# Étude des *Spywares*


| | |
|---|---|
| Étudiant : | DE SOUSA Bruno |
| Professeur responsable : | LITZISTORF Gérald |
| En collaboration avec : | TRUPHEME Florent |
| | Telecom System |
| Session: | 2005 |

# Plan de l'exposé

- Généralités (7 jours d'étude)
- Infection (12 jours)
- Protection (15 jours)
  - Logicielle
  - Matérielle
- Détection / suppression (10 jours)
- Démos
- Questions

# Environnement de travail

- Machine virtuelle VMWare
  - Processeur 2.8 GHz
  - Mémoire RAM 748 Mo
- Windows XP Pro SP2 de base
- Internet Explorer 6 de base

# Généralités

- Tout logiciel installé à l'insu de l'utilisateur et portant atteinte à sa vie privée

- Actions entreprises :
  - Créer des *backdoors*
  - *Keylogger*
  - *Tracker*
  - Collecter les données entrées dans les formulaires
  - Affichage de publicité
  - Flux chiffrés

- Symptômes :
  - Diminution des performances de la machine
  - Messages d'erreur, icônes inconnus, barres d'outils, …

# Infection

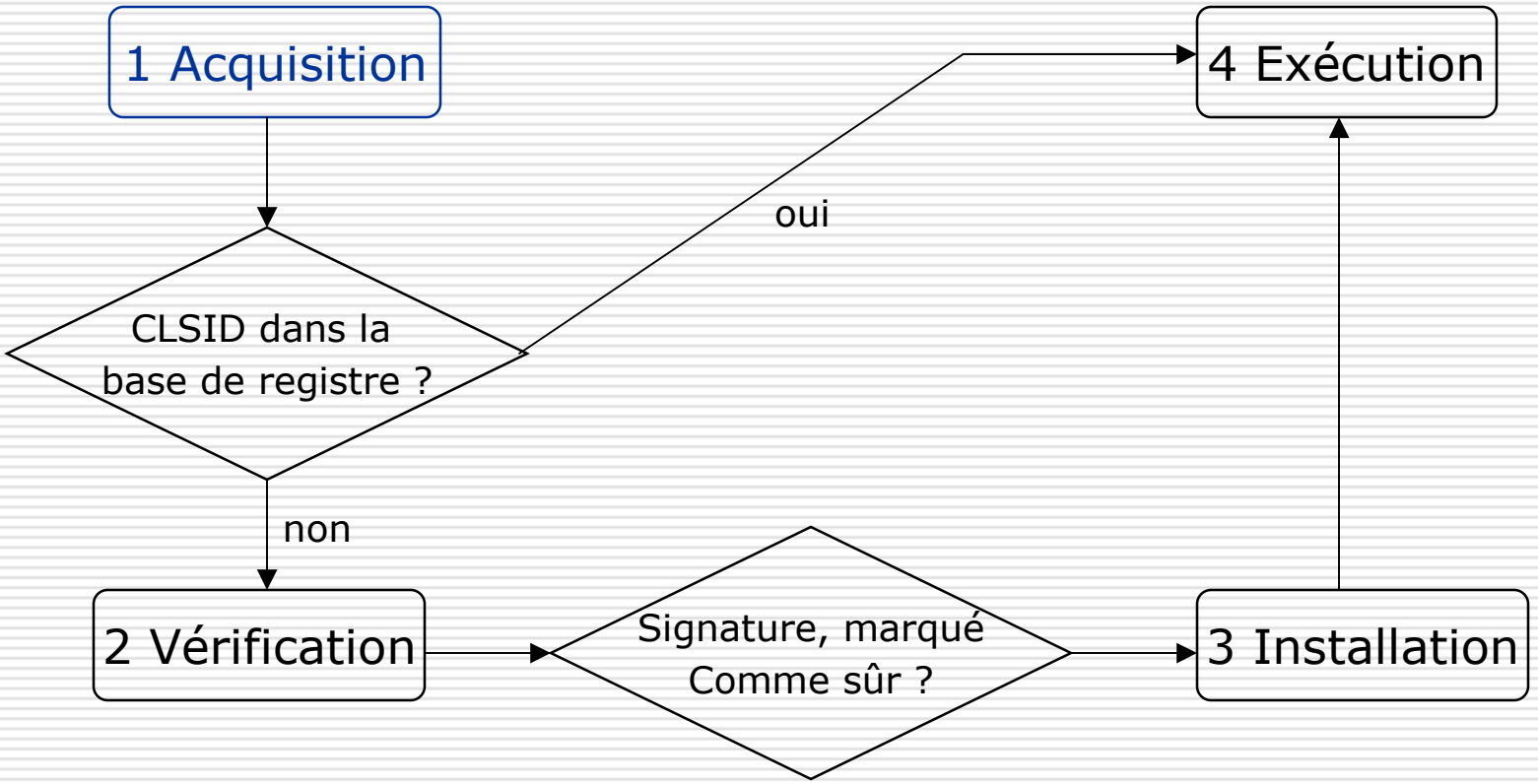
- *Bundled software (Kazaa, Grokster, …)*
- ActiveX (*Drive-by install*)
- Failles du navigateur IE (MS05-002, CHM, …) → Démo 1

# Infection : ActiveX

- Caractéristiques
  - Modèle de programmation objet COM
  - Composant ActiveX :
    - Librairies dynamiques ActiveX (.dll)
    - Exécutables ActiveX (.exe)
    - Contrôles ActiveX (.ocx)
  - Pas d'environnement bac à sable → Accès à tous les éléments de la machine
- Installation à partir de tout support informatique

# Infection : ActiveX – Installation à partir du web

- Admin, 4 étapes



# Infection : ActiveX

HTTP GET /d.x?82506 — Demande de la page d'accueil

HTTP OK — Envoi de la page d'accueil

HTTP GET /0006_cracks.cab — Requête sur le contrôle ActiveX

HTTP OK — Envoi du contrôle ActiveX

} Acquisition

Vérification, Installation

Exécution de l'ActiveX

Exécution de l'ActiveX après autorisation de l'utilisateur

HTTP GET /istdownload.exe

HTTP OK

HTTP GET /istsvc.exe

.

.

.

HTTP GET /powerscan.exe

HTTP OK

} Fichiers demandés par le code de l'ActiveX, ces fichiers installeront les *spywares*

# Infection : envoi / récupération d'informations

| | |
|---|---|
| HTTP GET /...ist_install.php?ist=5&istbar=5&istsvc=5&bb=5&ncase=...&download_key=3538f...d80fd2fa → | **IST service spyware** demande configuration |
| ← HTTP OK | Téléchargement des informations |
| HTTP GET /ShowAdSample.cgi?URL=http:%2F%2Fwww.google.ch&WIDTH=...&BGCOLOR=ededec → | Informations concernant les sites visités transmises au serveur, de manière à télécharger les publicités adéquates |
| ← HTTP Moved Temporarily | Source déplacée. La requête sera retransmise par la suite |
| HTTP GET /sacc/feedback.php?action=sacc_running&vinfo=Windows%20NT%20Workstation%205.1%20Buildnumber%20:%20%202600%20Service%20Pack%202... → | Envoi d'autres informations concernant la machine infectée (Windows NT Workstation 5.1 Service Pack 2 <-> Windows XP SP2) |
| ← HTTP No Content | Acquittement |

# Protection

- Logicielle
  - Orientée utilisateur particulier
- Matérielle
  - Orientée utilisateur professionnel (entreprise)
  - Blue Coat ProxySG 400

# Protection logicielle

- *Security Checklist*
- *Windows Update*
- Paramètres de sécurité du navigateur IE
- ActiveX *kill bit* (SpywareBlaster 3.4) → *Black list*
- Agent de protection temps réel → Démo 2
- Pare-feu applicatif
- Antivirus
- Naviguer de manière plus sûre !

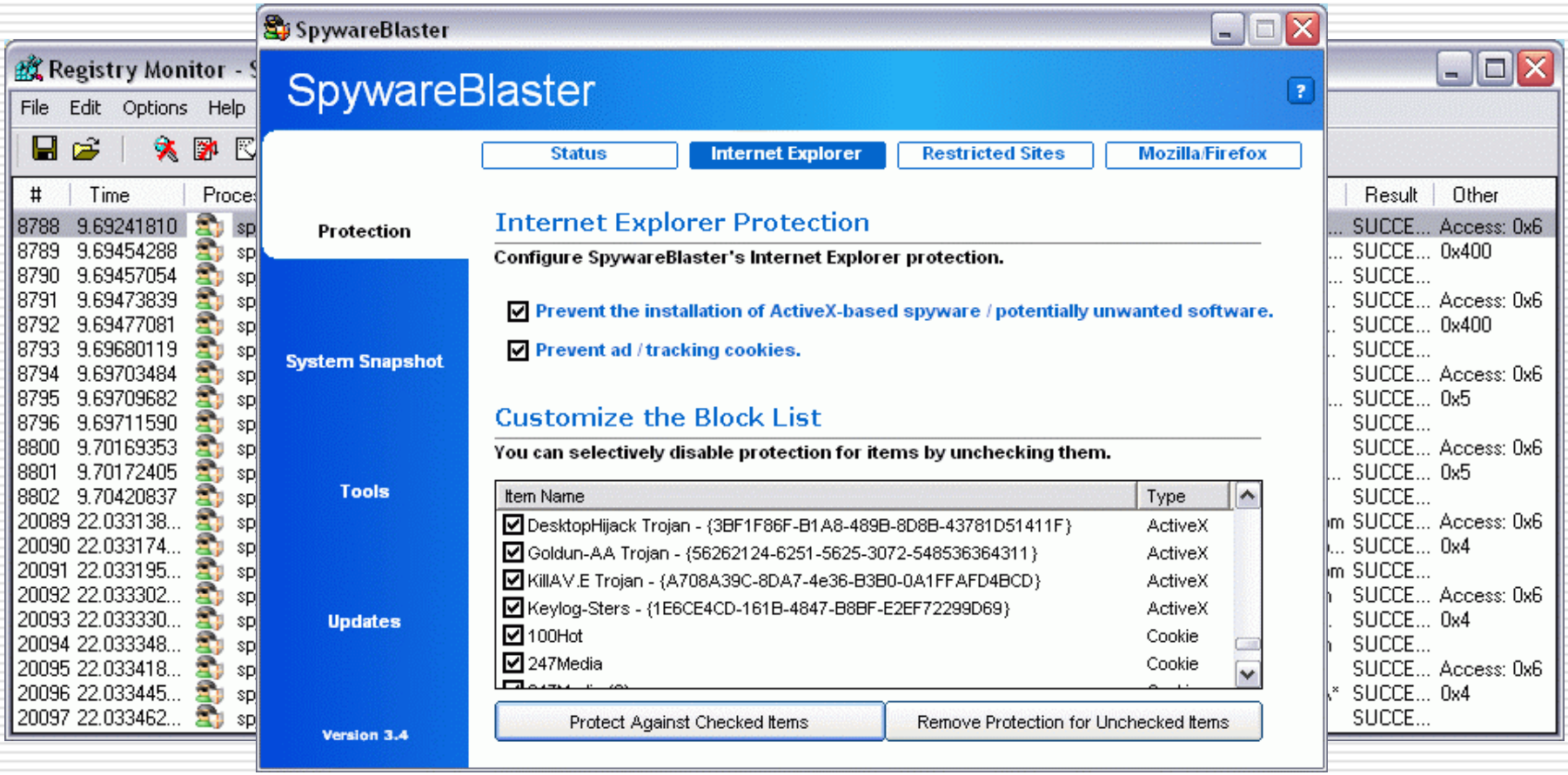
# Protection logicielle : *Checklist*

- Mots de passe pour tous les comptes
- Désactiver le compte « Invité »
- Renommer le compte « Administrateur »
- N'utiliser les comptes administrateur que lorsque nécessaire
- Désactiver le partage de fichiers simple
- Désactiver les partages par défaut
- Désactiver le bureau à distance
- Désactiver les services non nécessaires (*Remote registry*, Telnet, …)

# Protection logicielle : paramètres de sécurité du navigateur IE

| | Contrôles ActiveX et plugins | Élevé | Recommandé |
|---|---|---|---|
| Étape 1 | **Demander confirmation pour les contrôles ActiveX** | Désactiver | Activer |
| 2, 3 | **Télécharger les contrôles ActiveX non signés** | Désactiver | Désactiver |
| | **Télécharger les contrôles ActiveX signés** | Désactiver | Demander |
| | **Contrôles d'initialisation et de script ActiveX non marqués comme sécurisés** | Désactiver | Désactiver |
| | **Contrôles ActiveX reconnus sûrs pour l'écriture de scripts** | Désactiver | Demander |
| 4 | **Exécuter les contrôles ActiveX et les plugins** | Désactiver | Demander |

# Protection logicielle : SpywareBlaster 3.4 (*kill bit*)



# Protection logicielle : naviguer de manière plus sûre

- Éviter les sites de jeux et à contenu pornographique
- Télécharger uniquement à partir de sites connus
- Refermer les pop-ups en utilisant Alt-F4 ou la 'X' de fermeture de la fenêtre ou les bloquer
- Ne pas lire le contenu actif des e-mails, sauf s'il provient d'une source sûre
- Se méfier des *freewares*
- Lire les alertes de sécurité et les EULAs des logiciels installés

# Protection matérielle

- Création de règles pour Blue Coat ProxySG 400 → Démo 2

- Objectifs
  - Bloquer les sites de *spywares*
  - Bloquer les installations de *spywares*
  - Logger toute activité suspecte
  - Informer les utilisateurs dont les machines sont infectées

# Protection matérielle : définitions de base

- *White list*

```
define url.domain condition
    trusted_domains
    bluecoat.com
    microsoft.com
    unige.ch
    windowsupdate.com
end
define subnet IP_Interne
    10.1.0.0/16
end
define condition
    trusted_sites
    condition =
    trusted_domains
    url.address = IP_Interne
end
```

- *Black list*

```
define condition exe_blocks
    category="Adult Content"
    …
    category="Peer-to-Peer
    File Sharing"
    category="none"
end
define condition
    active_content_blocks
    condition=exe_blocks
    category="Hacking"
    …
    category="Games"
End
define condition phone_home
    category="Security PG"
end
```

# Protection matérielle : définitions de base

- *Black list* (suite)

```
define condition active_content_extensions      → ActiveX
    url.extension=cab
    url.extension=ocx
    response.x_header.Content-Disposition = "\.(cab|ocx)($|[^a-
    z0-9])"
end
define condition active_content_type
    response.header.Content-Type="application/cab"
    response.header.Content-Type="application/x-compress"
    response.header.Content-Type="application/x-compressed"
    response.header.Content-Type="zz-application/zz-winassoc-
    cab"
    response.header.Content-Type="application/x-cab-compressed"
    response.header.Content-Type="application/(x-|)java[^s]"
end
```

# Protection matérielle : bloquer les sites de *spywares*

- Catégories Websense (13 millions de sites)

```
<Proxy Spyware_PhoneHome>
    Condition=phone_home \
    FORCE_DENY("Requête bloquée car spyware
    $(quot)phoning home$(quot). Veuillez consulter votre
    ingénieur système.")
```

# Protection matérielle : bloquer les installations de *spywares*

- Extensions, type de contenu

```
<Proxy
   ActiveContent_Executable_control>condition=!trusted_s
      ites condition=active_content_blocks

   condition=active_content_extensions \
   FORCE_DENY("Requête bloquée car spyware $(quot)Drive-
   by Install$(quot) reconnue par
   active_content_extensions")

   condition=active_content_type \
   FORCE_DENY("Requête bloquée car spyware $(quot)Drive-
   by Install$(quot) reconnue par active_content_type")
```

# Protection matérielle : *logger* toute activité liée aux *spywares*

- 4 fichiers de logs
  - `Drive_by_install_denied`
  - `Executable_file_denied`
  - `Phone_home_detected`
  - `Risky_tags_striped`

```
<Proxy Spyware_PhoneHome>
    Condition=phone_home \
    FORCE_DENY("Requête bloquée car spyware
    $(quot)phoning home$(quot). Veuillez consulter votre
    ingénieur système.")
    access_log(phone_home_detected)
```

# Protection matérielle : informer les utilisateurs

```
define javascript user_alert
prolog <<ABC123 {
    alert( "Alerte de sécurité\n\n"+"Une communication avec un
    serveur spyware a été détectée.\n"+"Il se pourrait que vôtre
    machine soit infectée.\n"+"Veuillez consulter votre ingénieur
    système.");
}
ABC123
end
define action user_alert
    transform user_alert
end

<Proxy Spyware_PhoneHome>
    Condition=phone_home \
    FORCE_DENY("Requête bloquée car spyware $(quot)phoning
    home$(quot). Veuillez consulter votre ingénieur système.")
    access_log(phone_home_detected)
    action.user_alert(yes)
```

# Détection / suppression

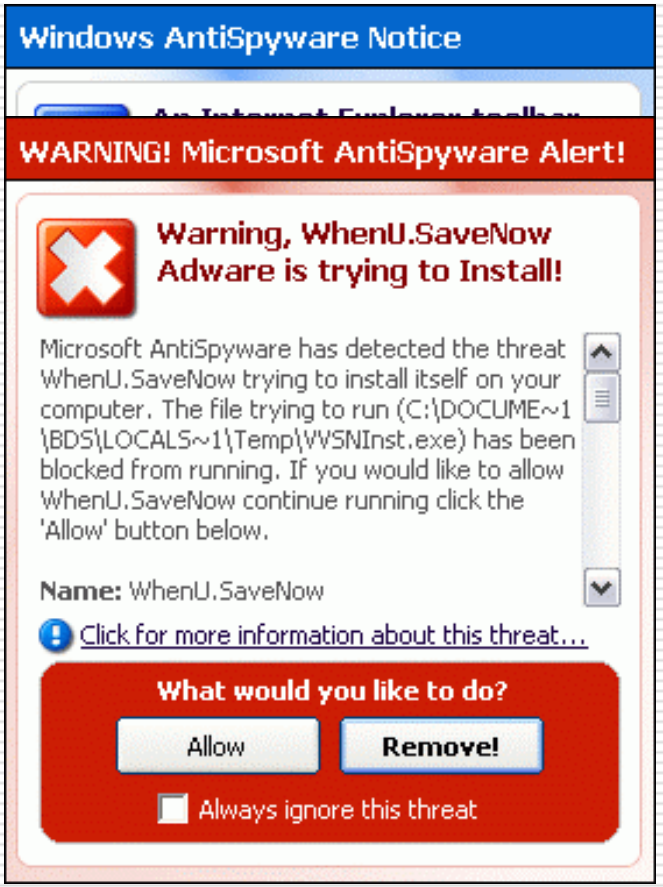
- Machine infectée avec 22 familles de menaces
- Lavasoft Ad-Aware SE Personal Edition 1.06r1
  - Suppression à posteriori
- Microsoft AntiSpyware Beta 1 v1.0.615
  - Suppression à posteriori
  - Agent temps réel
- Spybot – Search&Destroy 1.4
  - Suppression à posteriori
  - Agent temps réel

# Détection / suppression : performances de suppression

| Performances | Lavasoft Ad-Aware SE Personal Edition | Microsoft AntiSpyware Beta 1 | Spybot - Search&Destroy |
|---|---|---|---|
| **Menaces détectées** | 20 | 21 | 19 |
| **Menaces supprimées** | 12 | 21 | 15 |
| **Durée moyenne d'analyse** | 4 min. | 9 min. 50 s. | 3 min. 20 s. |
| **Efficacité après 3 analyses** | 55 % | 95 % | 68 % |

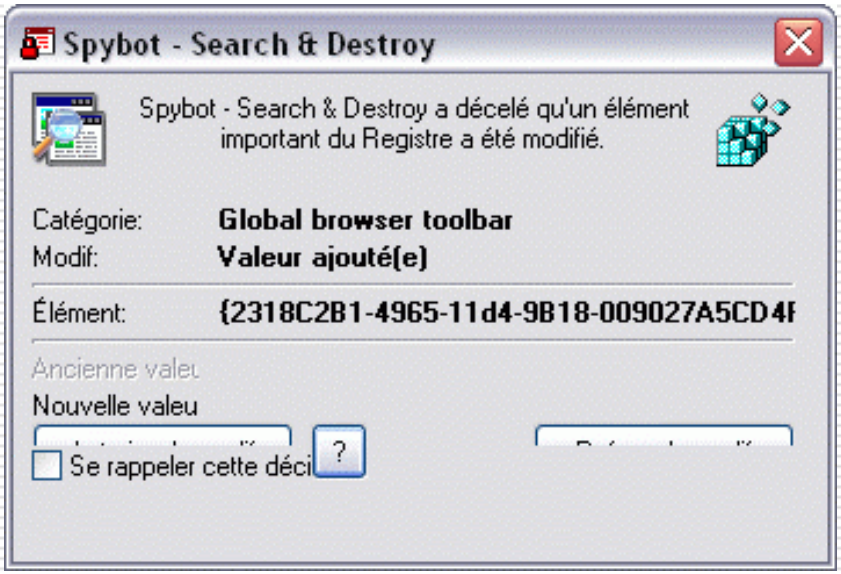
# Détection / suppression : Microsoft AntiSpyware Beta 1

- Protection temps réel
  - Agents internet
    - Paramètres de connexion internet (TCP/IP, DNS, …)
  - Agents système
    - Paramètres système (Hosts, services, …)
  - Agents application
    - Applications installées (IE, démarrage automatique, scripts, …)
  - Analyse périodique de certaines clés de registre (~ toutes les 20 secondes)



# Détection / suppression : Spybot Search&Destroy 1.4

- Protection temps réel
  - Résident « SDHelper »
    - Bloqueur de téléchargements
  - Résident « TeaTimer »
    - Réglages système fondamentaux
  - Analyse périodique de certaines clés de registre (~ toutes les secondes)



# Détection / suppression : comparaison des caractéristiques

| | **Lavasoft Ad-Aware SE Personal Edition** | **Microsoft AntiSpyware Beta 1** | **Spybot - Search&Destroy** |
|---|---|---|---|
| **Réparation après redémarrage** | Oui | Non | Oui |
| **Protection temps réel** | Payante | Oui | Oui |
| **Possibilité de restauration** | Oui | Oui | Oui |
| **Caractéristiques des *spywares*** | Non | Oui | Oui |
| **Planificateur d'analyse** | Non | Oui | Oui |
| **Autres** | Restauration des pages IE par défaut | *Spynet community*, outil d'exploration système (ActiveX, BHOs), … | Effaceur de sécurité, détection de traceurs, … |

# Résumé des outils intéressants

- Protection temps réel
  - Microsoft AntiSpyware → Windows Defender
- Pour savoir immédiatement si on a été attaqué
  - HiJackThis (c.f. mémoire)
- Pour supprimer les menaces
  - Microsoft AntiSpyware
  - Spybot - Search&Destroy
- Autres
  - Active Registry Monitor : comparaison de bases de registre
  - System Info for Windows : informations sur la machine

# Démos

- Démo 1 : exploits
  - Faille CVE-2004-1049 (MS05-002) : *Proof Of Concept* – prise de contrôle à distance avec telnet
  - Faille CVE-2005-1790 : *Proof Of Concept – remote code execution* (calc.exe)
- Démo 2 : efficacité de la protection
  - Règles Blue Coat
  - Agent temps réel Microsoft AntiSpyware

# Questions

?