

Pierre Catala
pierre.catala@puyinra.fr

Antivirus

CUME JT
21/10/2004

INRA
DISI - pSI (Système Informatique)
SIR (Service Infrastructure et Réseau)
Pôle Sécurité

Antivirus

Sommaire

- Opération antivirus du Groupe Logiciel
- Produits antivirus déployés
- Antivirus messagerie, HTTP, FTP

CUME JT
21/10/2004

Antivirus

Opération antivirus du Groupe Logiciel

CUME JT
21/10/2004

Antivirus

Opération antivirus du Groupe Logiciel

- Editeurs / Produits
- Evaluation de la charge induite par l'antivirus
- Evaluation de la détection virale
- Caractéristiques
- Notes
- Formation de formateurs antivirus McAfee/NAI
- Antivirus gratuits ?

CUME JT
21/10/2004

Antivirus

Opération antivirus du Groupe Logiciel

Editeurs / Produits	<ul style="list-style-type: none"> <input type="checkbox"/> 22 dossiers envoyés par 10 distributeurs <input type="checkbox"/> 7 éditeurs représentés <input type="checkbox"/> 9 produits proposés
	<ul style="list-style-type: none"> <input type="checkbox"/> F-Secure (F-Secure Anti-Virus) <input type="checkbox"/> Finjan (SurfinShield Corporate) <input type="checkbox"/> MicroWorld (eScan) <input type="checkbox"/> NAI-McAfee (Active VirusScan Security Suite) <input type="checkbox"/> Norman (Norman Virus Control) <input type="checkbox"/> Symantec (SA VCE 8.0) <input type="checkbox"/> Symantec (SCS) <input type="checkbox"/> Symantec (SA VEE 8.5) <input type="checkbox"/> Trend Micro (OfficeScan/Server Protect)

CUME JT
21/10/2004

Antivirus

Opération antivirus du Groupe Logiciel

Evaluation de la charge induite par l'antivirus	<ul style="list-style-type: none"> <input type="checkbox"/> Mesures réalisées sur une arborescence de 2Go <ul style="list-style-type: none"> ➢ 12000 fichiers et 600 répertoires ➢ 1Go de répertoires du système Windows 2000 ➢ 1Go d'archives d'installation de logiciels
---	---

CUME JT
21/10/2004

Evaluation de la
détection virale
(1/2)

- Réalisée au moyen des fonctions d'analyse virale incluses dans le menu contextuel de l'explorateur Windows
- En terme de sécurité
 - Limitation de la récursivité dans l'analyse des archives imbriquées n'est pas problématique
 - Une analyse en configuration standard qui ne porte pas sur l'ensemble des fichiers engendre une faille

Evaluation de la
détection virale
(2/2)

- Contenu du jeu de test viral (131 fichiers infectés)
 - 6 virus macros
 - ✓ w97mwalkere, wmcapa, vbsloveletter, w97mclass, wmwazzua, w97mmelissa
 - 14 virus exécutables
 - ✓ sircanworm, hybrismowmd, klezh, backdoor, magstr32768, livvad, lentinf, lèze, hybrismomb, gandaa, funlova4099, skal0000worm, bugteaa, sobigb
 - 7 exploits (code pour exploiter une faille de sécurité)
 - ✓ 2 concernent IIS (iisuricode, iisSprinter)
 - ✓ 2 ciblent Linux (sendmailInx, procmalInx)
 - ✓ 1 vise MS Office (officeua)
 - ✓ 1 concerne NT (winntdexploit)
 - ✓ 1 cible le proxy Gate Keeper (gkwarez)
 - Test sur une profondeur de 10 répertoires
 - Test avec des faux suffixes
 - Test de 7 archives (zip, zip résultat de 3 zip récursifs, zip résultat de 5 zip récursifs, zip auto-extractible PowerArchiver, cab, targz, tarbz2)

Caractéristiques

Caractéristiques	Analyse des flux	Firewall	Quarantaine	Décontamination	Spécificités
F-Secure	Aucun	Régage fin	Aucune	OK	
MicroWorld	POP3, SMTP	NA	OK	OK	Anti-spam et filtrage URL
Norman	POP3, IMAP, SMTP, NNTP	NA	OK	OK, nettoie correctement les archives zip imbriquées	
NAI (VirusScan 7)	Aucun	Régage fin	Aucune	Ne supprime pas des archives, les fichiers qui ne peuvent pas être décontaminés et laisse l'archive en place	Détection des outils de piratage
Symantec (SAVCE 8.0)	Aucun	NA	OK	OK	CD bootable pour analyse de secours
Symantec (SCS)	Aucun	Régage fin	OK	OK	CD bootable pour analyse de secours
Trend Micro	POP3	Blocage d'urgence (OfficeScan)	OK	OK	Protection des PDA

Notes

- Gamme de produits
 - 2 points pour les postes Windows 9x, ME
 - 2 points pour les postes Windows NT, 2000, XP
 - 2 points pour les serveurs Netware, Windows NT, 2000, 2003
 - 2 points pour les postes Macintosh
 - 2 points pour les machines Unix
- Qualité de la protection
 - 6 points pour les virus trouvés dans le jeu de test (6 si >= 120, 5 si >= 100, 4 si >= 80, 3 si >= 60)
 - -1 point si la charge induite sur la machine est trop importante
 - 2 points pour l'analyse des flux POP3 et IMAP (1 point pour chacun)
 - 2 points pour le firewall (2 s'il est finement paramétrable, 1 si simple choix de profils)
- Offre support technique
 - 8 points si accès au support de l'éditeur
 - 2 points si support auprès du distributeur

Formation de
formateurs
antivirus
McAfee/NAI

- VirusScan est l'antivirus à déployer sur les nouveaux postes
- Formation de personnels de CRI diffuseur
 - Pour redonner des formations ou pour aider en région
 - Formation porte sur
 - ✓ VirusScan Enterprise
 - ✓ ePolicy Orchestrator

Antivirus
gratuits ?

- Evaluations à venir
 - Antivir
 - Avast
 - AVG
 - Clamav
- Intérêt
 - Pour les postes n'appartenant pas à l'établissement mais présents sur le site

Produits antivirus déployés

Produits
antivirus
déployés

- F-Secure
- McAfee/NAI
- Symantec

Produits antivirus d'éployés

- | | |
|----------|--|
| F-Secure | <ul style="list-style-type: none"> <input type="checkbox"/> F-Secure Anti-Virus for Windows Workstations <ul style="list-style-type: none"> ➢ Version 5.43 <input type="checkbox"/> F-Secure Anti-Virus for Windows File Servers <ul style="list-style-type: none"> ➢ Version 5.50 <input type="checkbox"/> F-Secure Policy Manager <ul style="list-style-type: none"> ➢ Version 5.50 |
|----------|--|

Produits antivirus d'éployés

- | | |
|---------------------|---|
| McAfee/NAI
(1/3) | <ul style="list-style-type: none"> <input type="checkbox"/> McAfee Active Client Security <ul style="list-style-type: none"> ➢ VirusScan Enterprise (version 8) <ul style="list-style-type: none"> ✓ Postes NT4/2000/XP et serveurs Windows ➢ VirusScan (version 4.5.1) <ul style="list-style-type: none"> ✓ Postes Windows 9x/Me ✓ Machines Unix <ul style="list-style-type: none"> ▪ Linux, Solaris, HP-UX, AIX, SCO, FreeBSD ➢ McAfee Desktop Firewall (version 8) <ul style="list-style-type: none"> ✓ Postes NT4/2000/XP et serveurs Windows ➢ NetShield for Netware (version 4.6.2) ➢ Virex (version 7) <ul style="list-style-type: none"> ✓ Macintosh ➢ ePolicy Orchestrator (version 3.0.2a) <ul style="list-style-type: none"> ✓ Serveur d'administration centralisée ✓ Mais ne permet pas d'administrer les Macintosh |
|---------------------|---|

Produits antivirus d'éployés

- | | |
|---------------------|---|
| McAfee/NAI
(2/3) | <ul style="list-style-type: none"> <input type="checkbox"/> Administration centralisée <ul style="list-style-type: none"> ➢ ePolicy Orchestrator (version 3.0.2a) ➢ Permet <ul style="list-style-type: none"> ✓ Forcer les mises à jour ✓ Déployer l'antivirus sur certains postes <input type="checkbox"/> Centralisation des alertes <ul style="list-style-type: none"> ➢ Alert Manager (version 4.7.1) <input type="checkbox"/> Création de paquets d'installation pré-configurés <ul style="list-style-type: none"> ➢ Installation Designer (version 8) <input type="checkbox"/> Service de mise à jour <ul style="list-style-type: none"> ➢ AutoUpdate Architect (version 1.1.2) |
|---------------------|---|

Produits antivirus d'éployés

- | | |
|---------------------|---|
| McAfee/NAI
(3/3) | <ul style="list-style-type: none"> <input type="checkbox"/> Simple service de mise à jour centralisée <ul style="list-style-type: none"> ➢ Serveur Unix <ul style="list-style-type: none"> ✓ Récupère avec wget les fichiers DAT ✓ Dépose les MAJ dans un espace Samba ➢ Nécessite de configurer l'espace de MAJ dans le package d'installation avec Installation Designer |
|---------------------|---|

Symantec
(1/2)

- ❑ Symantec AntiVirus Corporate Edition (SAVCE 9)
 - Antivirus pour postes Macintosh
 - Antivirus pour Netware
 - Antivirus pour postes Windows
 - Antivirus pour serveurs Windows
 - Symantec System Center
 - ✓ Serveur d'administration centralisée
 - ✓ Mais ne permet pas d'administrer les Macintosh

Symantec
(2/2)

- ❑ Administration centralisée
 - Symantec System Center
 - Alert Management System
 - Quarantaine centralisée
 - Permet
 - ✓ Forcer les mises à jour
 - ✓ Déployer l'antivirus sur certains postes
 - ✓ Centraliser les alertes
- ❑ Simple service de mise à jour centralisée
 - Simple poste
 - ✓ Exécute LiveUpdate Administrator
 - ✓ Dépose les MAJ dans un espace Samba
 - Nécessite de déployer un fichier de configuration sur les postes clients pour indiquer l'espace de MAJ

Antivirus messagerie, HTTP, FTP

*Antivirus
messagerie,
HTTP, FTP*

- ❑ Antivirus à coupler à Amavis, MailScanner, Apache en mode proxy
- ❑ McAfee/NAI
- ❑ Sophos
- ❑ Symantec
- ❑ Trend Micro
- ❑ Conseils de mise en œuvre d'un antivirus de messagerie

Antivirus
à coupler à
Amavis,
MailScanner,
Apache
en mode proxy

- ❑ Clamav
 - Produit libre
- ❑ F-Secure - F-Secure Anti-Virus sous Unix
 - Linux
 - Nécessite l'acquisition d'un droit d'usage spécifique
- ❑ McAfee/NAI - VirusScan sous Unix
 - Linux, Solaris, HP-UX, AIX, SCO, FreeBSD
- ❑ Sophos - SAV sous Unix
 - Linux, Solaris, HP-UX, AIX, SCO, FreeBSD, Tru64
 - Pour l'acquisition, se reporter au protocole d'accord du Groupe Logiciel

McAfee/NAI

- ❑ McAfee/NAI - WebShield
 - Version Solaris en cours d'abandon
 - Solutions matérielles - WebShield for Appliance
 - ✓ Analyse antivirale SMTP, HTTP et FTP + anti-spam

- Sophos
- ❑ Sophos - PureMessage
 - Analyse antivirus SMTP + anti-spam
 - Pour l'acquisition, se reporter au protocole d'accord du Groupe Logiciel

- Symantec
- ❑ Différents produits Symantec
 - Antivirus Mail Security for SMTP
 - Antivirus Mail Security for Domino
 - Antivirus Mail Security for Microsoft Exchange
 - Antivirus Gateway
 - Anti-spam
 - Firewall intégrant un antivirus
 - ❑ Protocole d'accord du Groupe Logiciel pour les 5 premiers

- Trend Micro
- ❑ Antivirus SMTP et anti-spam
 - InterScan Messaging Security Suite
 - Sous Solaris, Linux, Windows
 - ❑ Antivirus HTTP, FTP
 - InterScan Web Security Suite sous Solaris
 - InterScan sous Linux
 - ❑ Antivirus pour Domino et Exchange
 - ❑ Protocole d'accord du Groupe Logiciel

- Conseils de mise en œuvre d'un antivirus de messagerie (1/2)
- ❑ Frontal de messagerie
 - Doit héberger l'antivirus, voire l'anti-spam
 - Eviter de cascader Sendmail ou autre avec un AV SMTP
 - ✓ Préférer l'appel d'un simple antivirus de fichiers
 - ✓ Permet de refuser les emails avec une erreur SMTP
 - ✓ Evite de multiplier les messages Mailer-Daemon
 - Si besoin, route ensuite vers les serveurs de BAL
 - ❑ Analyse virale des emails des serveurs de listes
 - Analyse en entrée
 - ✓ Donc analyse tous les retours sur erreur
 - Pour listes importantes, voir solution Sympa
 - Pas d'analyse en sortie

- Conseils de mise en œuvre d'un antivirus de messagerie (2/2)
- ❑ Opération lors de la découverte d'un virus
 - Nettoyage, sinon destruction
 - Pas de mise en quarantaine
 - ✓ Nécessite une place importante
 - ✓ Par expérience, aucun intérêt
 - ❑ Alerte lors de la découverte d'un virus
 - Pas d'avertissement automatique de l'émetteur
 - ✓ Non distinction, émetteur interne ou externe
 - ✓ Risque d'email bombing
 - ✓ Problème avec listes de messagerie non modérées
 - Si champ "Reply-to" à la liste