e i g

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale

Techniques utilisées par les rootkits

Etudiant: **Florent WENGER**
florent_wenger@hotmail.com

Professeur: Gérald Litzistorf
En collaboration avec la société ellisys

Laboratoire de transmission de données, décembre 2006

Introduction

- Rootkits: sujet brûlant
  - Croissance exponentielle (McAfee)
- Approche éthique
  - La technique est toujours neutre
  - L'intention varie: protéger ou attaquer ?
  - « Connais ton ennemi » (Sun Tzu)

Déroulement du travail

1. Fonctionnement interne de Windows

   5 semaines

2. Rootkits: techniques en mode *user*

   5 semaines

3. Rootkits: techniques en mode *kernel*

   2 semaines

Rootkits: définition

- Pré-requis: machine déjà compromise
  - Par exploit de faille / *social engineering*
- Ensemble de programmes
  - « permettant à un pirate de maintenir dans le temps un accès frauduleux à un système informatique » (Wikipédia)
- Ne se propage pas !
  - Peut donner accès à d'autres machines

Rootkits: objectifs

1. Assurer la furtivité
   - Dissimuler à l'utilisateur
     - Fichiers et dossiers
     - Processus & connexions TCP/IP
     - Clés de la BDR
2. Héberger d'autres *malwares*
   - *Trojan / keylogger / backdoor / etc.*
   - La vraie menace se situe là !

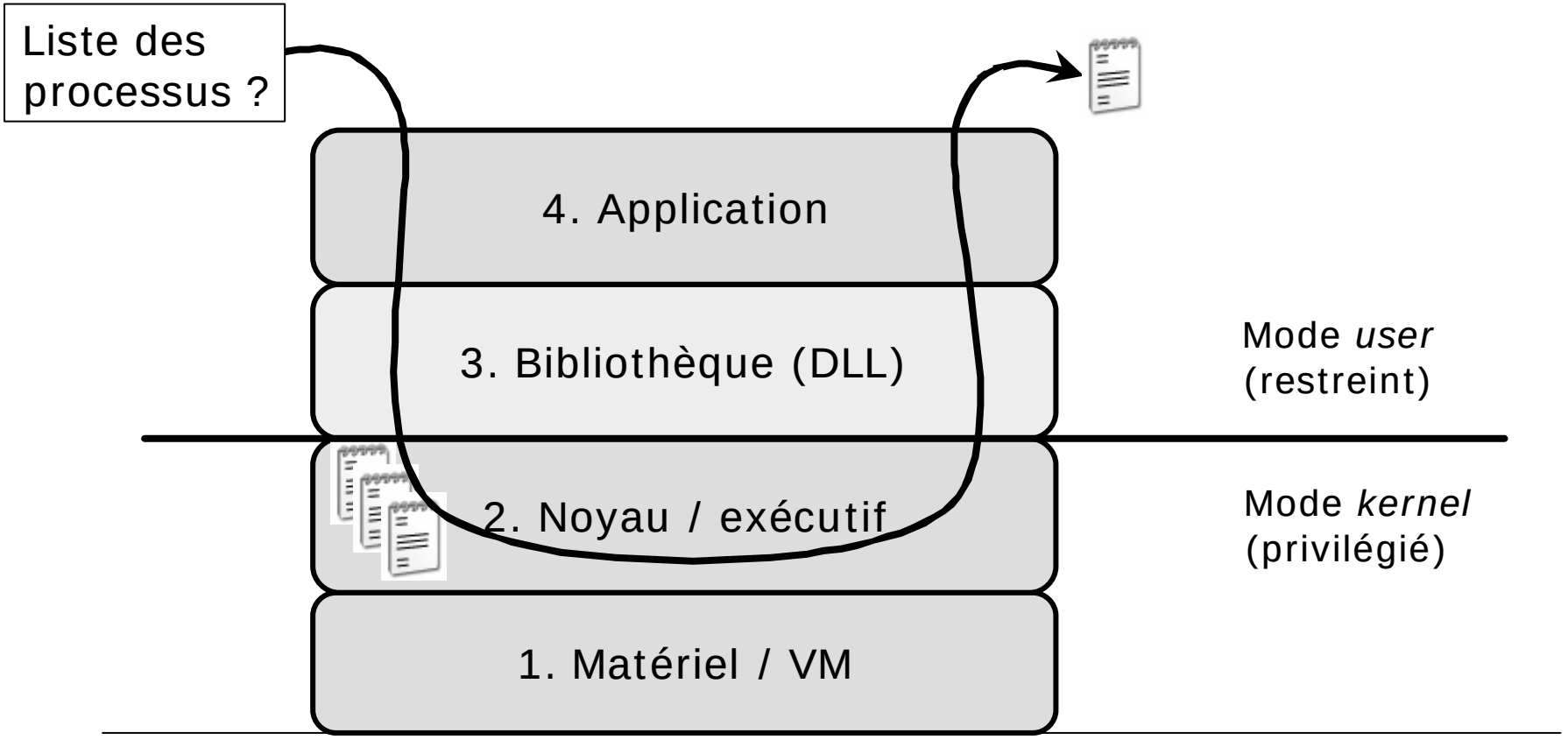
Scénario

Hypothèses :

- PC avec WinXP SP2
- Compte utilisateur standard

1. Corrompre les utilitaires
   - GUI: Explorer, TaskManager, ProcExp
   - CLI: cmd (dir), netstat, fport
2. Obtenir les droits d'administrateur
   - Interception de mots de passe (run-as)

Appel système



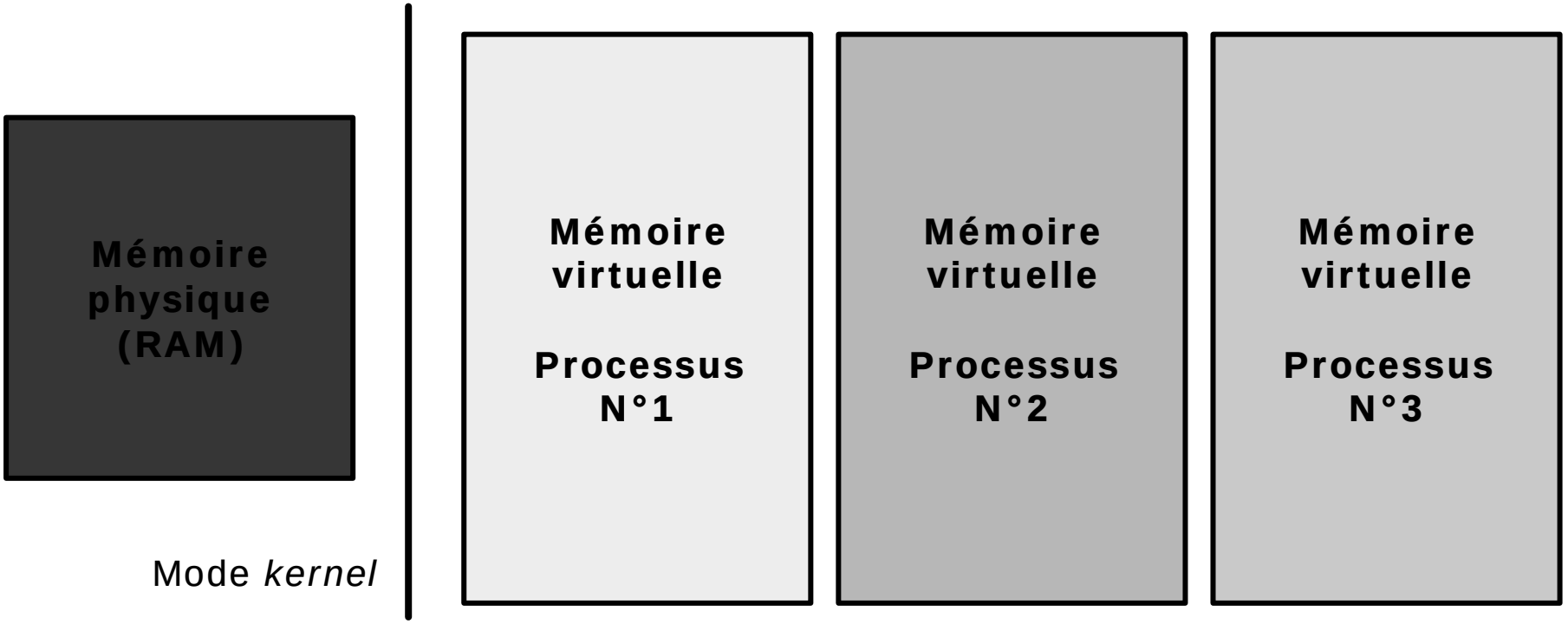
Stratégie du rootkit

- Guide d'opération
  - Plan A: Filtrer les informations
  - Plan B: Censurer l'affichage

- Attaque possible à plusieurs niveaux
  - Niveaux 1 & 2: accès interdit !
- Niveau choisi: API de Windows (DLLs)
  - Interface entre applications et OS

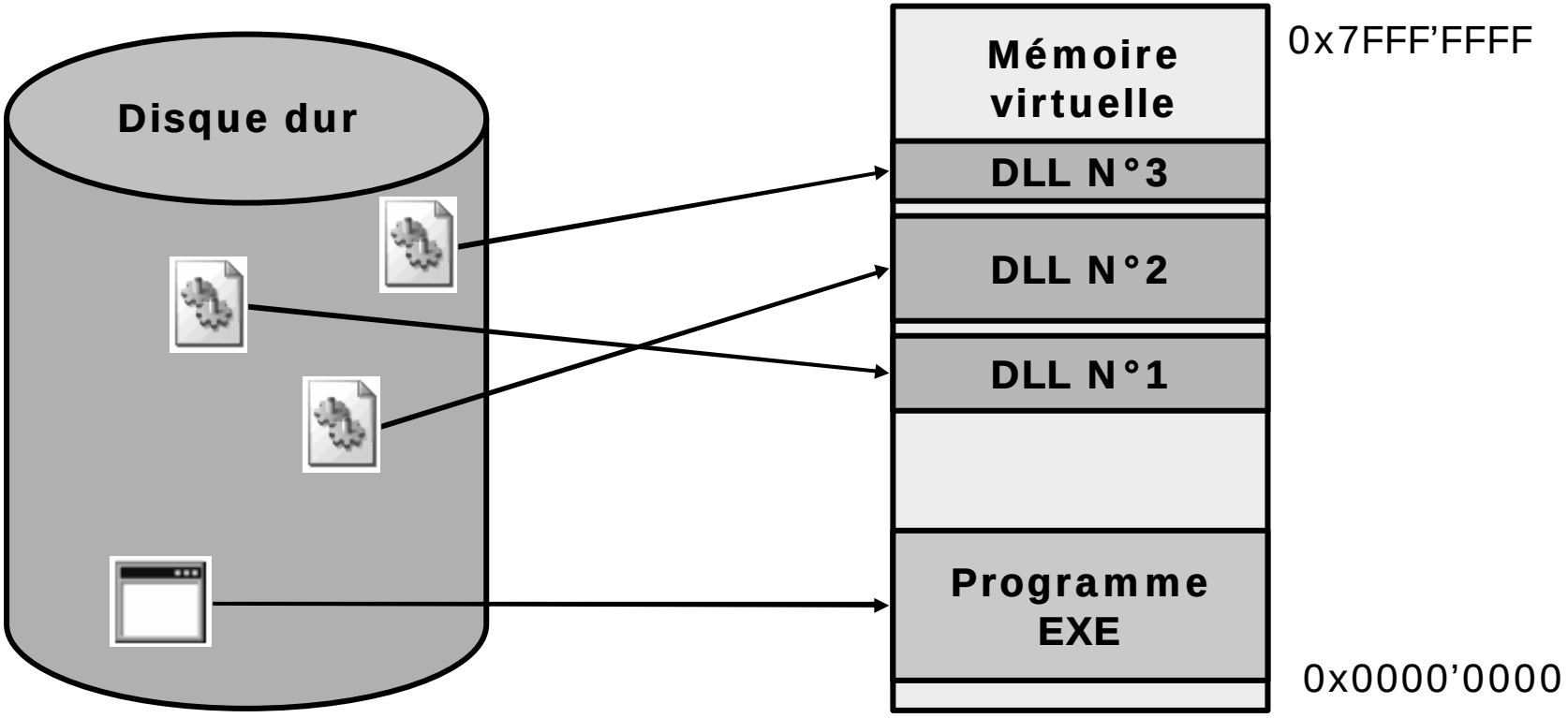
Isolement des processus

- Pas d'accès direct à la RAM
- Se voient seuls en mémoire !



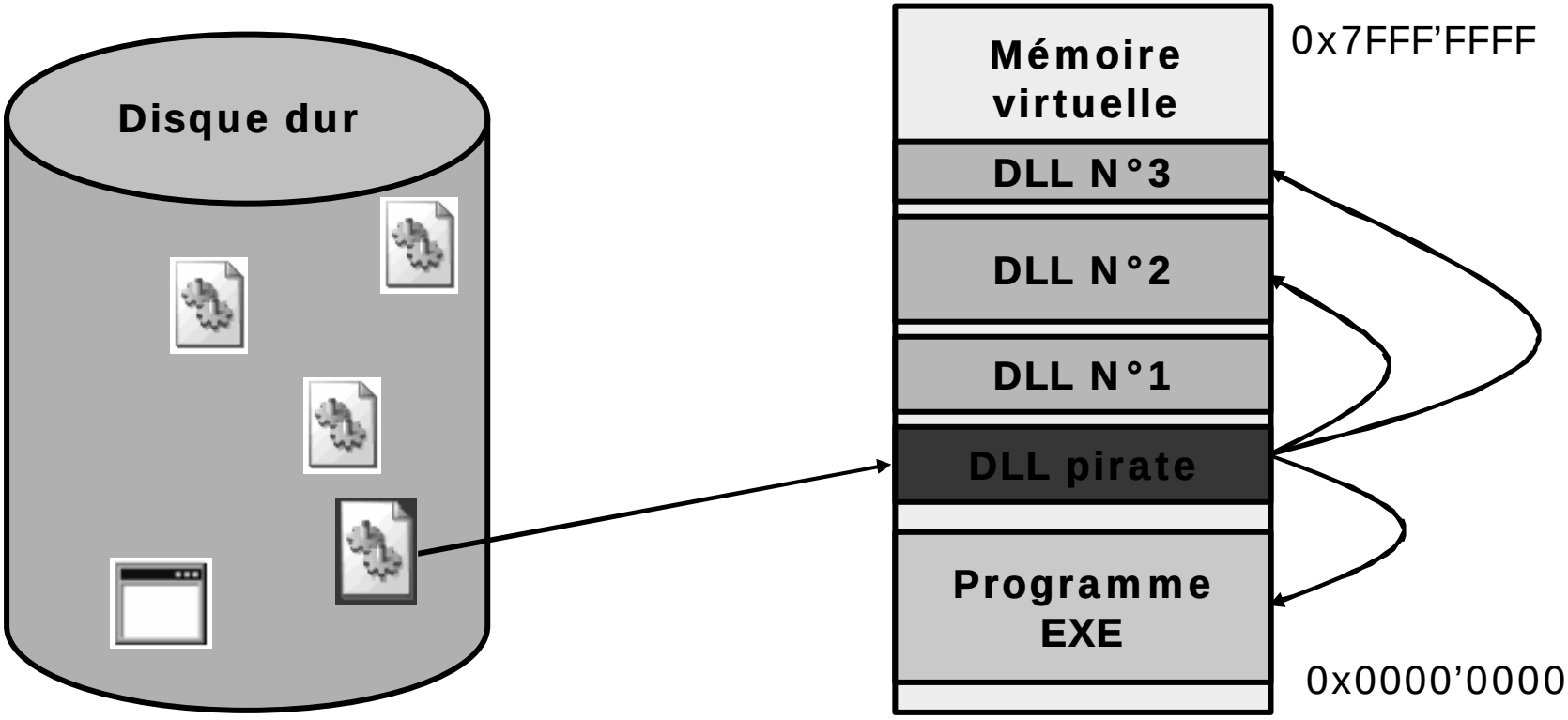
Occupation mémoire

- Chargement des modules (EXE ou DLL)



Injection du rootkit

- Insertion de son code et ses données



1ère démonstration

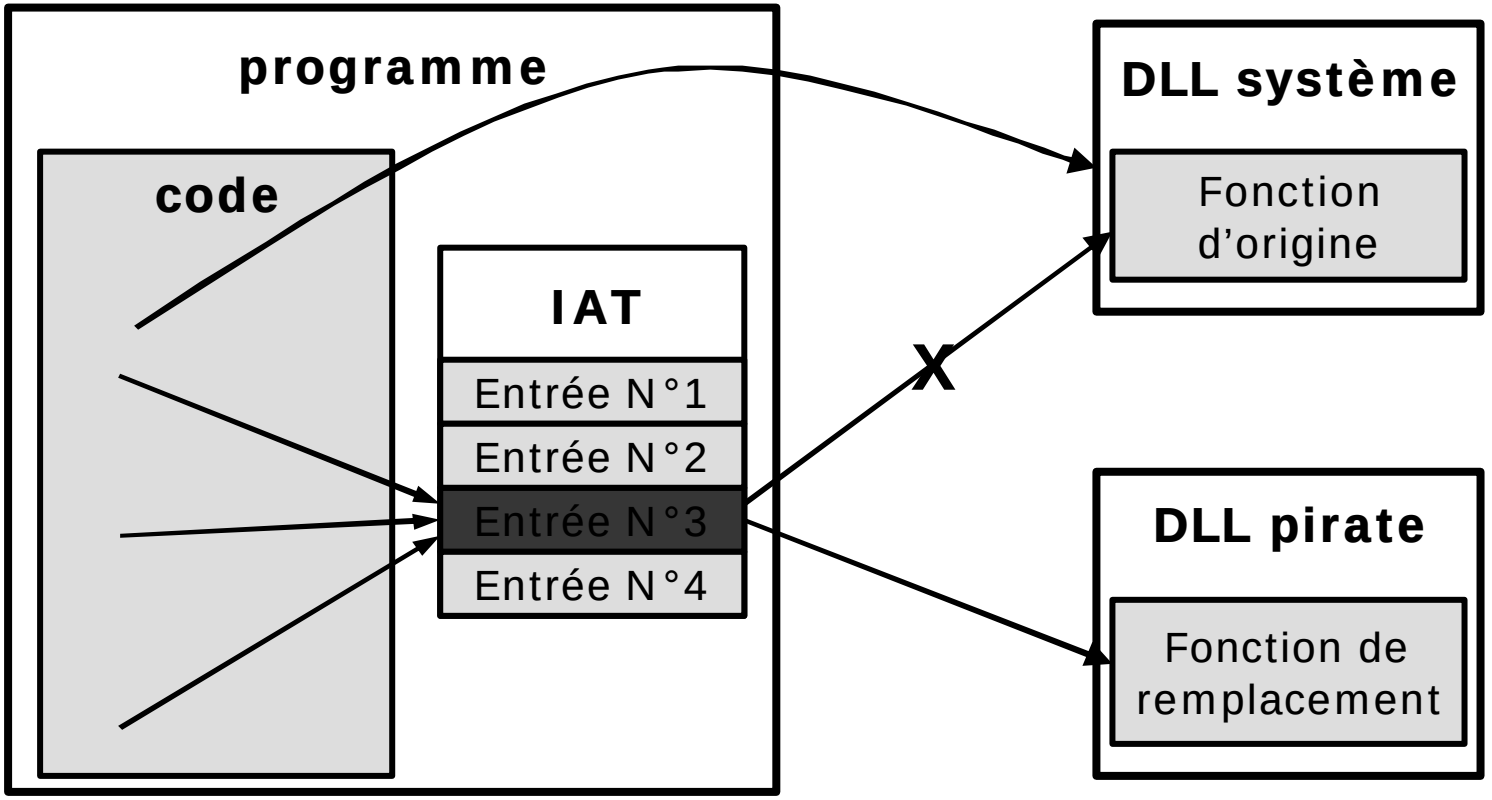
Wordpad: boîte de dialogue

- Fonction ShellAboutW() dans shell32.dll

1. Largage du rootkit dans wordpad.exe
   - Injection de DLL dans son espace d'adressage
2. Détournement de l'appel système
   - Ecrasement de pointeur de fonction dans l'IAT

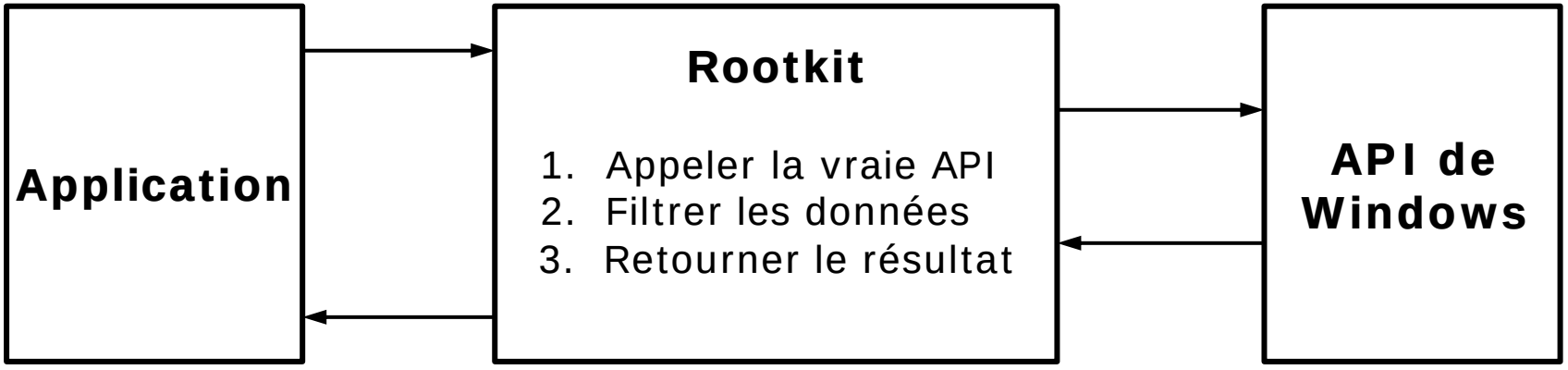
Détournement d'appel

- Altération de l'*Import Address Table*



Fonction de remplacement

- Tout est possible !
  - *Disponibilité*: déni de service
  - *Confidentialité*: espionnage des activités
  - *Intégrité*: corruption des données



2ème démonstration

Désactivation d'invite de commandes

- Stratégie locale définie dans la BDR
- \HKCU\Soft\Pol\MS\Win\Sys\DisableCMD = 1

1. Parachutage du rootkit dans cmd.exe
2. Altération des instructions
   - *Inline patching* de advapi32!RegQueryValueExW
3. Contournement de la restriction
   - Simulation de l'inexistence de clé

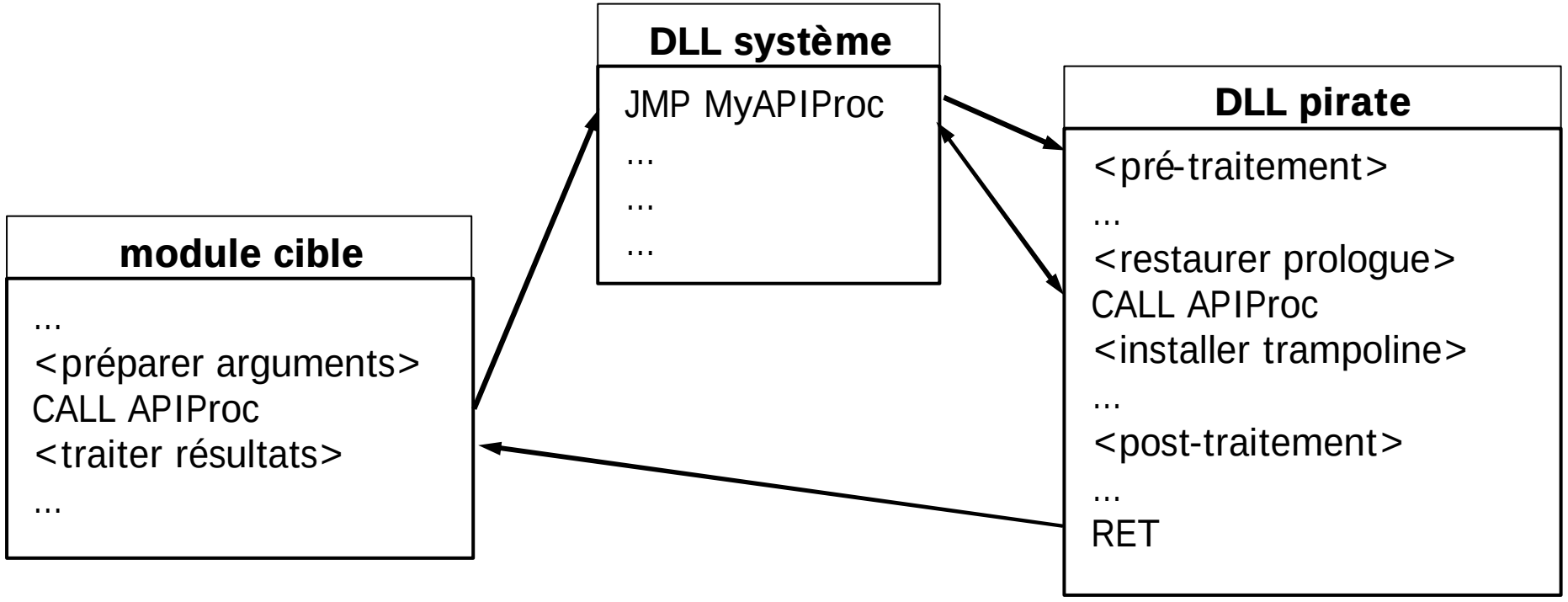
Furtivité du rootkit

- Aucune modification sur le disque...
  - EXE et DLLs intacts
- ... ni dans la base de registres
  - Clé toujours présente

- Tout se passe **en mémoire !**

Altération des instructions

- *Inline patching* du code machine



3ème démonstration

- Un vrai rootkit partiel ! (Hoglund)

1. Corruption du système d'exploitation
   - Chargement d'un pilote en mode *kernel*
2. Déroutement des services de l'OS
   - Ecriture de pointeurs de fonction dans la SSDT
3. Censure totale à la source
   - Suppression d'informations de processus
   - Simulation de l'absence de fichiers & dossiers

Prise de contrôle

- Modification de la SSDT
  - *System Service Descriptor Table*
  - Similaire à l'IAT mais en mode *kernel*

- Modèle à liste blanche
  - Contrôle de tous les processus...
  - ... sauf ceux qui sont hébergés

Et sous Windows Vista ?

- Toutes ces techniques fonctionnent !
  - Tests avec Windows Vista RTM Ultimate

- Mais...
  - Un rootkit tout seul est inoffensif
  - Possibilités pour les *malwares* hébergés ?
  - Hors du champ d'étude !

UAC sécurise le mot de passe

Conclusion

- Les rootkits existent pour longtemps !
  - Et si votre PC était sous contrôle ?
- Se méfier des exécutables...
- PRÉVENIR : HIPS, anti-virus, pare-feu
- DÉTECTER : SVV, RAIDE, etc.

Questions

- Merci pour votre attention !

- Avez-vous des questions ?