Les rootkits navigateurs

Christophe Devaux - christophe.devaux@sogeti.com
Julien Lenoir - julien.lenoir@sogeti.com

Sogeti ESEC

Agenda

Qu'est ce qu'un rootkit ?

Définition

Programme malveillant permettant à un attaquant de garder un contrôle partiel ou total sur un système après une intrusion

Propriétés des rootkits

- Furtivité
- Persistance
- Résistance

Exemples

- Windows : NtIllusion
- Linux : SucKIT
- Virtualisation : BluePill

Pourquoi un rootkit pour navigateur ?

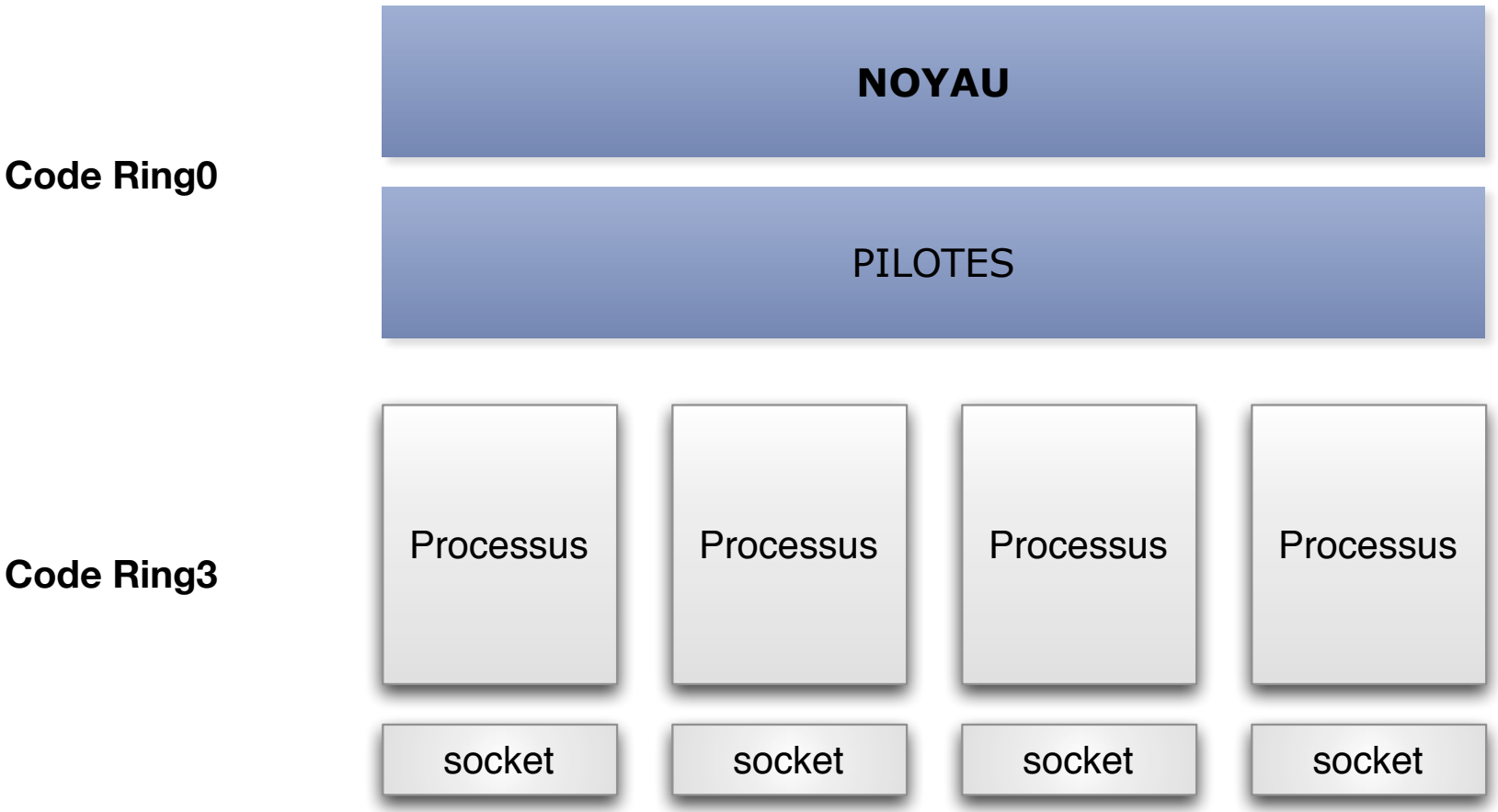
Une place centrale

- Installés par défaut sur tous les postes de travail
- Connectés à internet HTTP/HTTPS
- Font transiter des données sensibles (mots de passe, contenu confidentiel, ...)

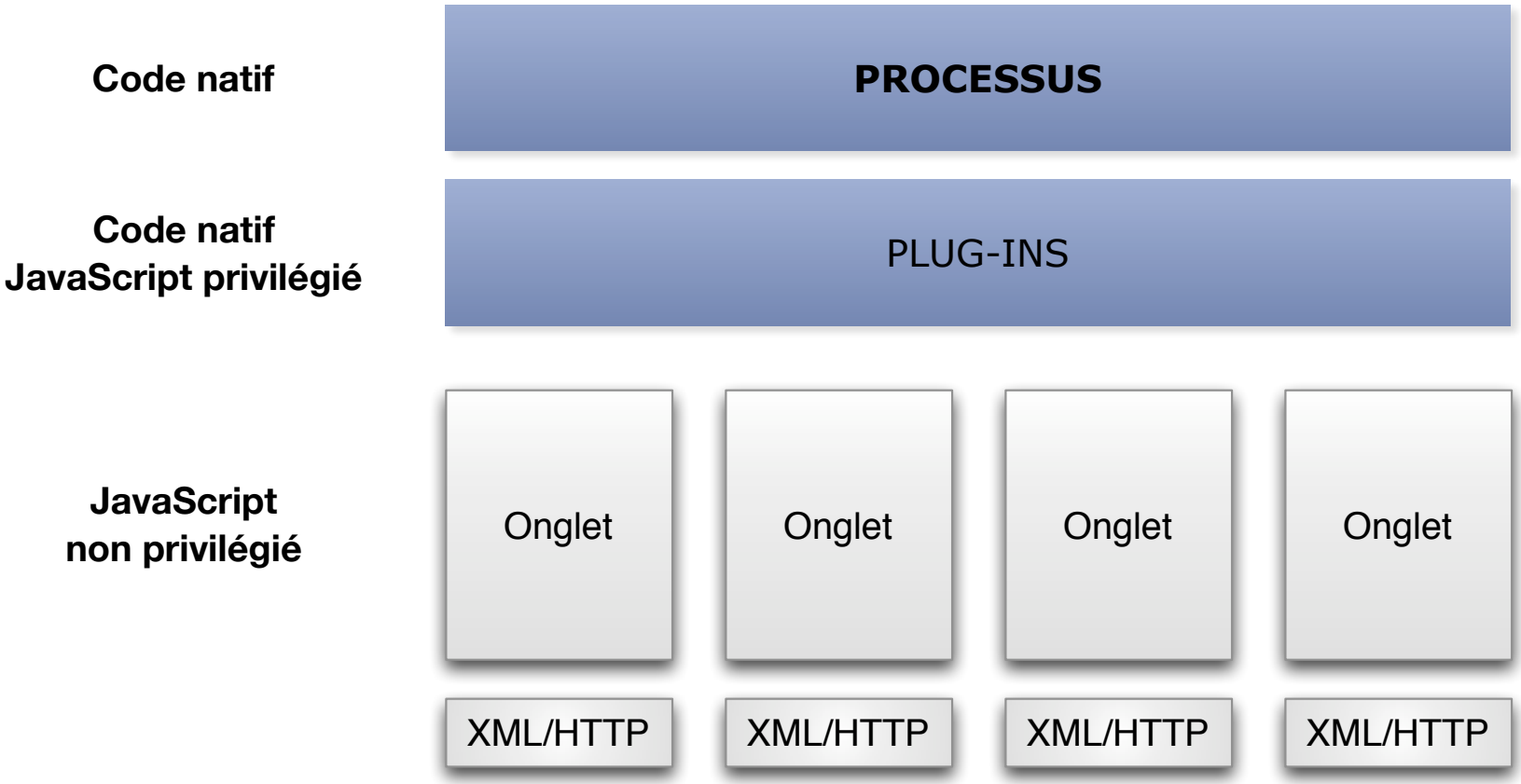
Des minis systèmes d'exploitation

- De plus en plus complexes
- Mécanismes de plug-ins
- Un nombre croissant de technologies supportées

Architecture d'un système d'exploitation



Architecture d'un navigateur



Contraintes et limites

Contraintes

- Droits restreints
- Privilégier la furtivité

Le système d'exploitation hôte

- Détection par un programme tiers
- Traces sur le réseau

FIREFOX

Plan

Principes généraux

Construire une extension pour Firefox comme un rootkit de type module kernel

Interêts :

- Se charge et reste persistant
- Se cache elle-même (du point de vue du navigateur)
- Communique et répond à des ordres distants

Contraintes :

- Doit être exploitable avec le minimum de droits
- Se concentrer sur la furtivité
- Multiplateforme

Qu'est ce qu'une extension ?

Une extension...

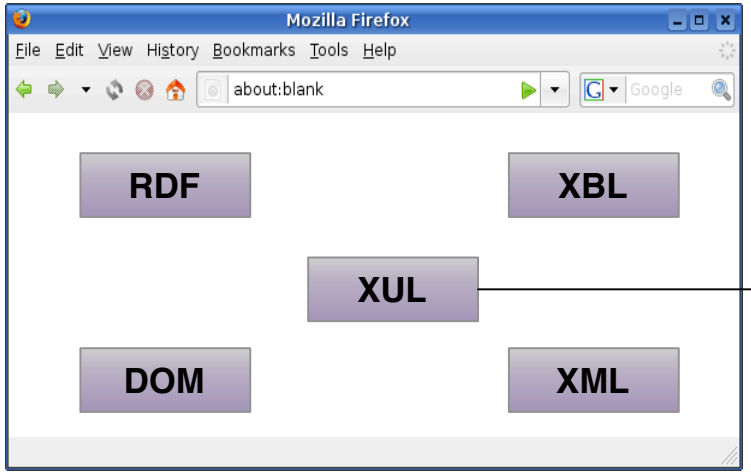
- est un simple fichier compressé contenant du JavaScript/XUL/CSS/binaires/...
- peut être multiplateforme
- ajoute des **surcouches** sur les fichiers XUL de Firefox

Une surcouche fournit un mécanisme pour :

- ajouter de nouvelles interfaces utilisateurs
- remplacer des parties de code XUL pré-existant
- réutiliser des parties de code XUL ou d'interfaces

Avec une surcouche sur *browser.xul*, nous pouvons contrôler la fenêtre principale de Firefox

Qu'est ce qu'une extension ?



FICHIERS DE L'EXTENSION MALICIEUSE

/chrome.manifest
/chrome/content/mozilla/core.js
/chrome/content/mozilla/config.js
/chrome/content/mozilla/browserOverlay.xul
/chrome/content/mozilla/rsa.js
/chrome/content/mozilla/id.js
/chrome/content/mozilla/browser.js
/chrome/content/mozilla/log.js
...

SURCOUCHE

FICHIERS XUL DE FIREFOX

/browser/content/browser.xul
/browser/content/preferences.xul
/browser/content/history/history-panel.xul
/browser/content/aboutDialog.xul
/browser/content/safeMode.xul
/mozapps/content/extensions/extensions/xul
/mozapps/content/profile/profileSelection.xul
...

Installation

Installation normale :

Fichier XPI installé par ingénierie sociale, courriels, P2P, ...

En utilisant un infecteur :

Executable qui modifie les fichiers du manager d'extensions de Firefox

En utilisant une vulnerabilité dans Firefox :

Qui permet une execution de code (MFSA 2008-34, MFSA 2008-41, ...)

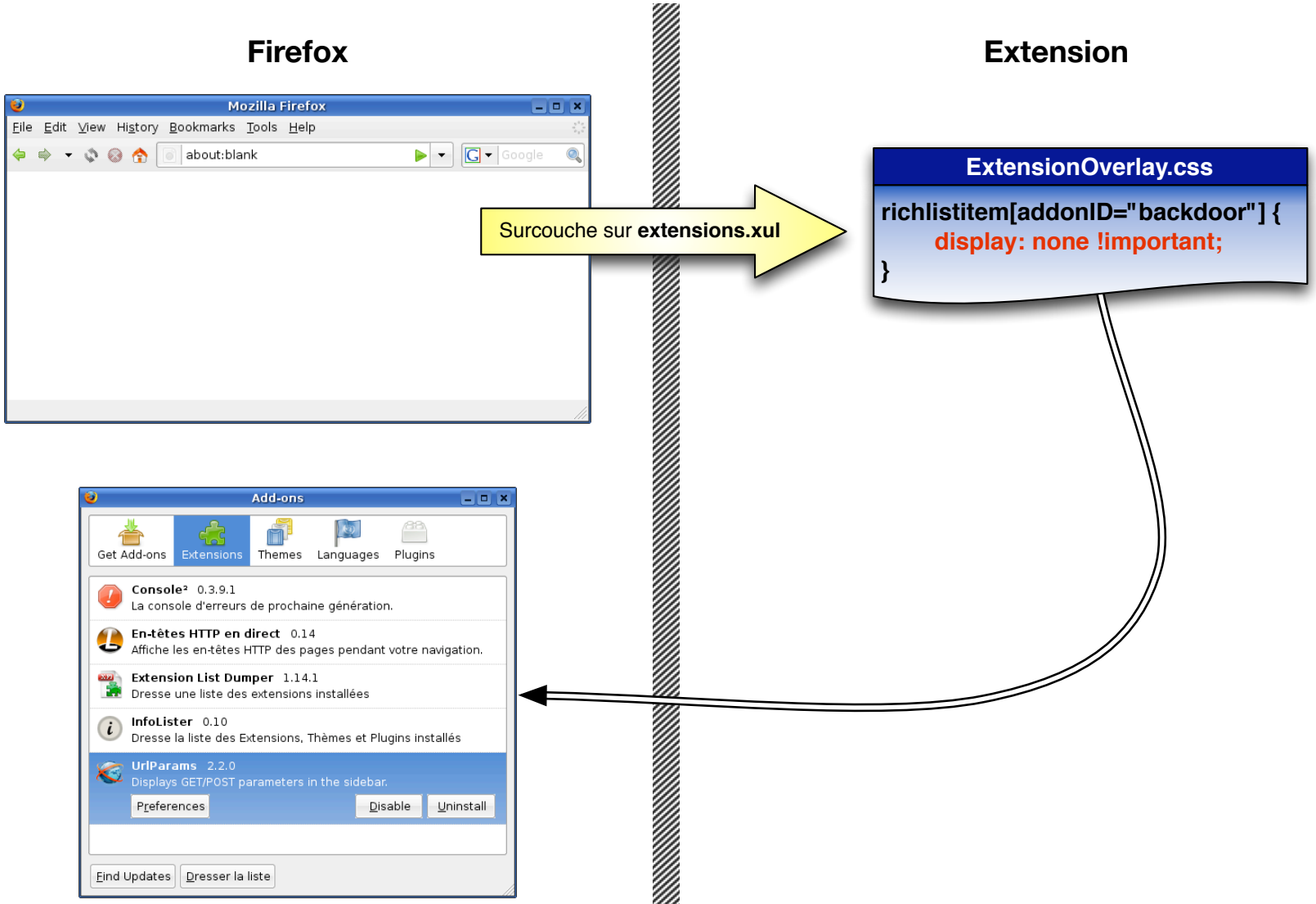
Plan

Cacher l'extension

Trois méthodes :

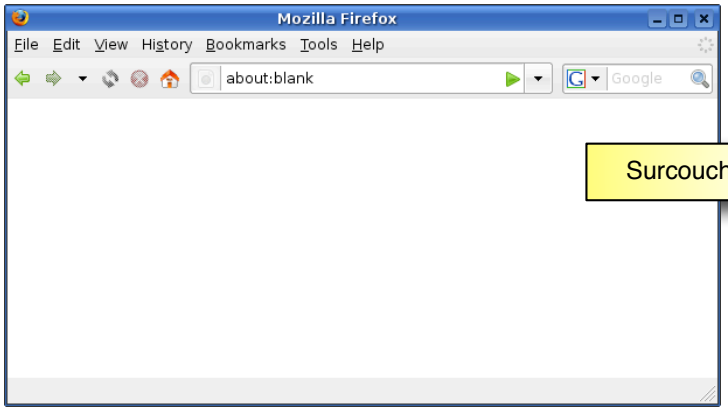
- Utiliser une feuille de style (fichier CSS) :
  - **L'utilisateur** ne voit plus l'extension
- Supprimer l'extension du composant *Gestionnaire d'extensions* :
  - **Firefox** ne voit plus l'extension
- Infecter une extension déjà installée :
  - Comportement traditionel d'un virus

Cacher l'extension



Cacher l'extension

Firefox



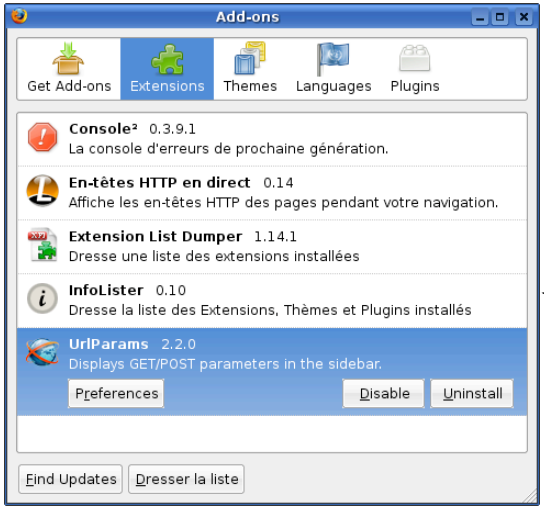
Surcouche sur **browser.xul**

Extension

Supprimer l'extension du gestionnaire d'extensions

```
function Hide()
{
    va xtensionDS = Components.classes["@mozilla.org/extensions/mana...
      Service  = Components.classes["@mozilla.org/rdf/rdf-service;1"]...
               = RDFService.GetResource("urn:mozilla:item:root");
    va tainer    = Components.classes["@mozilla.org/rdf/container;1"].Cr...
    Container.Init(extensionDS, root);
    var elements = Container.GetElements();

    while (elements.hasMoreElements())
    {
        var element        = elements.getNext();
        var elementRSC = element.QueryInterface(Components...
        var id                = elementRSC.Value.replace("urn:mozilla:item:", "");
        if (id == "backdoor") {
            Container.RemoveElement(element, true);
        }
    }
}
```



Plan

Communication

Processus de communication :

- Communication avec un serveurs HTTP(S) externe : passer les pare-feux
- XMLHttpRequest
- Interroge, execute, renvoie le résultat au maître
- Protocole chiffré utilisant RSA et RC4

Communication : contrôle des cibles

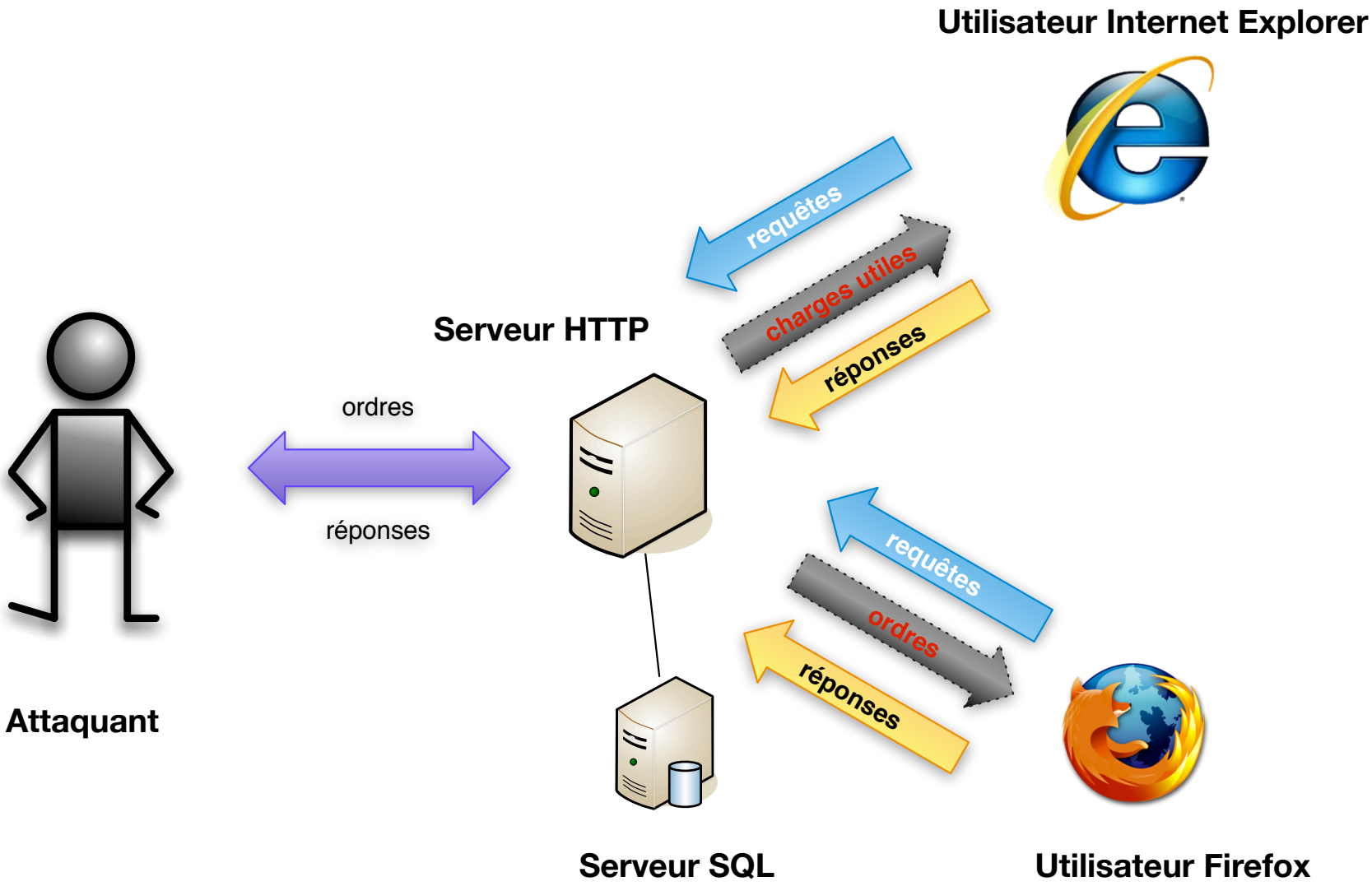
Pourquoi utiliser un serveur Web pour contrôler le rootkit ?

- Les navigateurs communiquent naturellement avec des serveurs Web
- L'envoie, la réception et le traitement de requêtes HTTP/XML sont supportés nativement par les navigateurs Web

Remarque

Le serveur Web peut être caché en utilisant une méthode fast flux

Architecture globale



Propagation

Mécanismes de propagation :

- Voies traditionelles : courriels, P2P, autres vers, ...
- Surveiller les webmails : intercepter les emails et ajouter un infecteur en fichier joint
- Récolter les courriels dans les pages Web visitées
  - Firefox peut envoyer des courriels de lui-même

Plan

XPCOM

XPCOM (Cross Platform Component Object Model)

- XPCONNECT permet l'utilisation de nombreux langages
- inclut des interfaces pour :
  - la gestion des composants
  - l'abstraction des fichiers
  - la gestion de la mémoire

	Composant	**Interface**	**Méthode**
Mots de passe	login-manager	nsILoginManager	getAllLogins()
Cookies	cookiemanager	nsICookieManager	enumerator
Favoris	nav-bookmarks-service	nsINavBookmarksService	executeQuery()
Historique	nav-history-service	nsINavHistoryService	executeQuery()
Executer	process/utils	nsIProcess	run()
Utiliser une socket	network/socket-transport-service	nsISocketTransportService	CreateTransport()

AddEventListener

AddEventListener

- Associer une fonction à un événement particulier
- Idéal pour surveiller l'activité d'un utilisateur

Action	**Événement à écouter**	
un onglet est ouvert	DOMContentLoaded	**enregistrer la navigation**
un onglet est fermé	TabClose, unload	**enregistrer la navigation**
une touche est pressée	keypress	**enregistrer le clavier**

- L'enregistrement est completé par un enregistrement des entêtes HTTP
- Les fichiers de logs sont chiffrés dans le cache du navigateur

Charges utiles

À partir de là, tout est possible 

- Voleur de mots de passe/cookies/favoris/historique
- Keyloggeur
- Prise de controle a distance de la machine(Shell "'ConnnectBack"')
- Sniffer (requêtes HTTP)
- Botnet
- Plate-forme de SPAM
- Interaction avec le système d'exploitation
- ...

Démonstration

Plan

Conclusion

- Un réel problème de **conception** et pas de solution simple à mettre en place
- Une extension Firefox malicieuse est facile à développer
- Il y a AUCUNE securité à propos des extensions dans Firefox

Nous ne serions pas surpris de voir ce type de spyware se développer dans le futur

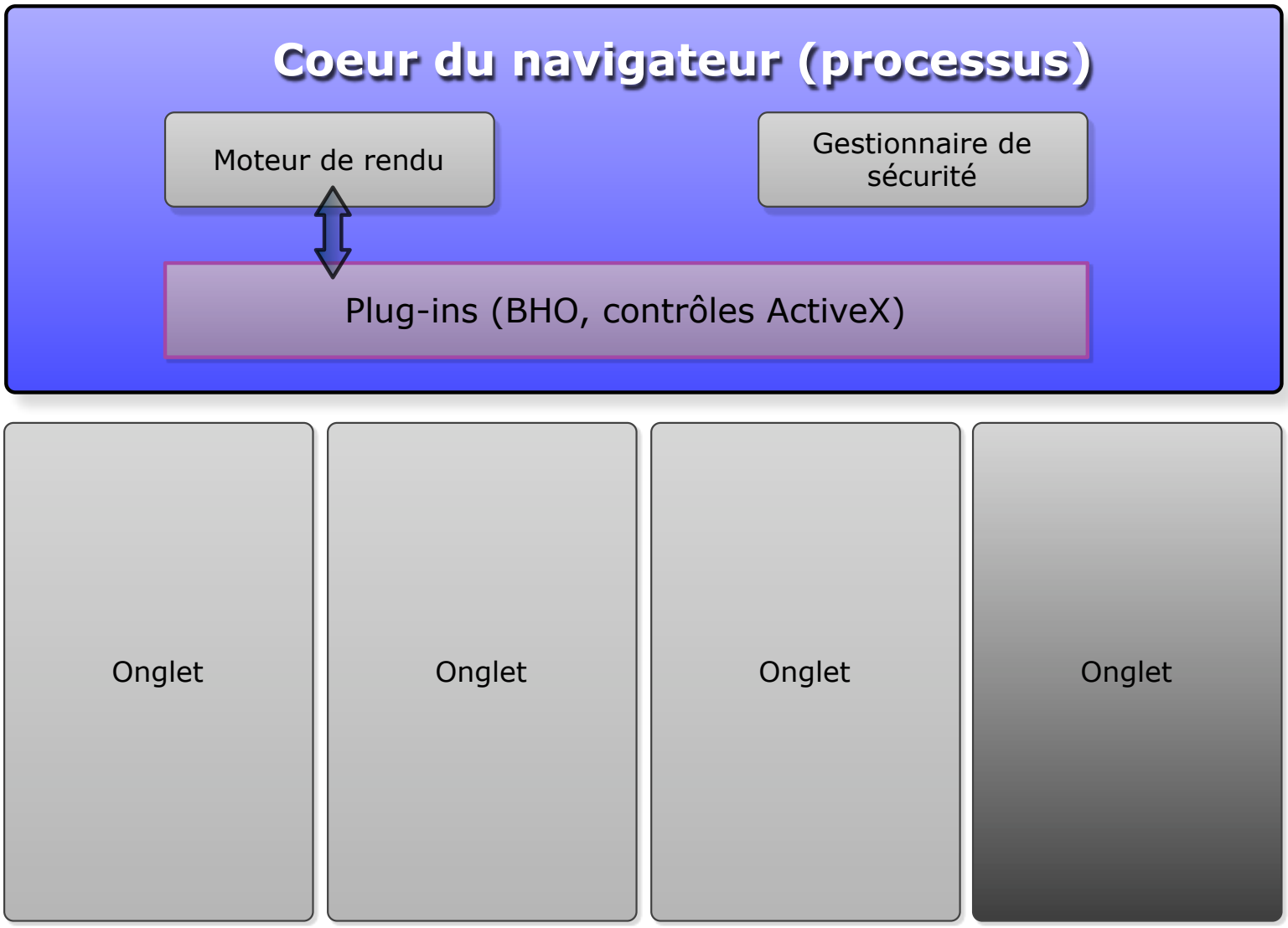
INTERNET EXPLORER 7

Un rootkit pour Internet Explorer

Contraintes

- Etre utilisable avec les droits de l'utilisateur courant
- Architecture tout-en-memoire
- Utiliser les fonctionnalités d'Internet Explorer

Plan


Coeur du navigateur (processus)
Moteur de rendu
Gestionnaire de sécurité
Plug-ins (BHO, contrôles ActiveX)
Onglet
Onglet
Onglet
Onglet

Les *Browser Helper Objects* : la menace la plus répandue

Avantage

- Prévus pour acceder au moteur de rendu

Inconvénients

- Les BHOs demandent des privilèges pour être installés
- Les BHOs laissent des traces dans la base de registre Windows
- Un composant du navigateur permet de les lister

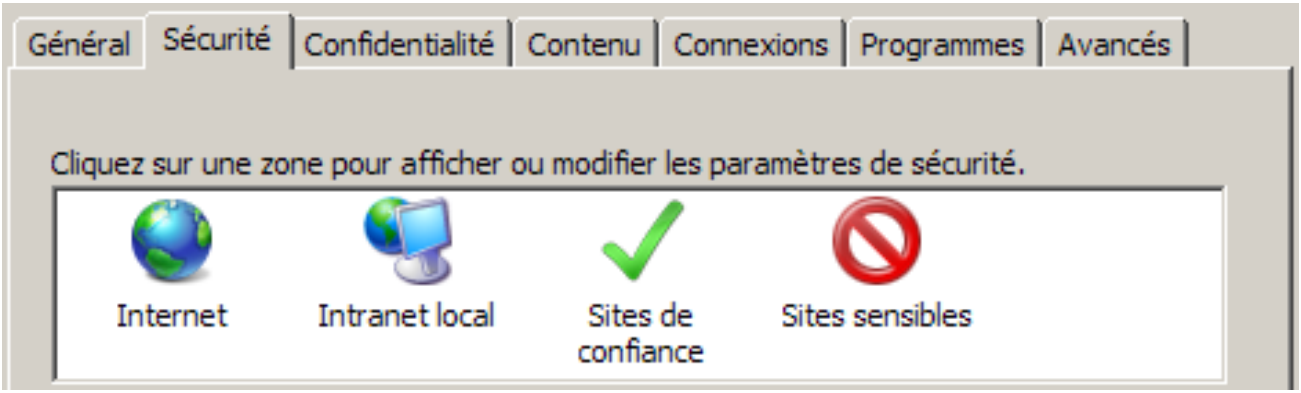
Incompatibles avec nos contraintes

On ne les utilisera pas

Les zones de sécurité

Cinq zones de sécurité

- Ordinateur local : pages Web sur les disques locaux
- Intranet : pages Web sur un Intranet
- Sites de confiance : liste blanche de sites de confiance
- Internet : pages Web qui ne rentrent pas dans les autres catégories
- Sites sensibles : liste noire de sites restreints



Paramètrage des zones de sécurité

Paramètrage

- Execution de code JavaScript
- Instanciation de composants ActiveX du système
- Sécurité de la machine Java
- Utilisation des cookies
- Communication intra-domaines

- Réglages par l'administrateur ou l'utilisateur
- Stockés dans la base de registre

Paramètrage fin

ACTION_FLAGs

Représentent toutes les actions qui peuvent être entreprises dans une zone de sécurité

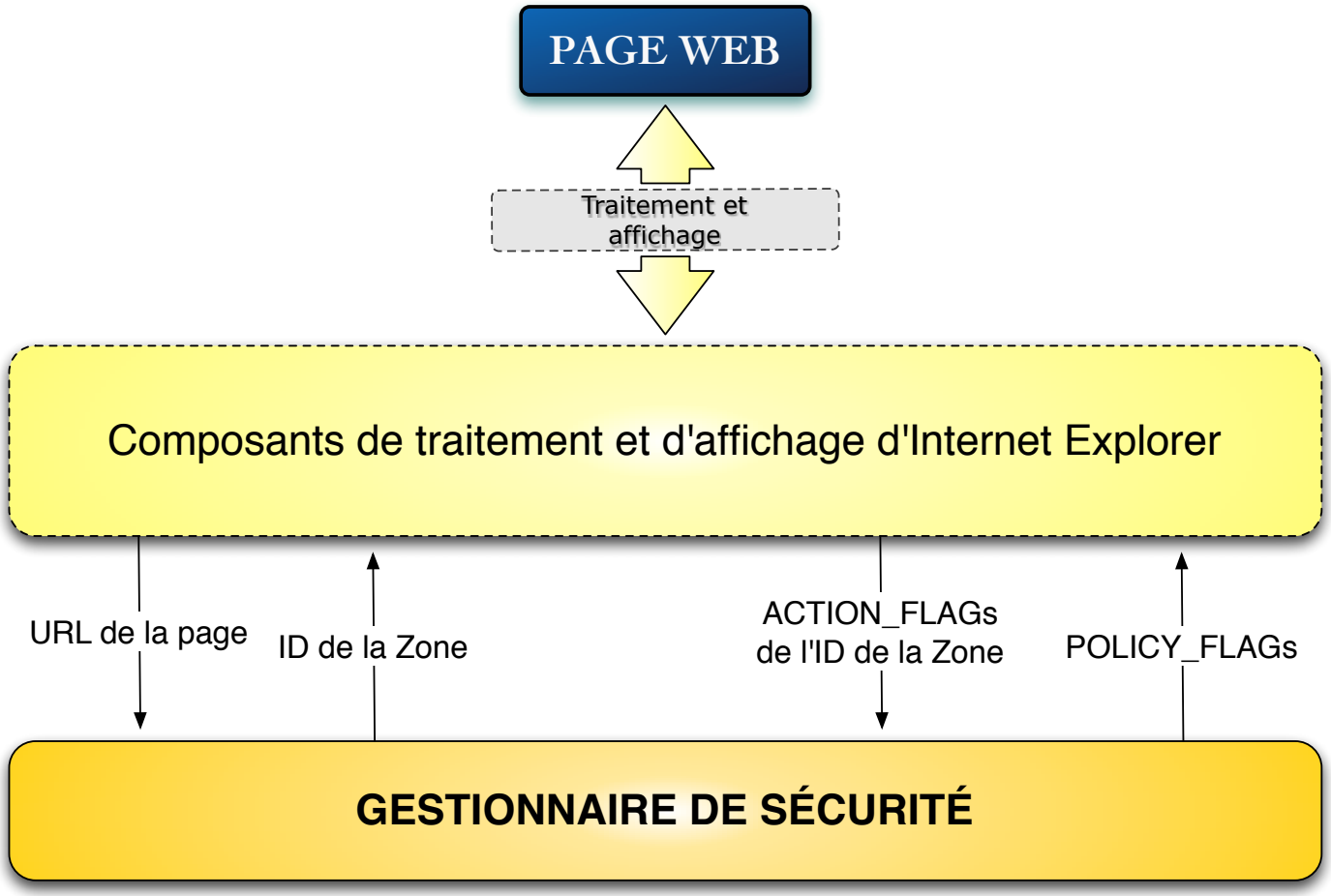
POLICY_FLAGs

Représentent comment le navigateur va réagir en fonction d'un ACTION_FLAG

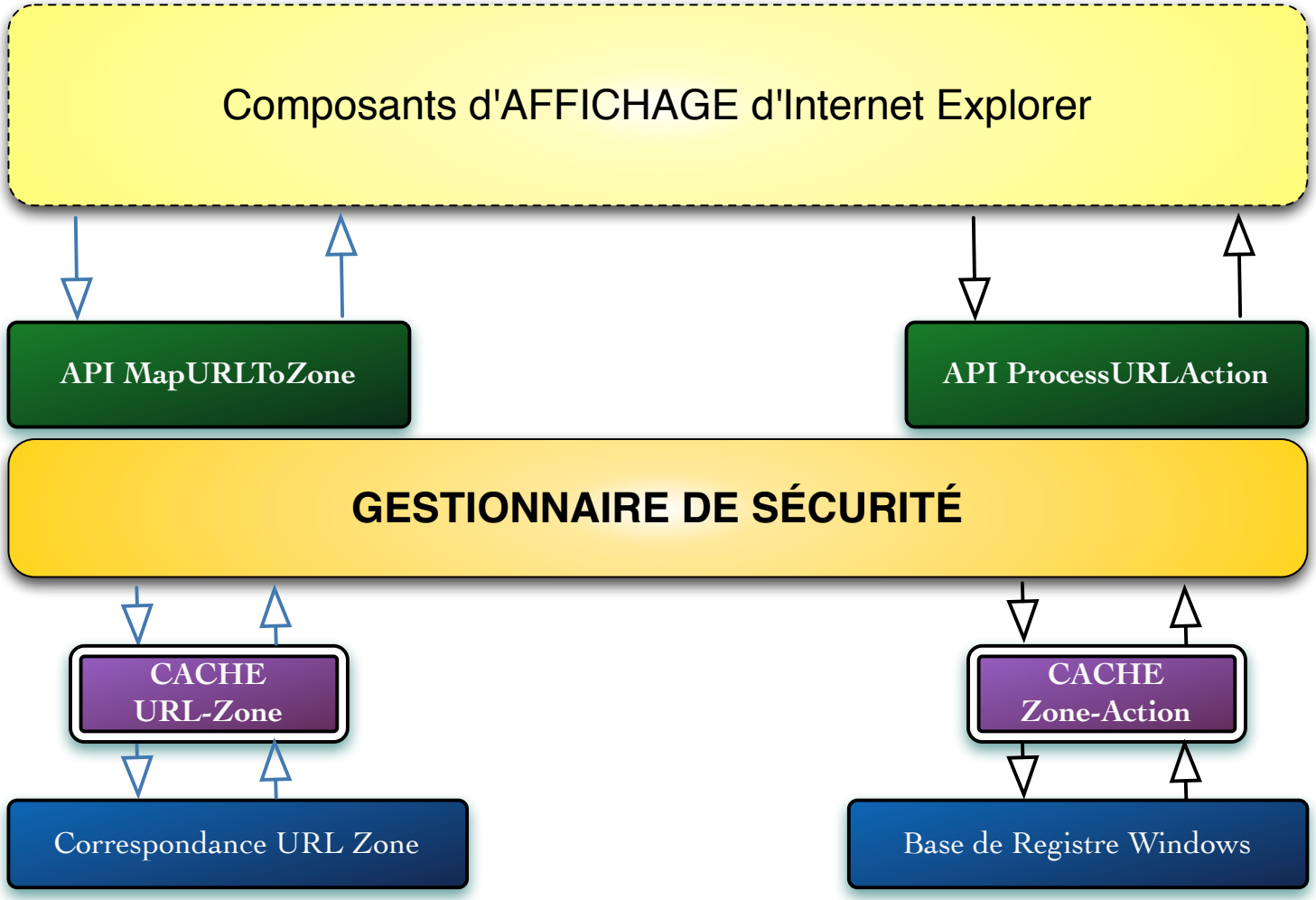
Politique de sécurité

Chaque zone a sa propre liste d'ACTION_FLAGs et de POLICY_FLAGs qui définissent sa sécurité

La sécurité appliquée a une page Web



Le gestionnaire de sécurité



Plan

Injecteur

Méthodes qui peuvent être employées

- Injecter le code depuis le système hôte
- Injecter le code à distance en utilisant une faille du navigateur
- Injecter le code en utilisant un plug-in malicieux

Module de création d'onglets : Élevation des privilèges

Le cache URL-Zone

Corruption du cache URL-Zone pour associer http ://evilsite à la zone que nous souhaitons

Le cache Zone-Action

Corruption du cache Zone-Action pour obtenir le plus haut niveau de privilèges sur la zone associée à notre site

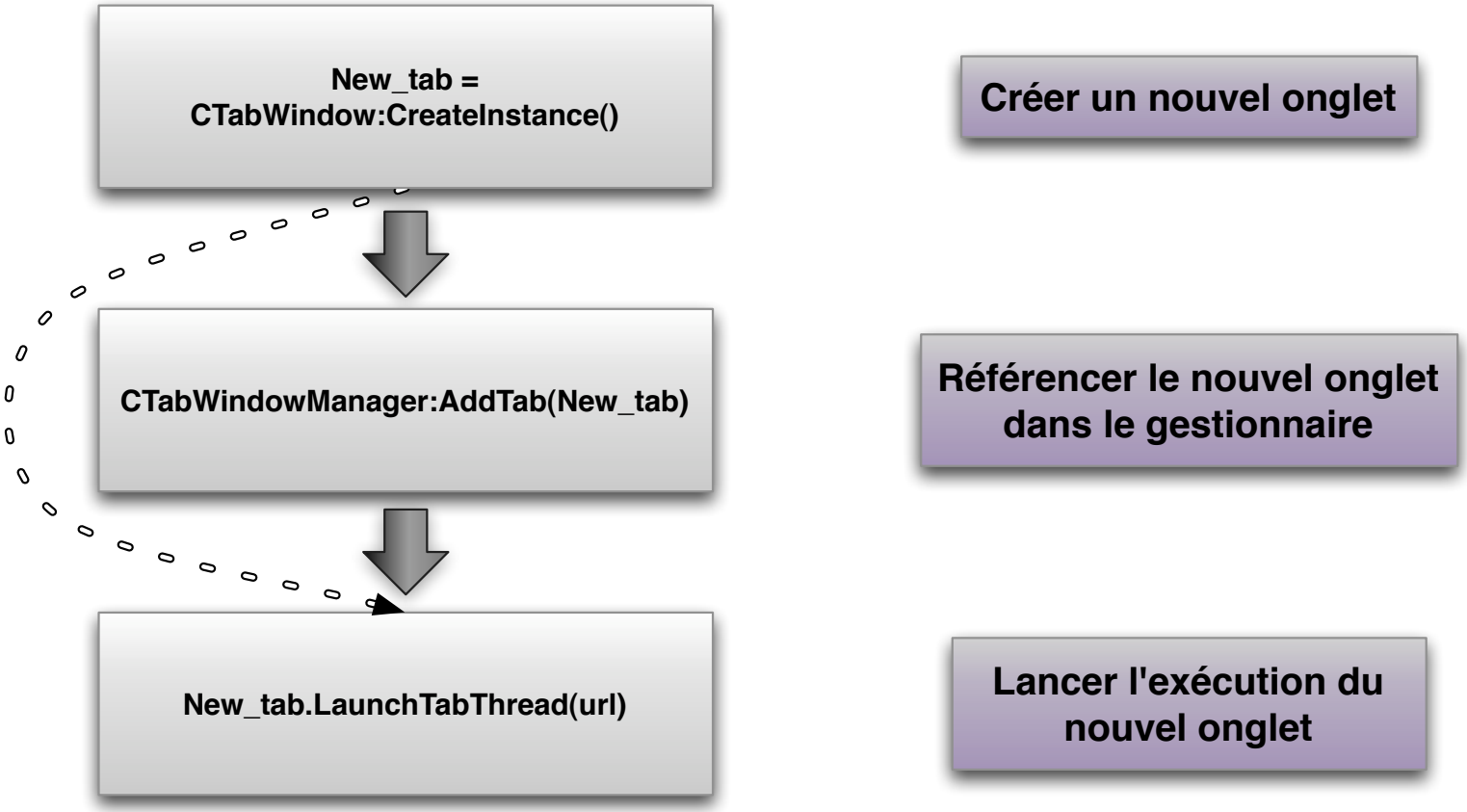
Résultats

Le site aura les plus hauts privilèges possibles

Problème

La création d'un nouvel onglet n'est pas furtive !

Charger et executer des pages : l'onglet invisible



Module de création d'onglets

Possibilités

- Lire/Ecrire des fichiers
- Lire/Ecrire dans le registre
- Créer des processus

Avantages

- Aucune modification du registre
- Invisible pour l'utilisateur

Inconvénients

- Cloisonnement des onglets

Module d'interception : données sensibles

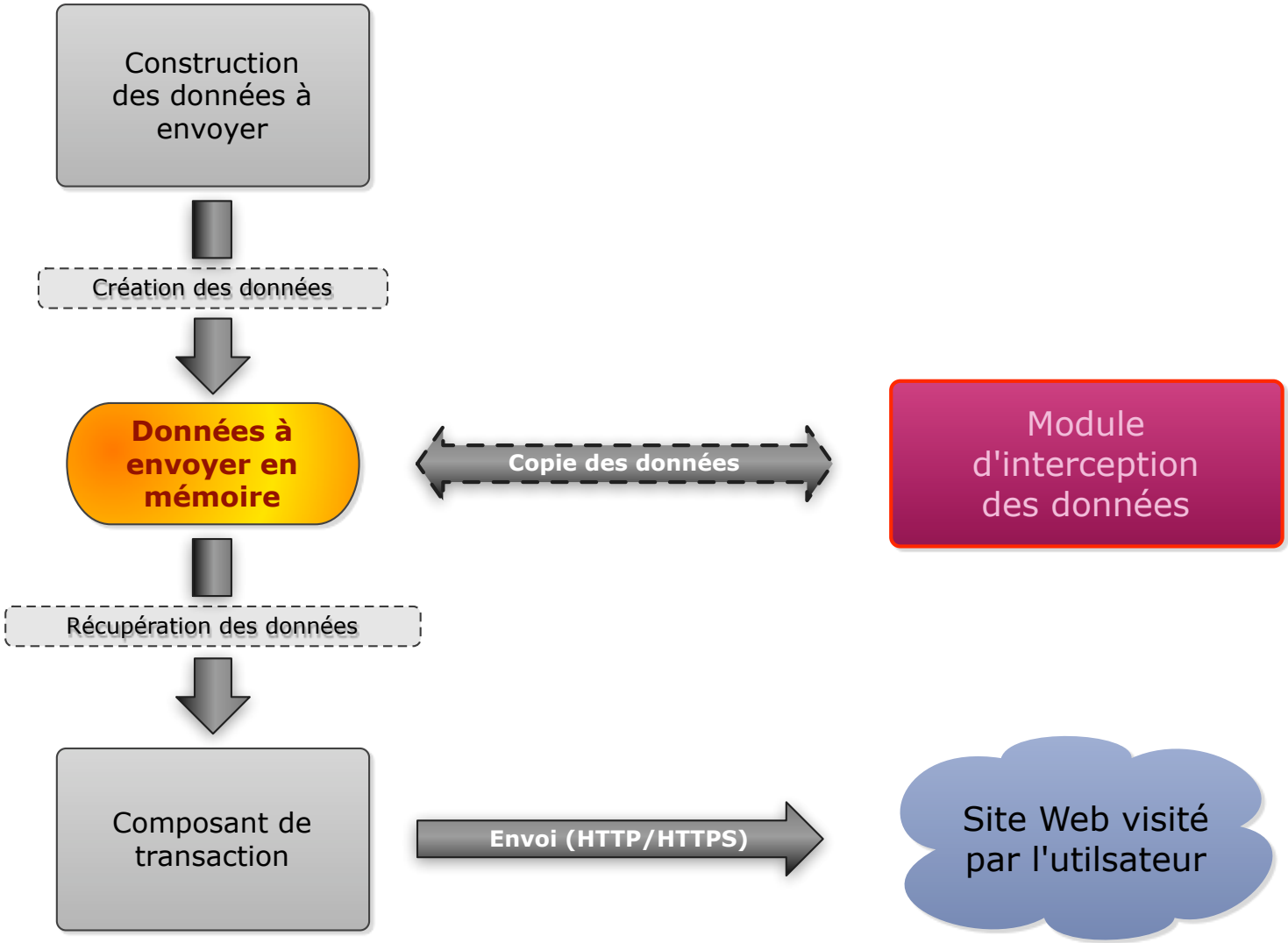
Quelles données ?

- Contenu des pages
- Mots de passe
- Données envoyées

Problème

Ne sont pas accessibles depuis un onglet

Module d'interception : les données à leur source



Module de communication : XmlHttpRequest

Objet XmlHttpRequest

- Permet de garder une connexion avec un serveur web distant
- Mode connecté à l'image d'un socket
- Fonctionne sur HTTP/HTTPS

Actions

- Recevoir les ordres en attente depuis le serveur de l'attaquant
- Rapatrier et executer la charge utile
- Renvoyer les résultats sur le serveur de l'attaquant

Avantages

- Fonctionnalités déjà integrées au navigateur
- Passe à travers les proxys

Charges utiles

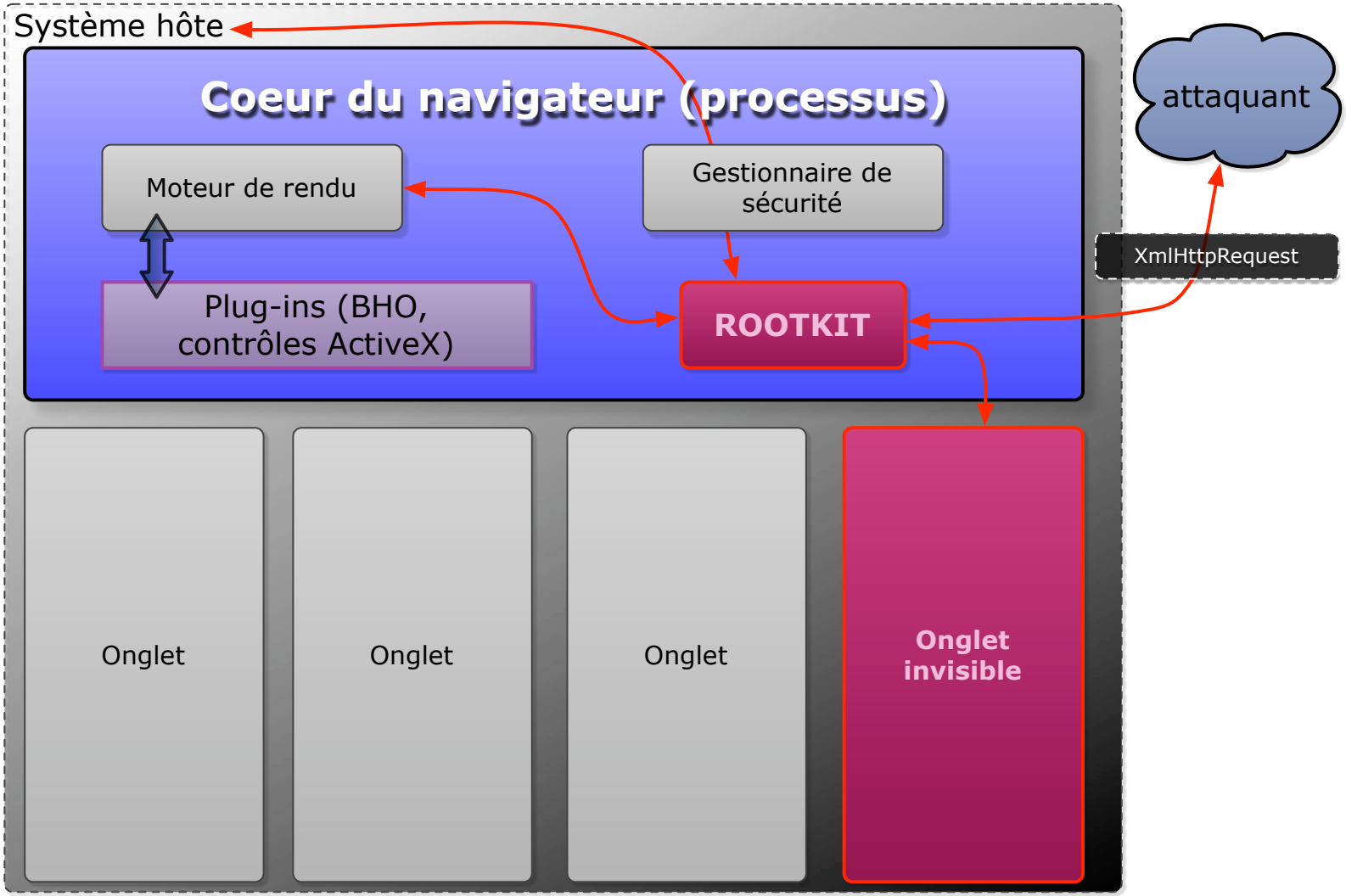
Possibilités

- Pages HTML malicieuses
- Code natif
- Programmes (format PE)
- Integrées comme module ou non

Fonctionnalités

- Exfiltrations d'informations de connexion
- Exfiltration de configuration du système hôte
- Execution de code sur le système hôte

Module de création d'onglets : l'onglet invisible



Démonstration

Plan

Conclusion à propos du rootkit pour Internet Explorer 7

Les rootkits pour navigateurs Web sont analogues aux rootkits kernel

- Création de nouveaux objets du navigateur (onglets, zones)
- Utilisation des fonctions internes du navigateur

Furtivité

- Approche entièrement en mémoire : allocation de mémoire ou modification de données existantes

À faire

- Regarder le mécanisme d'extensions d'Internet Explorer 8

Avez-vous des questions ?

Merci de votre attention