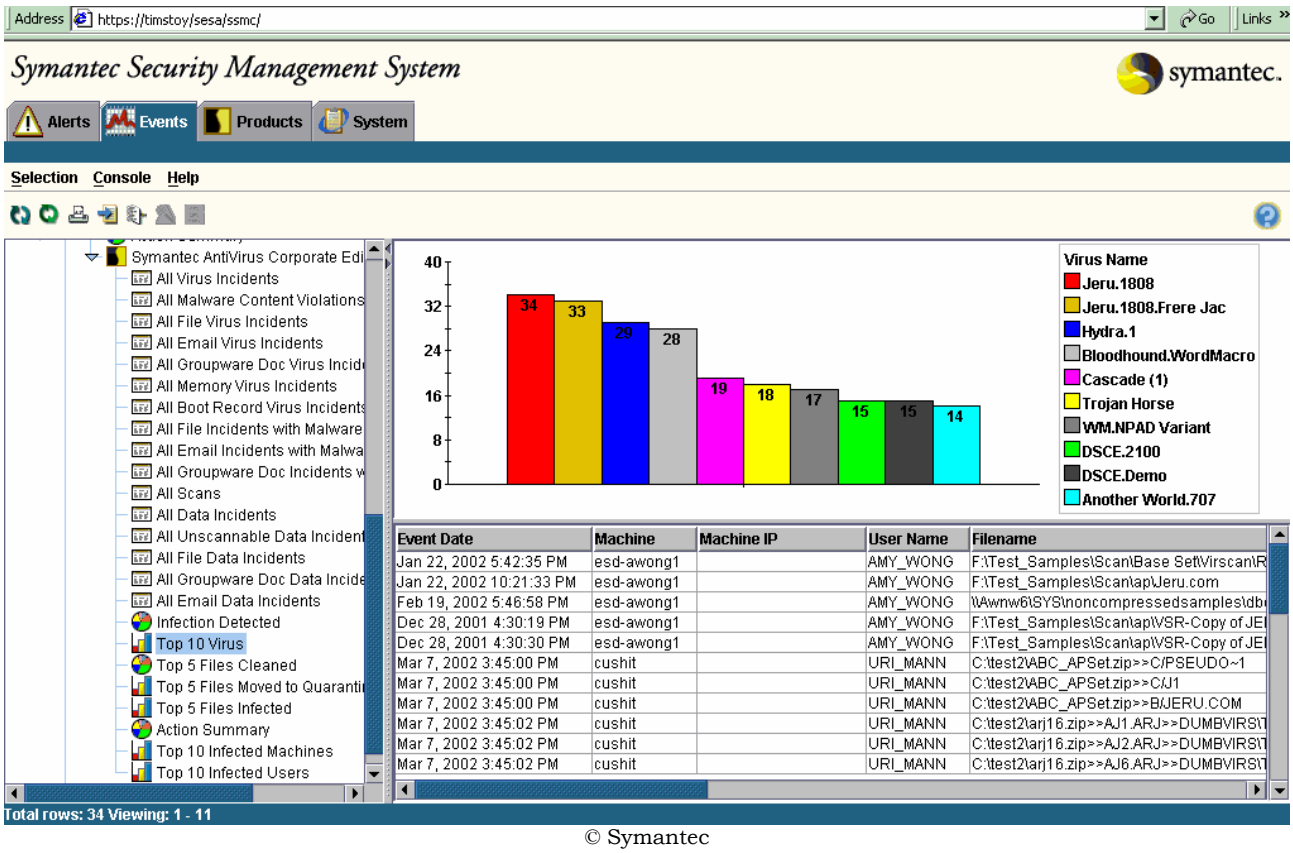
La multiciplicité des virus et de leurs variantes nécessitent de la part des administrateurs une vigilange soutenue. D'une manière plus générale, lors d'un déploiement d'une telle envergure, il parraît nécessaire de prendre le maximum de précautions pour sécuriser un réseau.

* * * * *

EVOLUTIONS ENVISAGEABLES

Le déploiement d'une solution antivirus telle que j'ai mis en oeuvre ne s'arrête pas un moment donné. En effet, un système d'information est une antité maléable et vivante. Rien n'est jamais figé, et il est nécessaire de faire évoluer un réseau ainsi que les systèmes qu'il comporte.

La solution mise en oeuvre était à l'origine un minimum nécessaire pour pouvoir protéger le réseau de R.E.A. Toutefois, Symantec propose des outils supplémentaires qui n'ont pas été déployés pour l'instant. Ces modules ne sont pas vitaux pour le réseau, mais permettent par exemple un reporting en temps réel via une console (SESA). Cela permet entre autre une réduction du temps passé à l'analyse du système antivirus, la génération de graphes



© Symantec

L'installation de ce module peut être bien pratique, mais elle nécessite des moyens matériels, financiers, et humains supplémentaires. En effet, il lui faut un serveur dédié avec une base de donnée de Oracle, puis plusieurs journées de formation et de prise en main.

A la fin de mon stage, il n'était pas question d'installer ce système, mais peut-être qu'un jour, le moment sera venu de le faire…

* * * * *

SYNTHESE

Ce stage m'a permis d'intégrer un déploiement de grande envergure au sein d'une équipe informatique pluridisciplinaire. Autant de chefs de projet, d'administrateurs, de techniciens, de prestataires externes furent nécessaires, avec pour chacun leur compétences propres, afin de mener à bien ce projet de longue haleine.

Je me suis adapté à un nième déploiement parmi ceux qu'i ont occupés quelques-uns de mes précédents contrats de travail. Mais cette fois-ci, ma fonction était bien précise, et reflétait bien l'un des problèmes actuels des systèmes d'informations : la sécurité informatique. Parmi les vulnérabilités d'un réseau d'entreprise, nous pouvons évidemment citer la banalisation des accès à internet ainsi que toutes les failles qu'elle peut comporter, les échanges de médias, la multitude d'ordinateurs nomades, ainsi que le comportement à risque de certaines personnes.

Cette nouvelle expérience m'a une fois de plus démontré que l'on ne peut pas se baser que sur l'existant. Il faut s'adapter en permanence afin de répondre au mieux aux besoins de l'entreprise, tout en limitant les risques au minimum, quels qu'ils soient.

La mise en place d'une solution antivirale sur trois niveaux ne fut qu'une partie du déploiement des 5000 postes et 70 serveurs. Néanmoins, elle a occupé la majorité de mes trois mois, ce qui n'est pas négligeable. Autant les virus dont l'intelligence artificielle (capacité de mutation, de camoufflage, de propagation) est de plus en plus poussée, autant les informaticiens doivent redoubler de vigilence. En tant qu'administrateurs systèmes et réseau, nous avons aussi un rôle esentiel qui est de prévenir les risques encourus pour une topologie donnée.

Mon stage pratique m'a permis de consolider mes connaissances sur windows server 2003. La formation théorique que nous avons eue étant largement axée sur les systèmes Unix, mon étape chez R.E.A. m'a apporté un complément de connaissances non négligeable. Il est en effet souvent demandé à un administrateur de connaître la famille des serveurs windows. De plus, je peux maintenant ajouter une corde à mon arc : celle de mon savoir-faire sur Symantec Antivirus Corporate Edition.

Le fait d'être intégré dans une structure telle que le siège social de Renault Europe Automobiles m'a apporté une autre ouverture d'esprit. En effet, il m'a fallu comprendre le fonctionnement du système d'information auprès des professionnels qui composent l'équipe informatique. C'est à partir de cette vision globale que j'ai pu ajouter une pièce au puzzle, de la manière la plus harmonieuse possible.

Bien que le déploiement continue sans ma présence, je pense pouvoir proposer mes compétences dans d'autres entreprises. Je reste bien évidemment conscient que la profession d'administrateur réseau & systèmes nécessite un apprentissage continu, mais un des avantages de notre métier, c'est justement de pouvoir évoluer dans un environnement variable.

* * * * *