



**EdelWeb**

# **Autopsie d'un malware (pourriciel)**

**Nicolas RUFF**

**EdelWeb**

**nicolas.ruff@edelweb.fr**



- Introduction
- Situation initiale
- 1ère analyse : le spyware
- 2ème analyse : l'injecteur
- 3ème analyse : le code binaire
- Compléments
- Conclusion



- **Le fléau des Spywares est réel**
  - Croissance exponentielle du nombre de "codes douteux"
  - La limite légal / illégal est incertaine
  - Il devient difficile de faire confiance à un logiciel téléchargé sur Internet
  
  - Et pourtant les Spywares ne sont pas perçus comme une menace pour la sécurité ...
  
- **Les auteurs de Spywares utilisent des techniques de pointe**
  - Attaques non patchées, voire non documentées
  
- **L'intérêt financier est motivant**
  - Cf. attaque massive baptisée "Ject"



## ■ Comportement aberrant d'un poste

- Le fond de la page d'accueil IE pointe sur le moteur de recherche "searchx.cc"
- Et pourtant la page d'accueil configurée est "about:blank" !

## ■ Environnement

- Windows XP "raisonnablement" patché
- Antivirus "raisonnablement" à jour
- Poste "vivant" (nombreux logiciels installés)
- Réseau d'entreprise classique (proxy)



## ■ Analyse

- Le comportement du navigateur a été modifié par un "Browser Helper Object" (BHO)

## ■ Solutions brutales

- Faire une recherche sur tous les fichiers contenant la chaîne "searchx.cc"
- Faire une recherche par date de création de fichier entre "avant" et "après"

## ■ Solution élégante

- Analyse avec "HiJackThis!"
- Tri entre les modules ("connus", "inconnus" et "suspects")

## ■ Résultat

- Identification de la DLL fautive
- Destruction de toutes les instances sur disque

## ■ Conclusion

- Le problème est résolu au reboot

# Le problème



EdelWeb

- **Oui, mais ...**
- **... moins d'une 1/2 heure après le composant est réinstallé !**



## ■ Que s'est-il passé ?

- "Quelque chose" a réinstallé de manière asynchrone le BHO fautif

## ■ Comment ?

- Soit le fichier est présent sur le poste
  - Sous une forme compressée ou modifiée car toutes les instances de la DLL d'origine (contenant "searchx.cc") ont été détruites
- Soit le fichier a été téléchargé depuis l'extérieur du poste

## ■ Que faire ?

- Identifier la méthode utilisée
- Identifier le "quelque chose"



## ■ Identification de la méthode : logs du proxy

- `nobody@nowhere:~$ cat access.log | grep 192.168.5.78 | grep octet-stream`
  - [...]
  - `192.168.5.78 TCP_MISS/200 37185 GET http://66.98.144.29/m.bin - DIRECT/66.98.144.29 application/octet-stream`
  - [...]
- `nobody@nowhere:~$ wget http://66.98.144.29/m.bin`
- `nobody@nowhere:~$ strings m.bin | egrep -i searchx.cc`
  - `<form id=formWeb style="FLOAT: left" action="http://searchx.cc/search.php" method="get">`
  - `<form id=formWeb action="http://searchx.cc/search.php" method=get target="_main">`

## ■ Le composant a bien été téléchargé depuis l'extérieur





## ■ Identification du "quelque chose" : logs Windows

- Security / Audit des succès / Accès aux objets
- 560 / Ouverture d'un objet :
  - Objet Serveur : Security
  - Objet Type : File
  - Objet Nom : C:\WINNT\system32\bmnnjc.dll
  - N° du nouveau handle : 2772
  - N° d'opération : {0,1008865}
  - N° de processus : 1924
  - [...]



- Security / Audit des succès / Suivi détaillé
- 592 / Un nouveau processus a été créé :
  - N° du nouveau processus : 1924
  - Nom du fichier image : \Program Files\Internet Explorer\IEXPLORE.EXE
  - N° du processus créateur : 1296
  - N° de la session : (0x0,0xE735)

- C'est donc Internet Explorer lui-même qui est à l'origine du téléchargement
- On suspecte un autre BHO, mais lequel ???



- **HiJackThis! n'indique rien**
  - Ni en mode normal
  - Ni en mode sans échec
  
- **TaskInfo indique une DLL "suspecte" dans l'espace du processus IE**
  - Taille : 0 octets !
  - Cette DLL est trouvée dans le répertoire "system32" par la fonction "rechercher un fichier"
  - Mais elle est invisible dans l'explorateur et la ligne de commande !



- La DLL est capturée par un redémarrage sur un environnement "sain"
  - Multiboot
  - CD bootable Linux (Knoppix, etc.)
  - CD bootable Windows (BartPE, ERD Commander, etc.)
  
- Le poste est alors "désinfecté"



- **La DLL capturée est un véritable "rootkit"**
  - **Code autodécryptable**
  - **Récupère dynamiquement les adresses de toutes les fonctions importées (pas d'imports)**
  - **Crée et enregistre le BHO**
  - **Se masque sur le disque et dans la base de registres par API Hooking**
  
- **Heureusement imparfait ...**

- **Mais pourquoi est-il si méchant ?**
  
- **nobody@nowhere:~\$ host 66.98.144.29**
  - 66.98.144.29 does not exist (Authoritative answer)
- **nobody@nowhere:~\$ whois 66.98.144.29**
  - OrgName: Everyones Internet, Inc.
  - OrgID: EVRY
  - Address: 2600 Southwest Freeway
  - Address: Suite 500
  - City: Houston
  - Country: US
  - [...]
  
- **"Everyones Internet" est un fournisseur d'accès américain**



- **nobody@nowhere:~\$ whois searchx.cc**
  - **OrgName: .TV Corporation**
  - **Registrant: Galina Charmandjieva (xboy66a@yahoo.com)**  
**Address: City Chess 8.1**  
**Elista, NONE 358000**  
**RU**
  - **Birth Date: 5-41-62**
  
- **Brillante page d'erreur sur "whois www.tv"**
  - **<http://www.idotz.net/whois.cfm?domain=www&tld=tv>**



## ■ telnet 66.98.144.29 80

- HEAD / HTTP/1.0
- HTTP/1.1 404 Not Found
- Server: Apache/1.3.29 (Unix) PHP/4.3.4

## ■ nmap 66.98.144.29

- tcp/53 open (BIND 9.2.1)
- tcp/80 open (Apache 1.3.29)
- Linux kernel 2.4.x





- **Comment a été infecté le poste ?**
  - Probablement via un site Web
  - Manquait-il un patch IE, ou non (0-day) ?
  
- **Quelles sont les fonctions "cachées" du spyware ?**
  - Rétroanalyse longue et complexe
  - Evolution possible du code téléchargé sur le Web



- **Le code installé sur le poste est réellement "malveillant"**
  - Techniques de dissimulation
  
- **Il est mis à jour toutes les 30 minutes depuis le site de l'auteur**
  
- **Aucun contrôle sur le code téléchargé n'est effectué, ce qui permet à un tiers malveillant d'utiliser ce mécanisme**
  - Ex. spoofing DNS
  
- **L'antivirus ne voit que la première partie ...**