

# Системне програмування

Лекція № 8

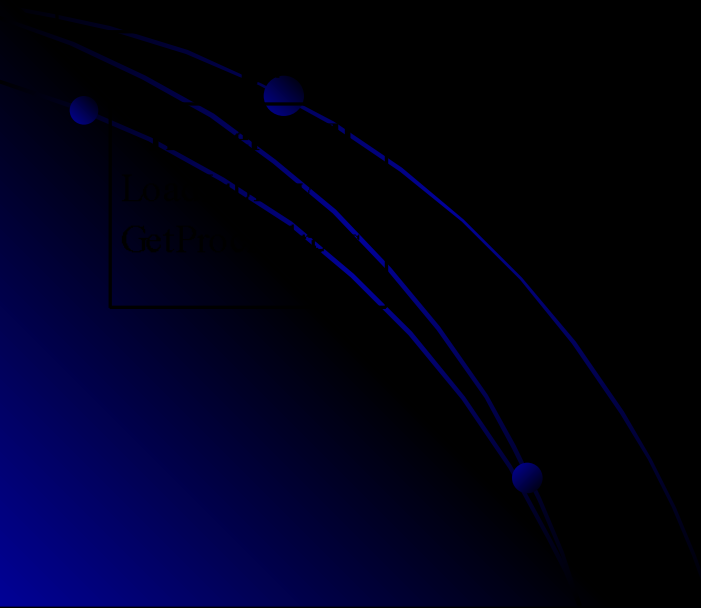
Лектор Артамонов Є.Б.



# RootKit-віруси і методи їх виявлення



# Принцип виклику API функції



# Модифікація машинного коду прикладної програми для перехоплення виклику функції

Код, що  
викликає API

CALL



# Модифікація таблиці імпорту

Таблиця імпорту



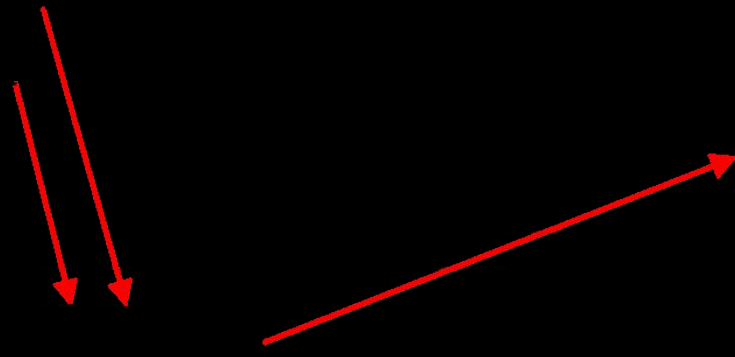
# Перехоплення функцій LoadLibrary і GetProcAddress



# Модифіковані методи перехоплення API функцій

Таблиця  
імпорту

**Kernel32.dll**  
LoadLibrary  
GetProcAddress



# 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

Початок

Run\_Pr

Завантаження програми і збереження списку файлів з обраного каталогу в файлі F\_list\_0

Reg\_Ch

Коригування реєстру операційної системи для примусового запуску програми в native-інтерфейсі

ReBoot

Перезавантаження операційної системи

Run\_Nat

Завантаження програми в native-середовищі

Copy\_Fld

Збереження списку файлів з обраного каталогу в файлі F\_list\_1

End\_Prg

Завершення роботи програми і продовження завантаження операційної системи

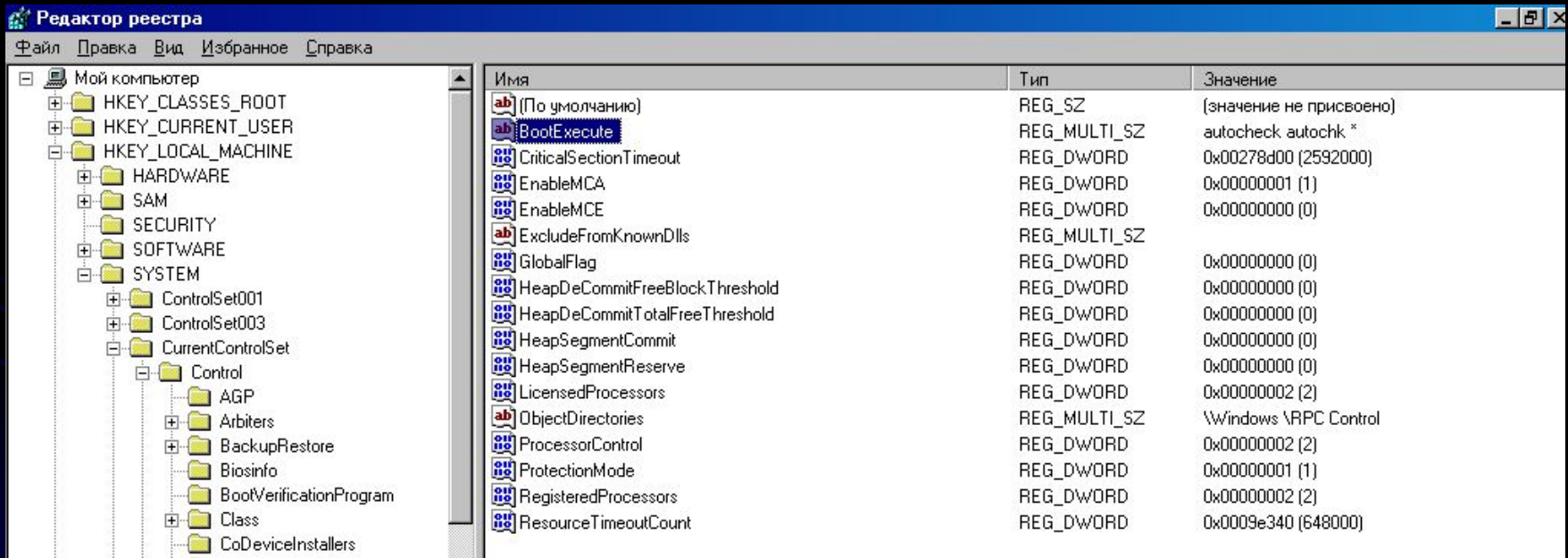
File\_cmp  
(F\_list\_0,  
F\_list\_1)

Формування списку розбіжностей між двома файлами

Кінець

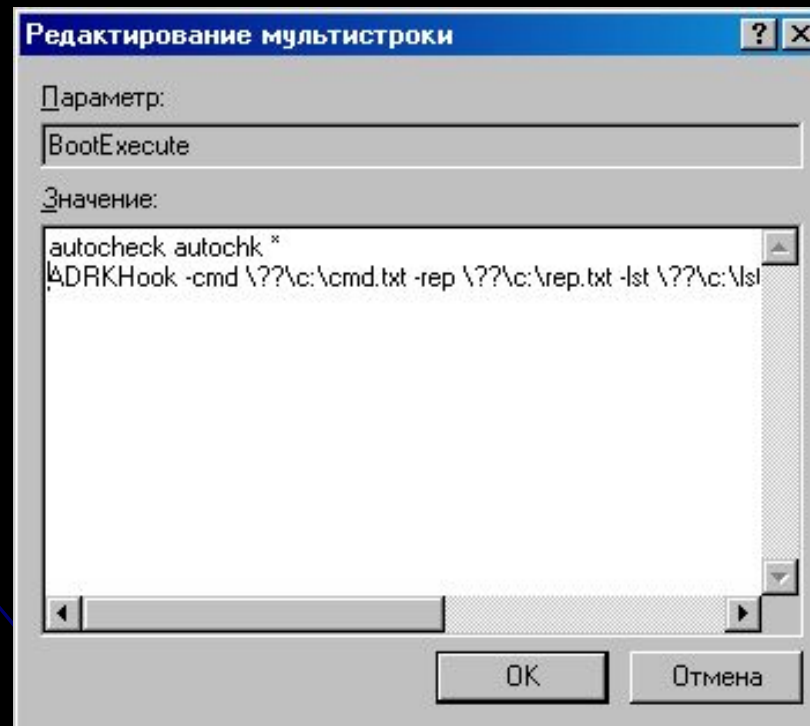
# Завантаження програми

- 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 464aebad 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!

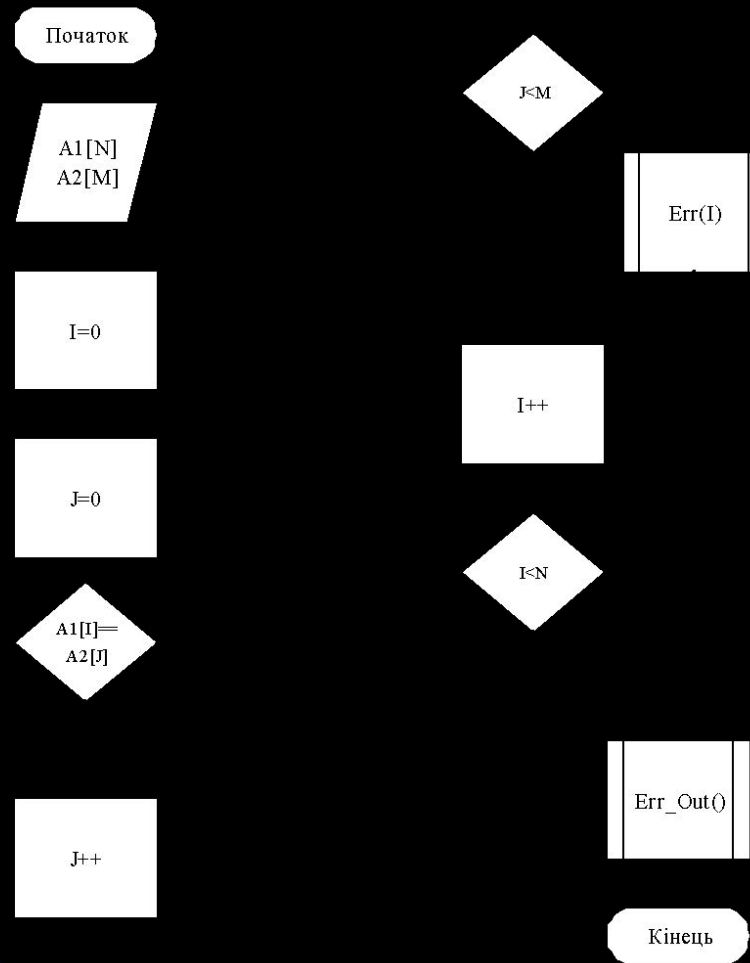
C:\temp\!\Release>
```



# Результат перевірки системних каталогів

```
C:\>ls -l Unicode 171068 Кор 0
\\?\C:\WINDOWS\System32\drivers\atintuxx.sys edd66332608d27f4fd5069bcd0bc5164
\\?\C:\WINDOWS\System32\drivers\atinxbxx.sys 3e7d485cbd0b0d9f6ea2ad9442411831
\\?\C:\WINDOWS\System32\drivers\atinxsxx.sys 77b575d7aab35d5908ae6ce681608d62
\\?\C:\WINDOWS\System32\drivers\ativmc20.cod 8e59f9be251c8ae32a1ceb068b3f96b1
\\?\C:\WINDOWS\System32\drivers\atmarpc.sys 9916c1225104ba14794209cfa8012159
\\?\C:\WINDOWS\System32\drivers\atmepvc.sys 39a0a59180f19946374275745b21aeba
\\?\C:\WINDOWS\System32\drivers\atmlane.sys ae76348a2605fb197fa8ff1d6f547836
\\?\C:\WINDOWS\System32\drivers\atmuni.sys e7ef69b38d17ba01f914ae8f66216a38
\\?\C:\WINDOWS\System32\drivers\atv01nt5.dll a1e2a7e2a35df4f1ee74559c7ea8e3fc
\\?\C:\WINDOWS\System32\drivers\atv02nt5.dll dabb94d9e0cb66f0533e96b8bb90e517
\\?\C:\WINDOWS\System32\drivers\atv04nt5.dll a0c0c3d3795c505162954eac97c10778
\\?\C:\WINDOWS\System32\drivers\atv06nt5.dll 02b7893a313216c953a131febfd17a42
\\?\C:\WINDOWS\System32\drivers\atv10nt5.dll 057b7c883f9429eef669913885db40b8
\\?\C:\WINDOWS\System32\drivers\audstub.sys d9f724aa26c010a217c97606b160ed68
\\?\C:\WINDOWS\System32\drivers\battc.sys 0d93976f7801b7fcd8135cc77257bbd0
\\?\C:\WINDOWS\System32\drivers\bcbthub.sys b990976940e0e93b4932cccb536f446d
\\?\C:\WINDOWS\System32\drivers\beep.sys da1f27d85e0d1525f6621372e7b685e9
\\?\C:\WINDOWS\System32\drivers\blueletaudio.sys 5ff9a3f3476d726ae62da82d5da94c36
\\?\C:\WINDOWS\System32\drivers\BlueletSCOAudio.sys bd91afc523fd59f881e1763c38fb772f
\\?\C:\WINDOWS\System32\drivers\bridge.sys f934d1b230f84e1d19dd00ac5a7a83ed
\\?\C:\WINDOWS\System32\drivers\btcusb.sys fb2abc6d08d9f8d5ed8e02cbd18b39bb
\\?\C:\WINDOWS\System32\drivers\bthenum.sys b279426e3c0c344893ed78a613a73bde
\\?\C:\WINDOWS\System32\drivers\BTHidMgr.sys dfca4fe4c8aec786b4d0f432eb730f48
\\?\C:\WINDOWS\System32\drivers\bthmodem.sys fca6f069597b62d42495191ace3fc6c1
\\?\C:\WINDOWS\System32\drivers\bthpan.sys 80602b8746d3738f5886ce3d67ef06b6
\\?\C:\WINDOWS\System32\drivers\bthport.sys 3576f003eb9101e68db1890ac263de03
\\?\C:\WINDOWS\System32\drivers\bthprint.sys bb68cebffd181e18a26112d1b9f90f3d
\\?\C:\WINDOWS\System32\drivers\bthusb.sys 61364cd71ef63b0f038b7e9df00f1efa
\\?\C:\WINDOWS\System32\drivers\btnetdrv.sys c5cce2b26f73f8cf7f3c82159e79aa08
\\?\C:\WINDOWS\System32\drivers\BTNetFilter.sys 4f26303becbb7cc5ca8ff39593124cf2
\\?\C:\WINDOWS\System32\drivers\cbidf2k.sys 90a673fc8e12a79afbed2576f6a7aaf9
\\?\C:\WINDOWS\System32\drivers\CCDECODE.sys 0be5aef125be881c4f854c554f2b025c
\\?\C:\WINDOWS\System32\drivers\cdaudio.sys c1b486a7658353d33a10cc15211a873b
\\?\C:\WINDOWS\System32\drivers\cdfs.sys c885b02847f5d2fd45a24e219ed93b32
\\?\C:\WINDOWS\System32\drivers\cdr4_xp.sys bf79e659c506674c0497cc9c61f1a165
\\?\C:\WINDOWS\System32\drivers\cdralw2k.sys 2c41cd49d82d5fd85c72d57b6ca25471
\\?\C:\WINDOWS\System32\drivers\cdrom.sys 1f4260cc5b42272d71f79e570a27a4fe
\\?\C:\WINDOWS\System32\drivers\ch7xhnt5.dll bdf776fddc617fd66d68abb606d976cb
```

# Схема алгоритму порівняння змісту каталогів



Дякую за увагу!!!  
Зустрінемося на лекції через  
ТИЖДЕНЬ

Знайти лектора можна в аудиторії 5-214

або

за e-mail-ом: [eart@ukr.net](mailto:eart@ukr.net)

або

вКонтакте: <http://vk.com/id6416748>