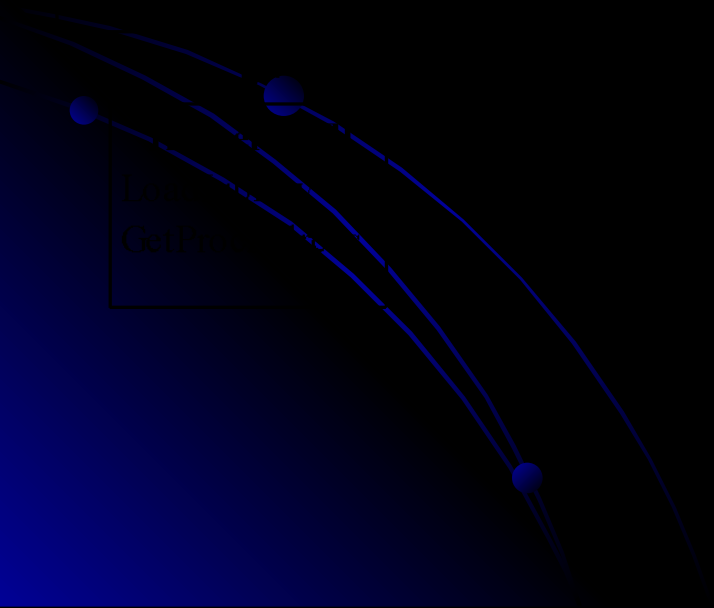
Системне програмування

Лекція № 8

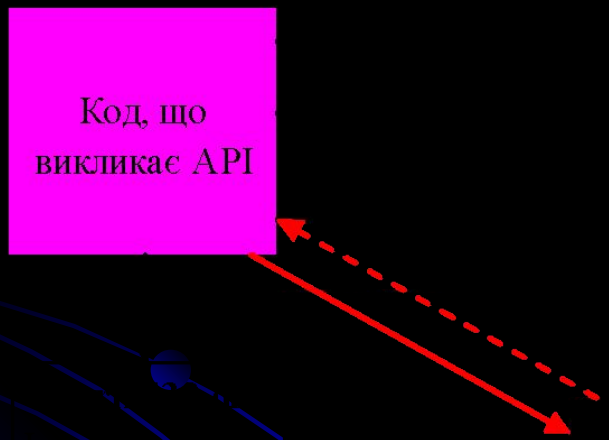
Лектор Артамонов Є.Б.

RootKit-віруси і методи їх виявлення

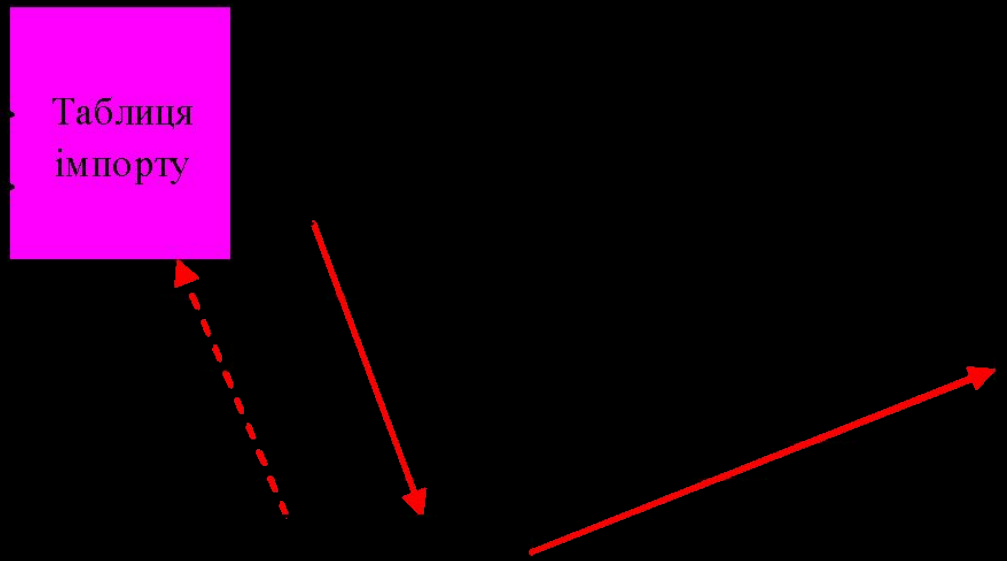
Принцип виклику API функції



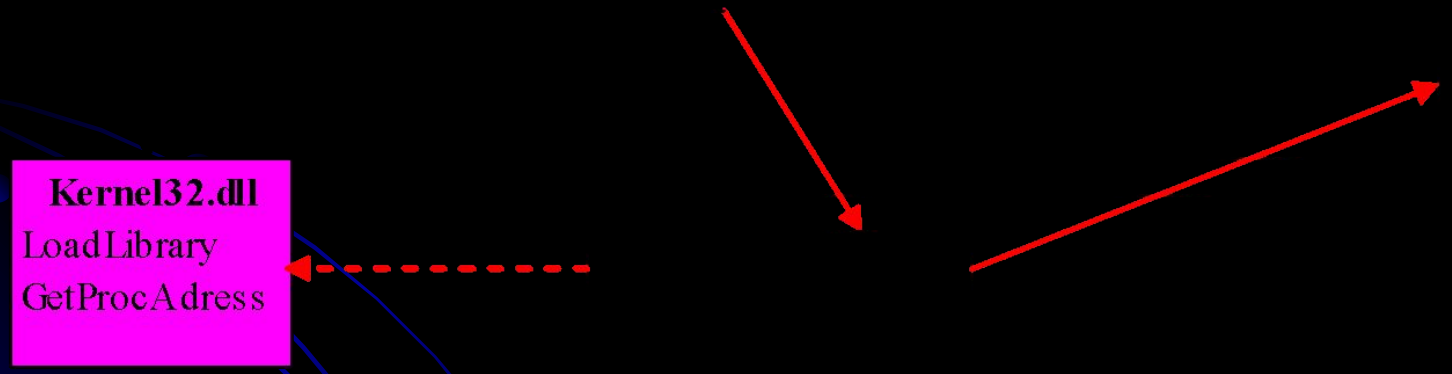
Модифікація машинного коду прикладної програми для перехоплення виклику функції



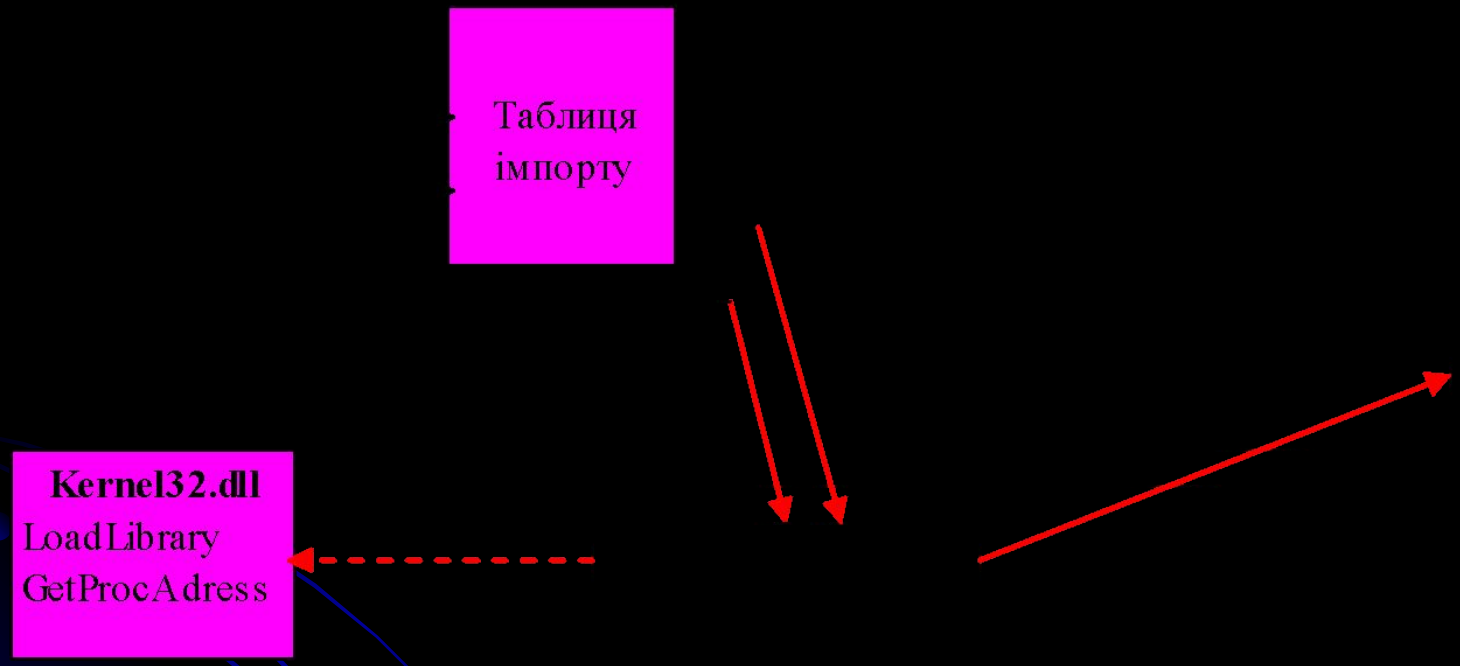
Модифікація таблиці імпорту



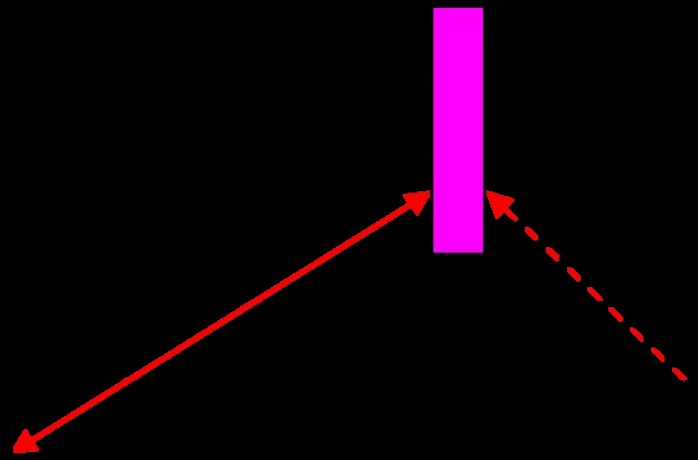
Перехоплення функцій LoadLibrary і GetProcAddress



Модифіковані методи перехоплення API функцій



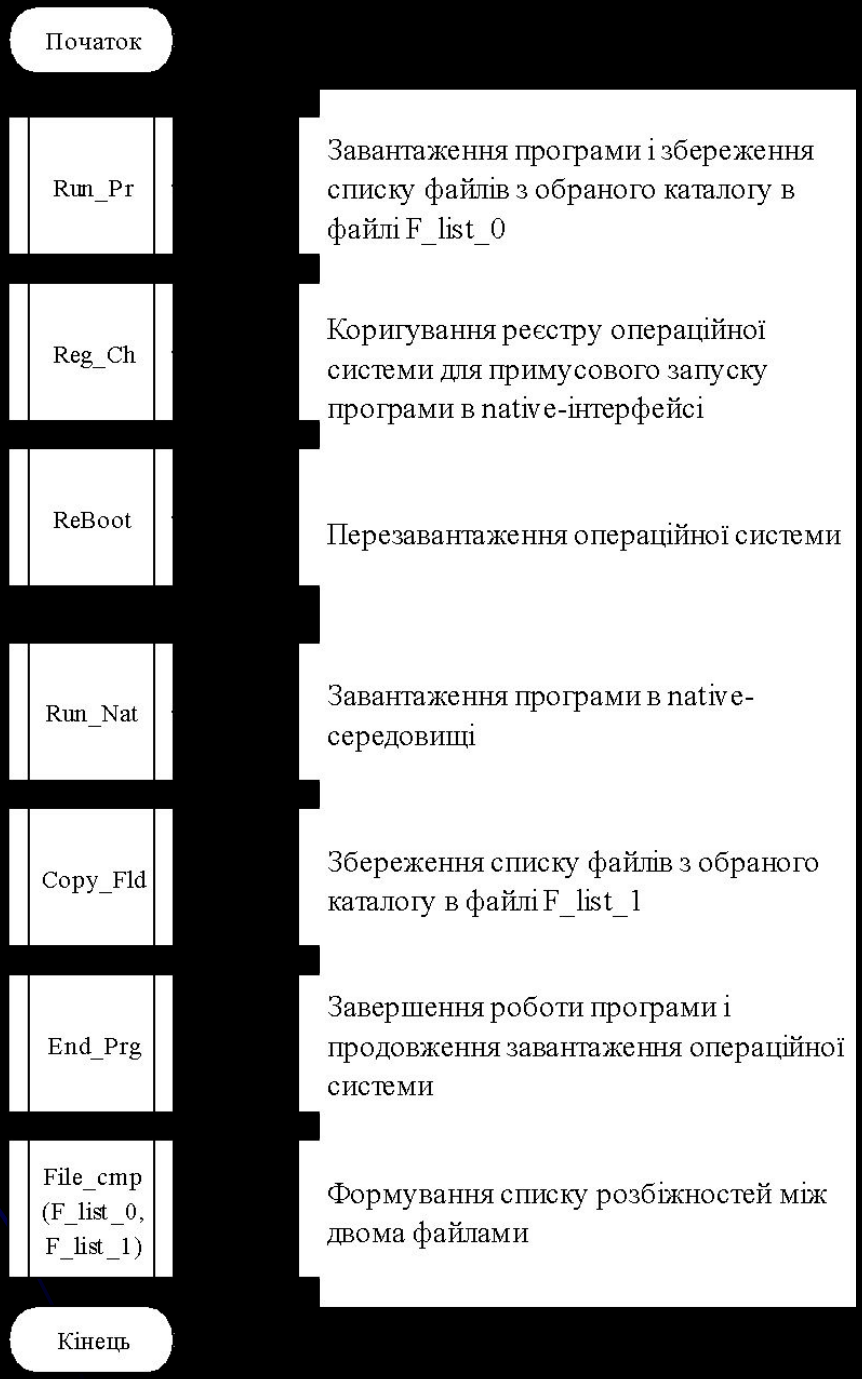
Модифікація програмного коду API функції



Основні задачі, які необхідно розв’язати при реалізації модуля виявлення вірусів-rootkit:

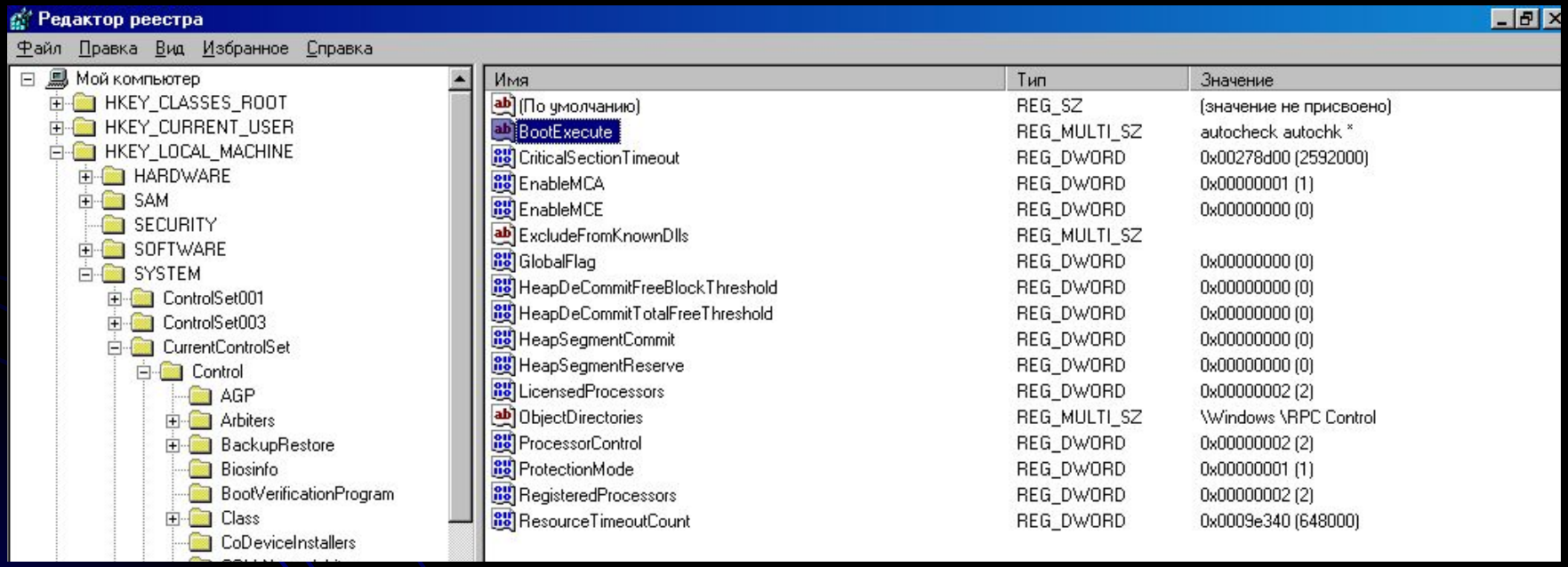
- реалізувати метод примусового завантаження програми в native-інтерфейсі;
- реалізувати процедури відкриття каталогу і файлів в native-інтерфейсі (набір процедур обмежено бібліотекою ntdll.dll);
- реалізувати приховування отриманого списку файлів від можливого втручання root-kit вірусом;

Схема роботи програмного модуля виявлення вірусів rootkit



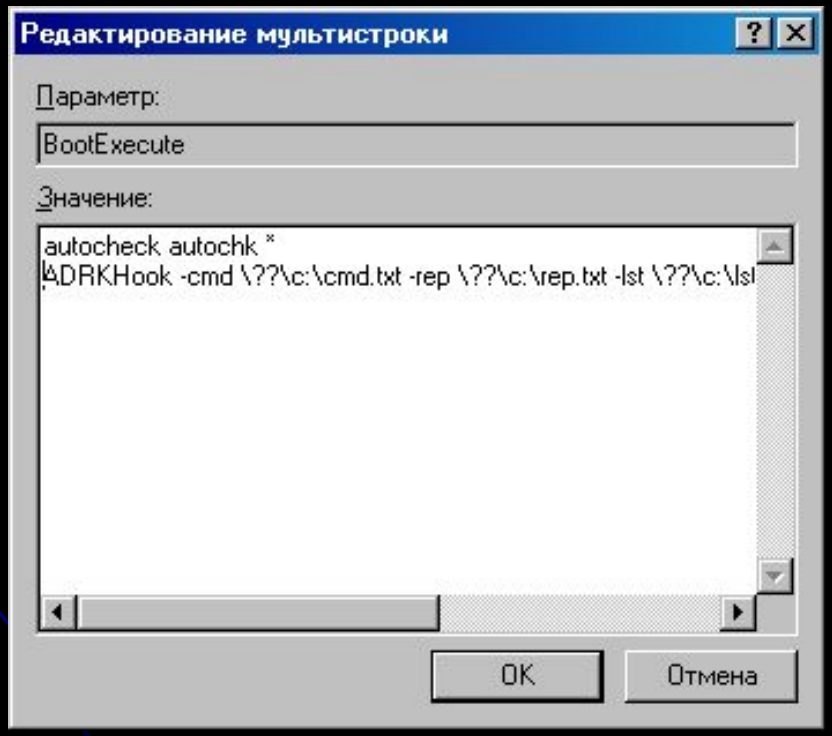
Завантаження програми

- Зміна параметрів реєстру



Завантаження програми

- Рядок завантаження програми через реєстр



Основні вікна роботи програми

- Кодування командного файлу

```
C:\temp\!\Release>ADRKHook_crypt.exe cmd
Usage: crypt_gen <src_file> <out_file> [new]

C:\temp\!\Release>ADRKHook_crypt.exe cmd cmd0
m=
3cc46413 71daaf60 d5711bc4 e658c476
s=
9b340e46 464ae6ad e68989e9 02ac64a6 70bea5f8 68dfbe0c bf8b3703 eeb33491
53292fdd 6c495a3a 4aa65568 b760cb6f 824d2561 6b3150b2 6e0fef26 13d71e79
m'=
3cc46413 71daaf60 d5711bc4 e658c476
Verification OK
```

⇓

- Виконання перевірки файлів

```
C:\temp\!\Release>ADRKHook.exe -lst \??\c:\lst -cmd \??\c:\cmd -log \??\c:\log -rep \??\c:\rep
Creating detailed list...
 Done
Processed... 35
```

⇓

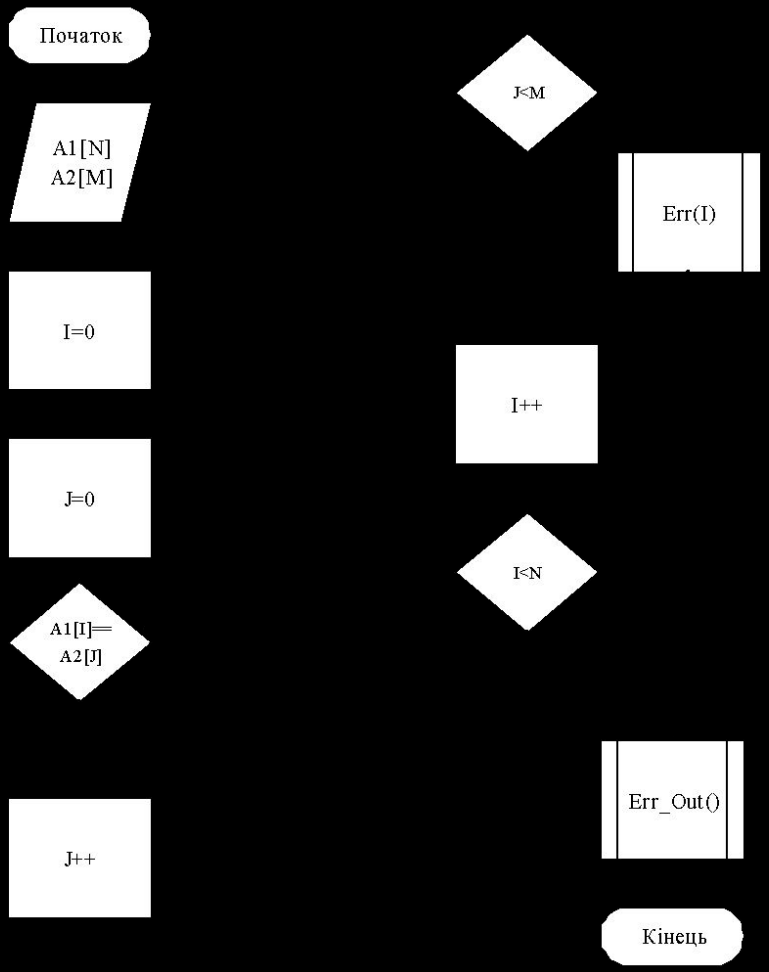
- Результат порівняння звітів про зміст каталогів

```
C:\temp\!\Release>ADRKHook_test.exe -cmp c:\lst -cmd c:\cmd2 \??\c:\
List file: c:\lst
Command file: c:\cmd2
\??\C:\WINDOWS\system32\DRIVERS 1
Deleted file: \??\C:\WINDOWS\system32\DRIVERS\afd.sys
Everythings clear!

C:\temp\!\Release>
```

Результат перевірки системних каталогів

Схема алгоритму порівняння змісту каталогів



Дякую за увагу!!!
Зустрінемось на лекції через тиждень

Знайти лектора можна в аудиторії 5-214
або
за e-mail-ом: eart@ukr.net
або
вКонтакте: http://vk.com/id6416748