Compromettre le système d'information d'une entreprise via ses utilisateurs

Benjamin CAILLAT – b.caillat@security-labs.org
Eric DETOISIEN – valgasu@rstack.org

AVERTISSEMENT

AUCUN SYSTEME D'INFORMATION EN PRODUCTION N'A ETE MALTRAITE DURANT LA REALISATION DE CETTE PRESENTATION

CECI N'EST PAS UNE INCITATION AU PIRATAGE

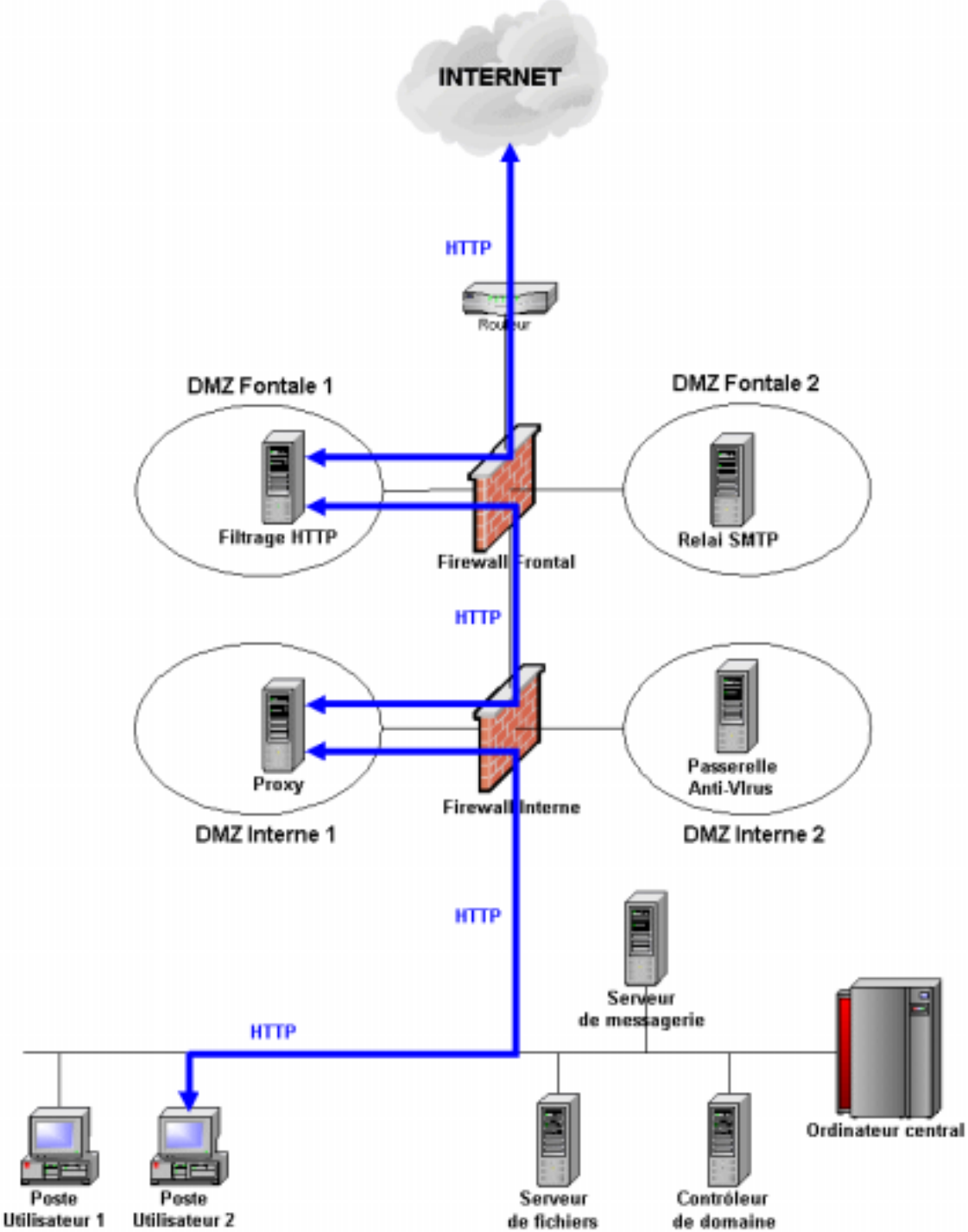
[0x4F 0x55 0x20 0x50 0x41 0x53]

INTRODUCTION

- Le SI des entreprises est-il vraiment menacé ?
- Si oui alors est-ce que tous ces jolis logiciels et ces gentils consultants, RSI et autres RSSI sont suffisants (nécessaires ?) à la protection du SI ?
- Compromettre le SI avec un cheval de Troie : la faisabilité, la facilité, l'efficacité ?
- Étapes d'une compromission par l'exemple avec un SI fictif mais un cheval de Troie réel et réaliste

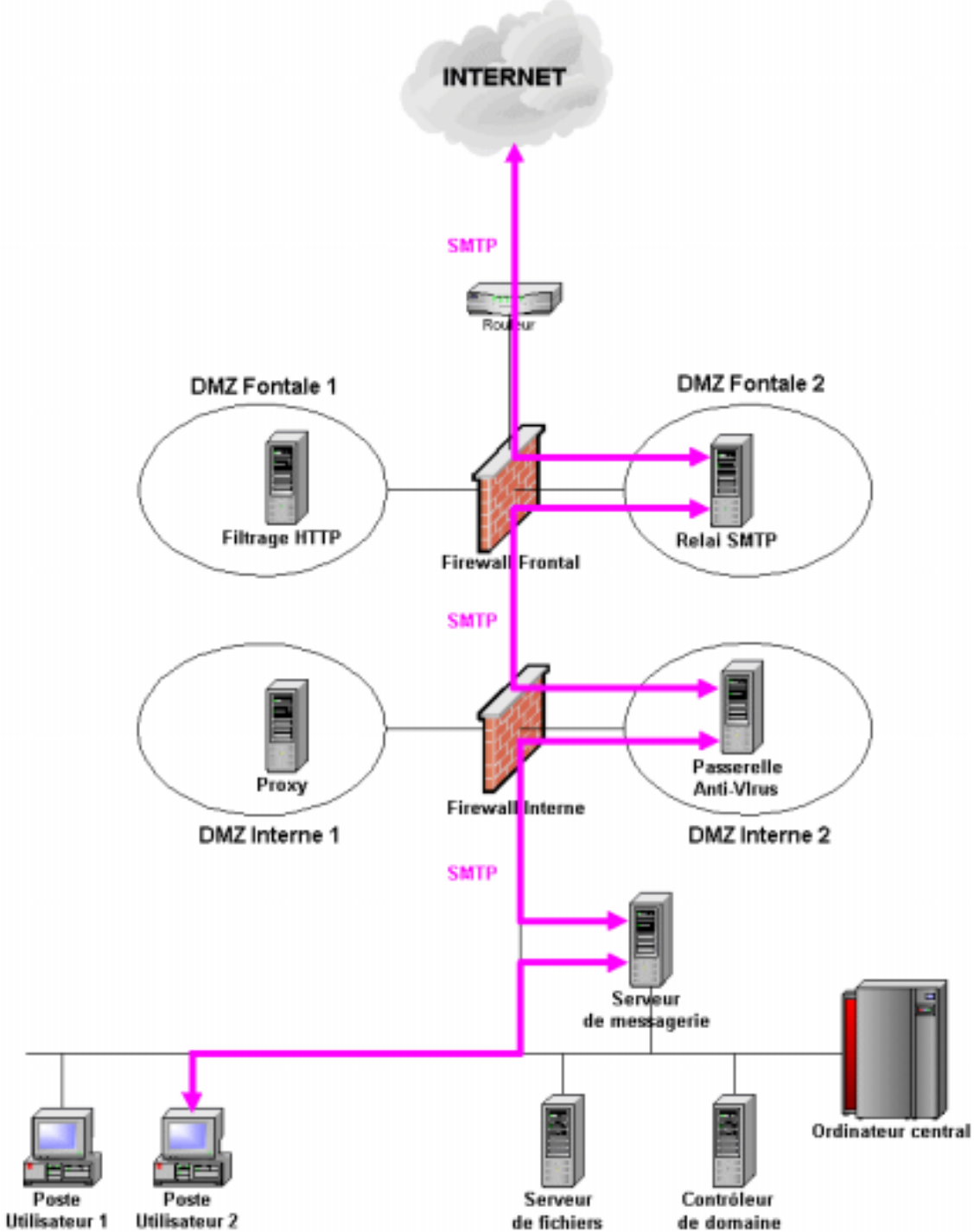
Architecture de la cible (1)

- Accès au Web
  - Proxy Squid avec authentification des utilisateurs
  - Seul HTTP autorisé vers Internet depuis le poste
  - Filtrage de contenu HTTP
  - Filtrage d'URLs de sites non productifs (black list)


INTERNET
HTTP
Routeur
DMZ Fontale 1
DMZ Fontale 2
Filtrage HTTP
Firewall Frontal
Relai SMTP
HTTP
Proxy
Passerelle
Anti-Virus
Firewall Interne
DMZ Interne 1
DMZ Interne 2
HTTP
Serveur
de messagerie
HTTP
Ordinateur central
Poste
Utilisateur 1
Poste
Utilisateur 2
Serveur
de fichiers
Contrôleur
de domaine

Architecture de la cible (2)

- Accès à la messagerie
  - Anti-virus sur le poste
  - Anti-virus sur le serveur de messagerie
  - Relais SMTP avec filtrage anti-virus
  - Filtrage d'extension


INTERNET
SMTP
Routeur
DMZ Fontale 1
DMZ Fontale 2
Filtrage HTTP
Firewall Frontal
Relai SMTP
SMTP
Proxy
Passerelle
Anti-Virus
Firewall Interne
DMZ Interne 1
DMZ Interne 2
SMTP
Serveur
de messagerie
Ordinateur central
Poste
Utilisateur 1
Poste
Utilisateur 2
Serveur
de fichiers
Contrôleur
de domaine

Architecture de la cible (3)

- Protection du poste utilisateur
  - Windows 2000 SP4 + hotfixes à jour
  - Droits utilisateur de base sur le poste
  - Anti-virus à jour
  - Firewall personnel

PROFILING DU SYSTEME D'INFORMATION

Récupération d'informations (1)

- Mode non intrusif
  - Recherches d'informations sur les sites Web (moteurs, newsgroups, mailing-list, sites institutionnels, partenaires, fournisseurs, clients, registre du commerce, brevets, interviews, …)
  - Quelles informations : e-mails, profil de l'entreprise, données techniques sur le SI

Anonymat : surfer depuis un cyber café, un AP gratuit ou celui du voisin ; chiffrement des informations récupérées

Récupération d'informations (2)

- Mode intrusif
  - Web Bug

```
<IMG src="http://monsiteamoi.fr/env.php">

[28/03/05 - 13:01:34] - 12.34.56.78
 HTTP_USER_AGENT
 Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)
 HTTP_VIA
 1.0 proxy.victime.com:8080 Squid/2.3.STABLE1)
 HTTP_X_FORWARDED_FOR
```

  - Inopérant si proxy avec authentification ou blocage du téléchargement automatique des images

Récupération d'informations (3)

- Mode intrusif
  - Envoi d'un e-mail avec un lien sur une page d'un site contrôlé (avec une redirection sur une page officielle)
  - Les infos obtenues sont identiques (à la différence qu'il s'agit de la version du navigateur et non du client de messagerie)

Anonymat : prise de contrôle d'un site web avec du PHP ; accès via des relais et/ou depuis une origine banalisée ; chiffrement

Récupération d'informations (4)

- Mode intrusif
  - Envoi d'un e-mail avec un destinataire inexistant, informations dans l'en-tête du message d'erreur

```
Received: from y.y.com ([172.18.1.12]) by z.y.com
  with Microsoft SMTPSVC(5.0.2195.5329);
Received: from x.y.com (unverified) by y.y.com
  (Content Technologies SMTPRS 4.2.10)
with ESMTP id <xxxxxxx@y.y.com> for <bob@y.com>;
[...]
X-BrightmailFiltered: true
X-Brightmail-Tracker: XXX==
```

Anonymat : prise de contrôle d'un serveur pour l'envoi d'e-mails ; accès via des relais et/ou depuis une origine banalisée

Récupération d'informations (5)

- Mode intrusif
  - Envoi d'un e-mail classique, informations identiques avec en plus la version du client de messagerie

```
X-Mailer: Lotus Notes Release 5.0.3 (Intl) 21 March 2000
```

  - Détection du filtrage d'extension par envoi d'un e-mail avec le type de fichier en pièce jointe vers un destinataire inconnu (message d'erreur alors aucun filtrage)

Récupération d'informations (6)

- Mode intrusif
  - Détection du filtrage anti-virus par envoi d'un e-mail avec un virus (genre `eicar.com` ou un vrai), si réception d'un message d'erreur alors aucun filtrage)
  - Il arrive que l'anti-virus envoie un message à l'expéditeur lors d'une détection

```
Scanned by ScanMail for Lotus Notes 2.6 SP1
with scanengine 7.000-1011
and pattern version 2.522.00
```

INTRODUCTION DU CHEVAL DE TROIE

- Objectifs à atteindre à tout prix
  - Réception du cheval de Troie sur le poste cible
  - Exécution du cheval de Troie
- Pour y parvenir à distance deux vecteurs principaux
  - Pièce jointe d'un e-mail
  - Téléchargement depuis un site Web
- Les exemples présentés sont classiques mais relativement efficaces sachant que les vecteurs ne dépendent que de l'imagination et des compétences

INTRODUCTION DU CHEVAL DE TROIE

Pièce jointe (1)

- Format ZIP
  - Classique fichier zippé avec mot de passe
  - Modification de l'en-tête zip : marquer le zip comme chiffré, taille de décompression importante, modification de l'extension du fichier zippé, …
- Word et contrôle OLE
  - Encapsulation de l'exe dans un fichier Word
  - Outrepasser le filtrage et induire l'utilisateur en erreur en modifiant directement le fichier Word

INTRODUCTION DU CHEVAL DE TROIE

Pièce jointe (2)

- Excel et macro
  - Mise à jour du code de la macro via Internet ou des données stockées dans le classeur Excel (cellules, commentaires, …)
  - Téléchargement du code depuis Internet avec un objet COM ou directement des API comme `URLDownloadToFile`
  - Protection contre l'auto-update de code depuis Office 2002

INTRODUCTION DU CHEVAL DE TROIE

Internet (1)

- Concept de contrôle ActiveX
  - Un composant logiciel (une DLL) s'intégrant dans un navigateur
- Modèle de sécurité
  - Un ActiveX peut être marqué comme « sûr » ou « non sûr » (choix effectué par le développeur)
  - Deux solutions pour introduire le Cheval de Troie : forcer l'installation d'un ActiveX malicieux, utiliser les ActiveX déjà installés

INTRODUCTION DU CHEVAL DE TROIE

Internet (2)

- Génération d'un ActiveX malicieux effectuant le téléchargement du cheval de Troie, il est marqué comme « sûr » et signé par un faux certificat Microsoft
- Conditions d'exécution
  - L'utilisateur doit être administrateur
  - Le navigateur doit être Internet Explorer
  - L'utilisateur doit accéder à la page contenant l'ActiveX et accepter son exécution

INTRODUCTION DU CHEVAL DE TROIE

Internet (3)

- Windows intègre des dizaines de contrôles ActiveX, certains permettent le création de fichiers, …
- Utilisation des contrôles `Scripting.FileSystemObject` et `WScript.Shell` :
  - Marqués comme « non sûr » ils ne peuvent être utilisés par une page de la zone externe
  - Fonctionne avec une page HTML envoyée par mail

INTRODUCTION DU CHEVAL DE TROIE

Internet (4)

- Conditions d'exécution
  - Le navigateur doit être Internet Explorer
  - Ouverture d'un fichier HTML sur le disque dur
  - L'utilisateur doit accepter l'exécution de l'ActiveX

PRESENTATION DU CHEVAL DE TROIE

- Pour établir un canal de communication avec le pirate
  - Client initiant des connexions vers un serveur
  - Communiquer via des canaux cachés au sein des protocoles autorisés
  - Obtenir les paramètres de connexion (adresse du proxy, paramètres d'authentification)
- Une fois le canal établit
  - Survie (au sein de la session utilisateur et au redémarrage)
  - Stabilité des transferts et furtivité système et réseau

PRESENTATION DU CHEVAL DE TROIE

Présentation de Fratus (1)

- Établissement d'un canal par la backdoor Fratus :
  - Client initiant des connexions vers un serveur et une partie cliente communiquant par des canaux cachés au sein de HTTP et HTTPS
  - Elle s'exécute comme un processus séparé et récupère les paramètres de connexion via wininet.dll (pour IE) ou les fichiers de configuration (Netscape, Firefox)

Présentation de Fratus (2)

- Limitations
  - Furtivité : processus visible dans la liste des tâches
  - Détecté par les firewalls personnels
  - Ne fonctionne pas avec un proxy requerrant une authentification

PRESENTATION DU CHEVAL DE TROIE

Présentation de Parsifal (1)

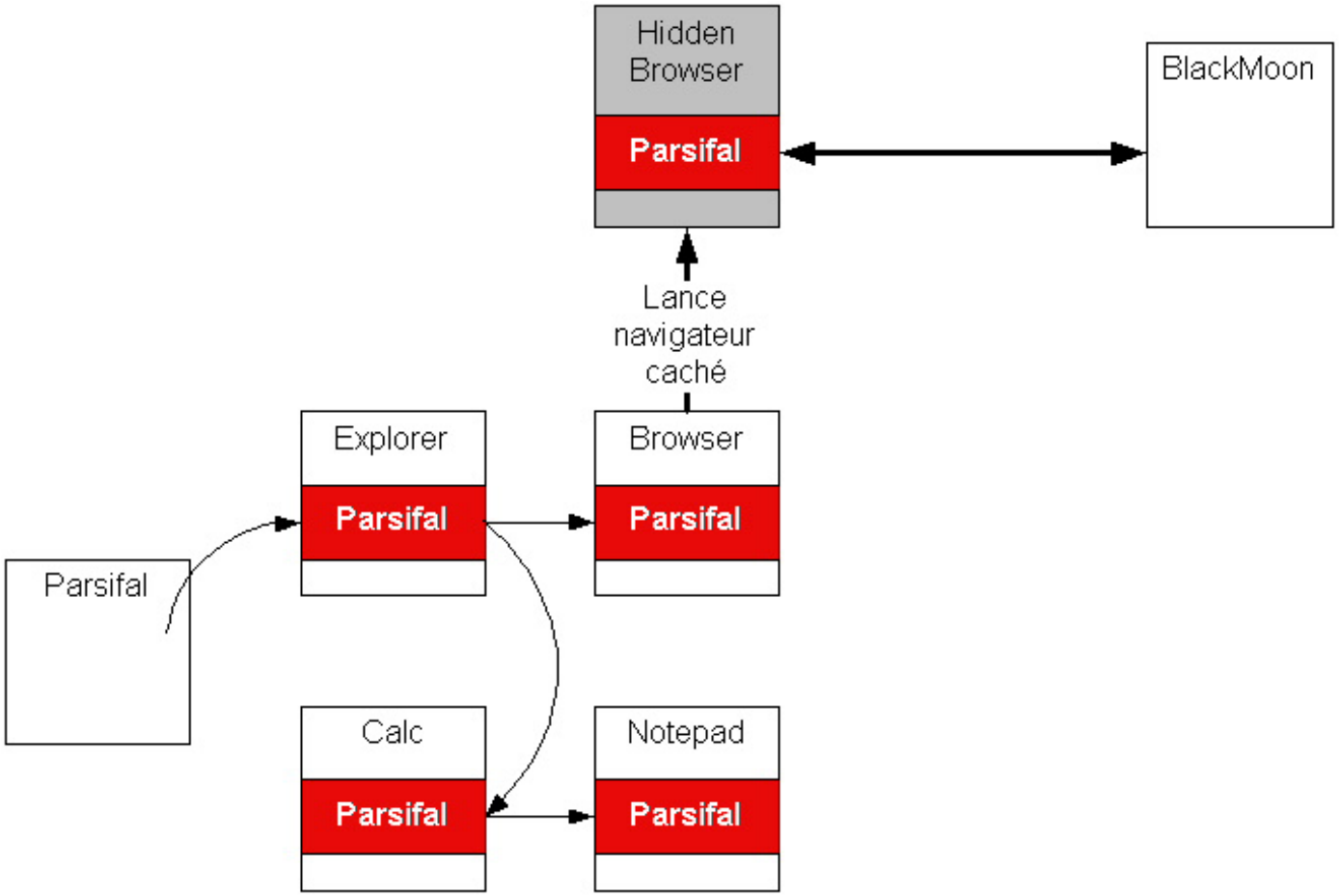
- Parsifal fonctionne sous forme de thread injecté dans les navigateurs, la récupération des paramètres de connexion se fait en hookant les fonctions `send` et `connect`
- Avantages
  - Furtivité : pas de processus supplémentaires dans la liste des tâches, pas de détection par les firewalls personnels
  - Fonctionne même si le proxy utilise une authentification simple

PRESENTATION DU CHEVAL DE TROIE

Présentation de Parsifal (2)

- Problème : la survie au cours de la session utilisateur
- Solution : Parsifal adopte un comportement viral en mémoire

PRESENTATION DU CHEVAL DE TROIE



Présentation de Parsifal (3)

- Problème : peu de connaissances sur l'architecture interne du réseau
  - Outils nécessaires pour progresser au sein du réseau non identifiés
  - L'évolutivité de la backdoor est un enjeu crucial
- Solution
  - Parsifal adopte une architecture modulaire
  - Parsifal implémente une interface standard et assure le transport des données

PRESENTATION DU CHEVAL DE TROIE

Présentation de Parsifal (4)

- Un module est une DLL uploadée sur le poste, chargée dans l'espace du navigateur, assurant des fonctionnalités
- Modules déjà implémentés

CMD	équivalent de « cmd » distant
GPW	récupère les mots de passe dans les edits box
SCAN	scanner de port (TCP SYN, connect, UDP, ping)
BNR	récupération de bannières
FIF	recherche récursive de chaîne dans les fichiers
VRS/SRV	architecture évolutive de propagation

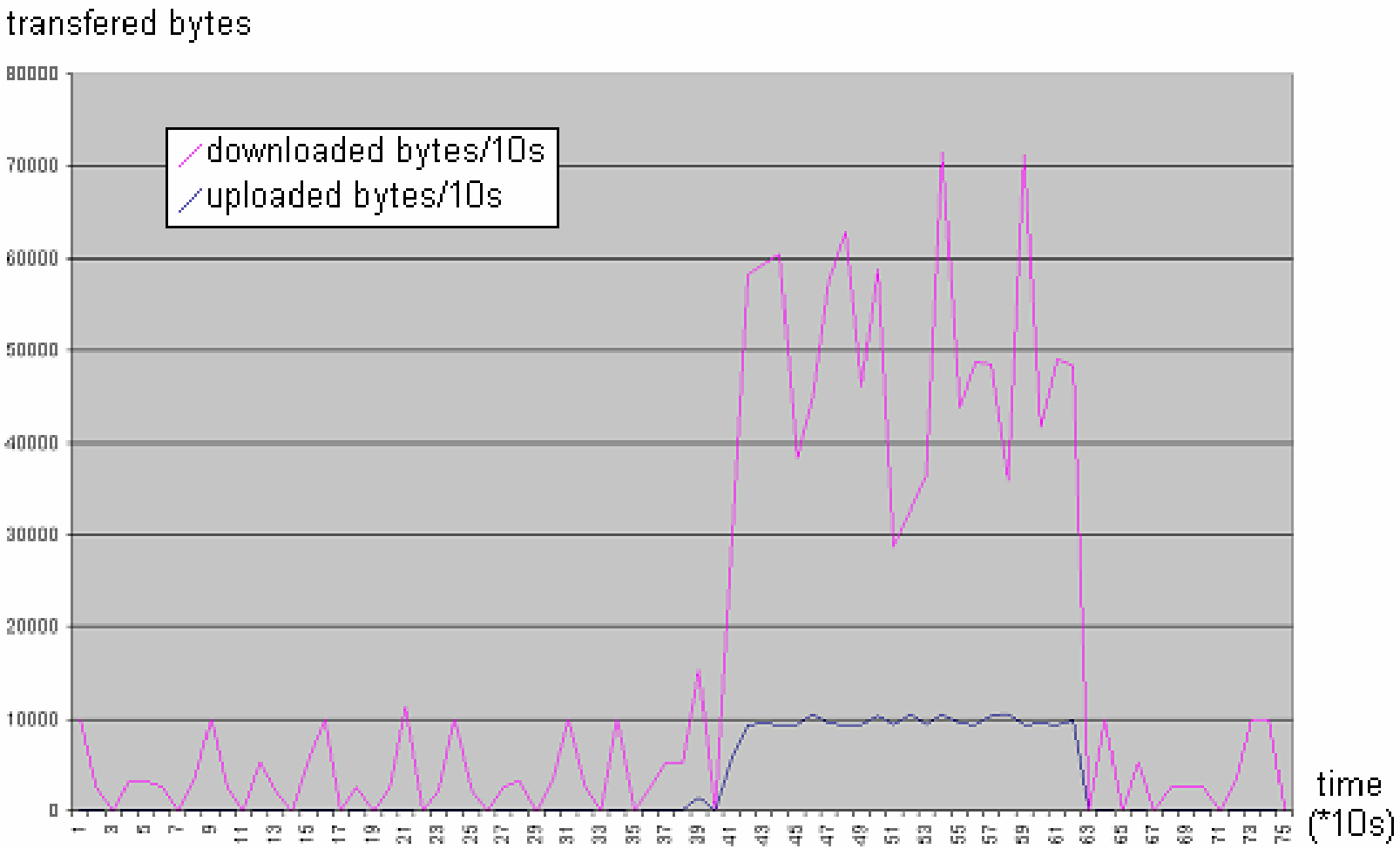
Présentation de Parsifal (5)

- Avantages
  - Possibilité d'étendre facilement les fonctionnalités de la backdoor
  - La backdoor reste de taille raisonnable

Fonctionnalités avancées : furtivité (1)

- Furtivité au niveau réseau
  - Maîtrise des vitesses de transfert
  - Choix automatique du protocole (HTTP ou HTTPS) en fonction du sens du transfert
  - Connexion de durée limitée
  - URI demandée aléatoire
  - Irrégularité du trafic
- Trafic généré par Parsifal

PRESENTATION DU CHEVAL DE TROIE



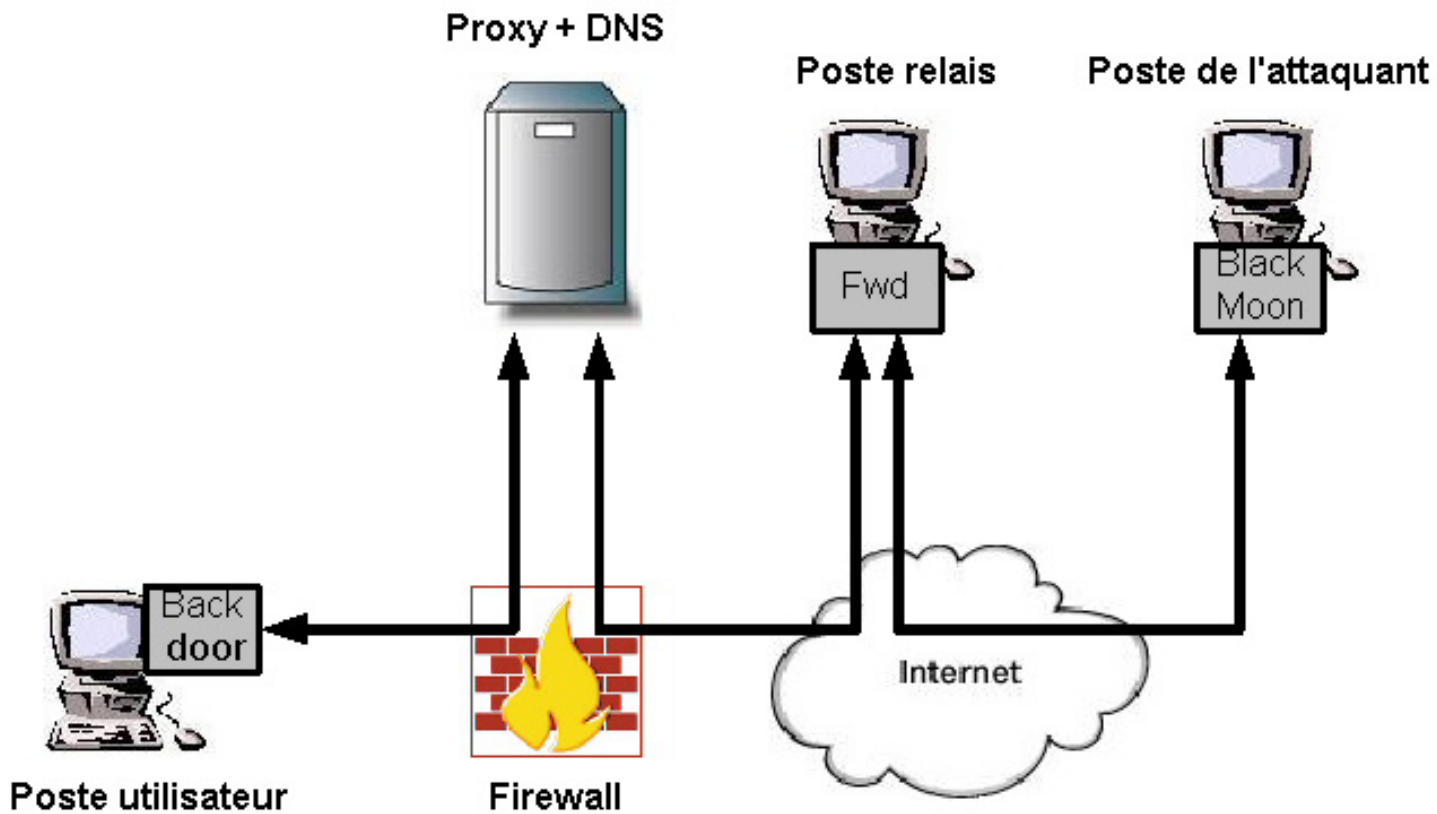
Fonctionnalités avancées : furtivité (2)

- Furtivité au niveau système
  - Exécution ponctuelle du processus
  - Fonctionnalité de rootkit user-land (système de fichiers et base de registre)
  - Fonctionnalité de rootkit mode noyau (via un module)

Fonctionnalités avancées : relais (1)

- Les communications Parsifal - BlackMoon génèrent des traces qui peuvent conduire au pirate, notamment au niveau du proxy
- Solution : passer par un relais
- Toute instance de Parsifal peut devenir un relais

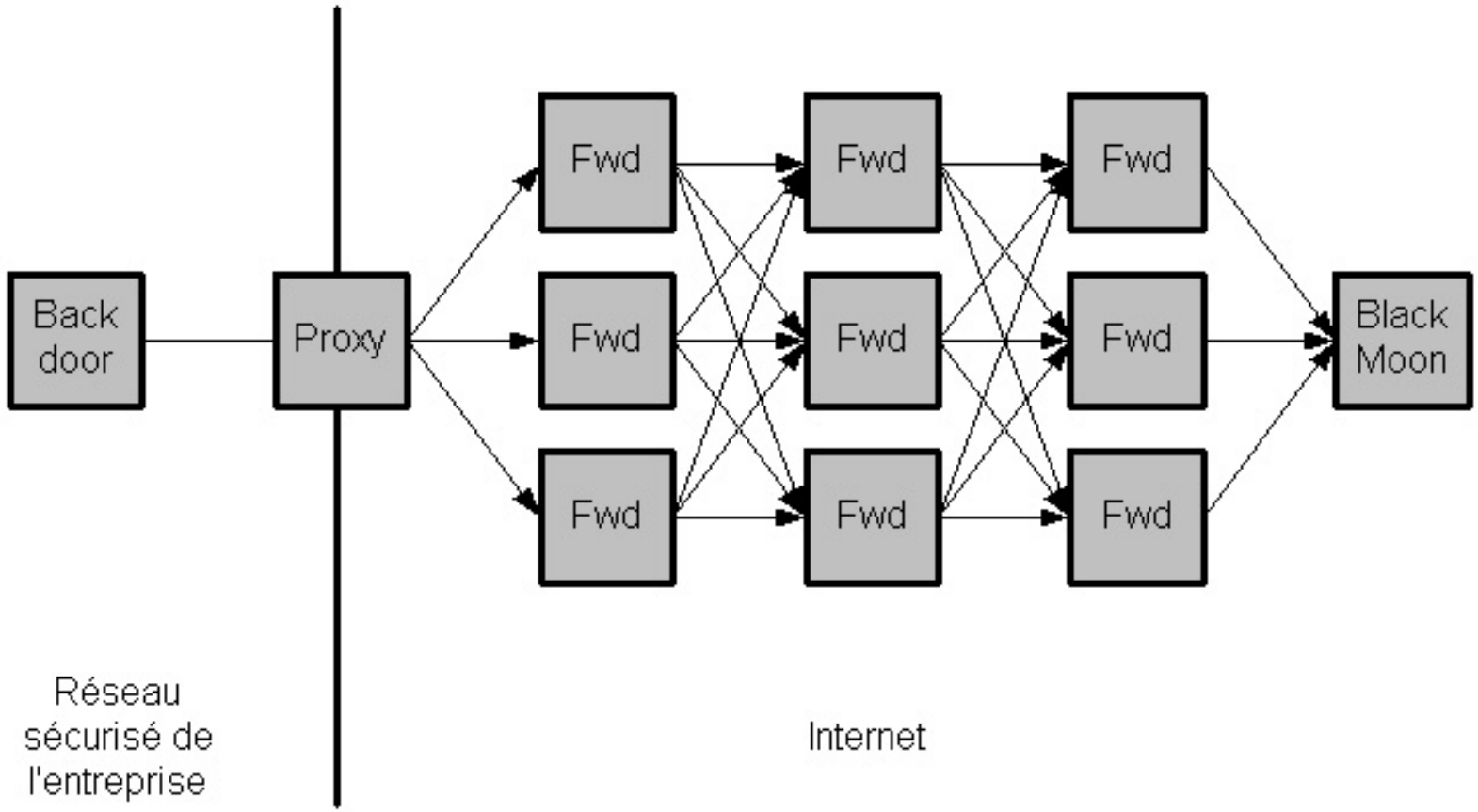
PRESENTATION DU CHEVAL DE TROIE



Fonctionnalités avancées : relais (2)

- Généralisation de ce principe de relais
  - Il ne doit exister aucune relation entre le relais et le pirate
  - Il faut que la chaîne comporte plusieurs maillons
- Le chemin varie à chaque connexion HTTP et s'adapte si un relais devient inactif

PRESENTATION DU CHEVAL DE TROIE



DANS LA PLACE

- Identification précise de l'ordinateur (système, applications, …)
- Reconnaissance du réseau (domaine, partages, utilisateurs, postes et serveurs, …)
- Augmentation de privilèges locale et globale (à l'ancienne avec des comptes faiblement protégés ou grâce à de gentils amis fournisseurs en 0days)
- Prise de contrôle d'autres machines pour assurer son maintien dans le réseau (si nécessaire)

DANS LA PLACE

- Rationalisation des données techniques récupérées en fonction de l'objectif visée (surveillance, vol de documents, de données, …)
- Identification des éléments du SI en fonction de l'objectif (réseau, serveurs, applications, protections)
- Upload des outils nécessaires
- Sortie des données via le cheval de Troie

Anonymat : effacer les traces ; transmissions des données aux moments adéquats

CONCLUSION

- Compromission d'un SI même bien protégé tout à fait possible et sans doute une réalité sur une attaque ciblée
- Ce type de cheval de Troie est opérationnel et ne demanderait que du temps et quelques amis motivés pour être toujours plus efficace
- Ce temps certains sont prêts à le payer pour obtenir des informations stratégiques et/ou confidentielles

CONCLUSION

- Les solutions sont connues et classiques (sans doute pas suffisantes) mais est-ce que les responsables cherchent vraiment à protéger leur SI ou seulement à faire de la politique, du commercial ou du banal carriérisme ?