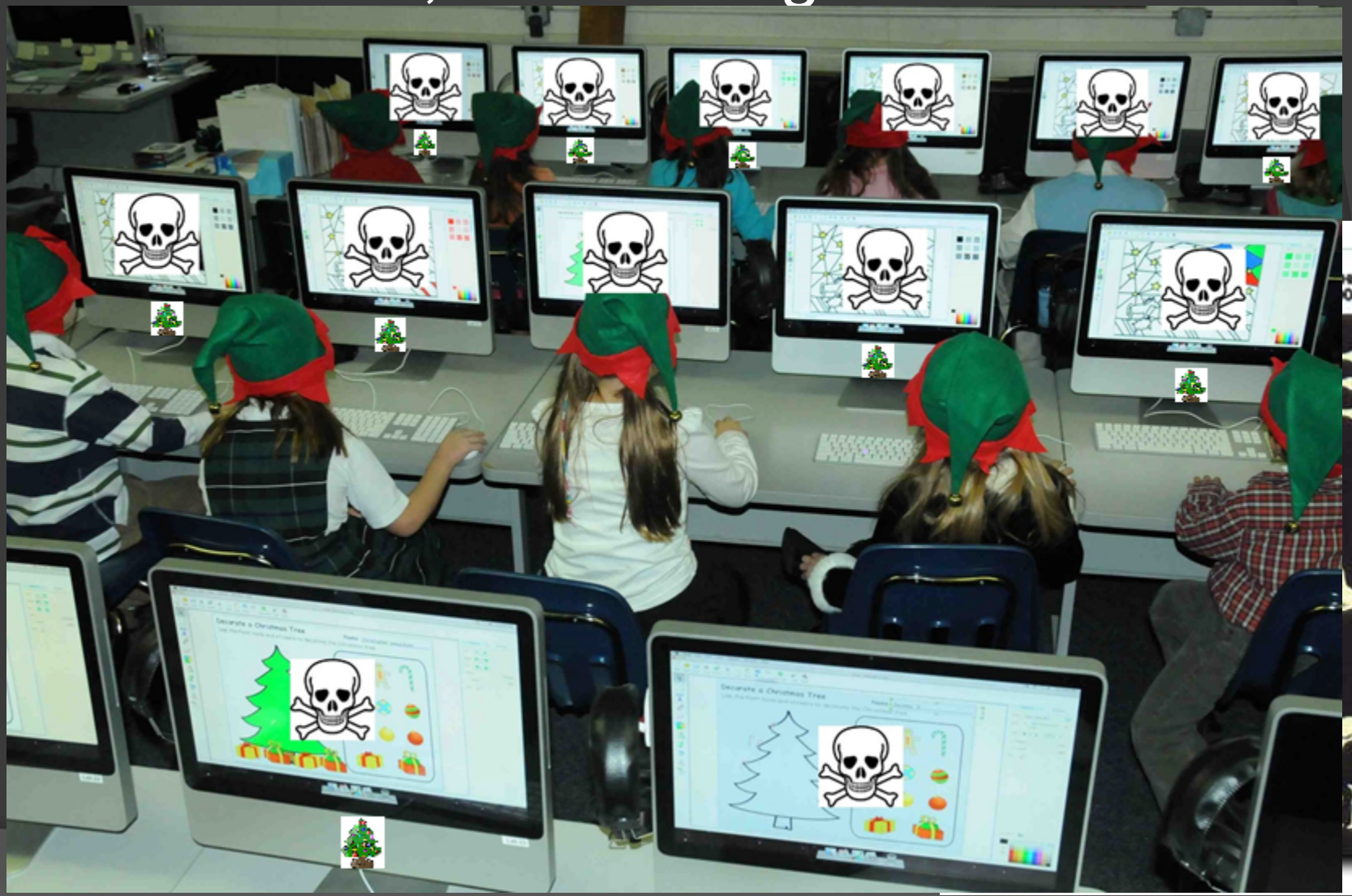
THE NECURS ROOTKIT

Nico Yturriaga

September 27, 2014

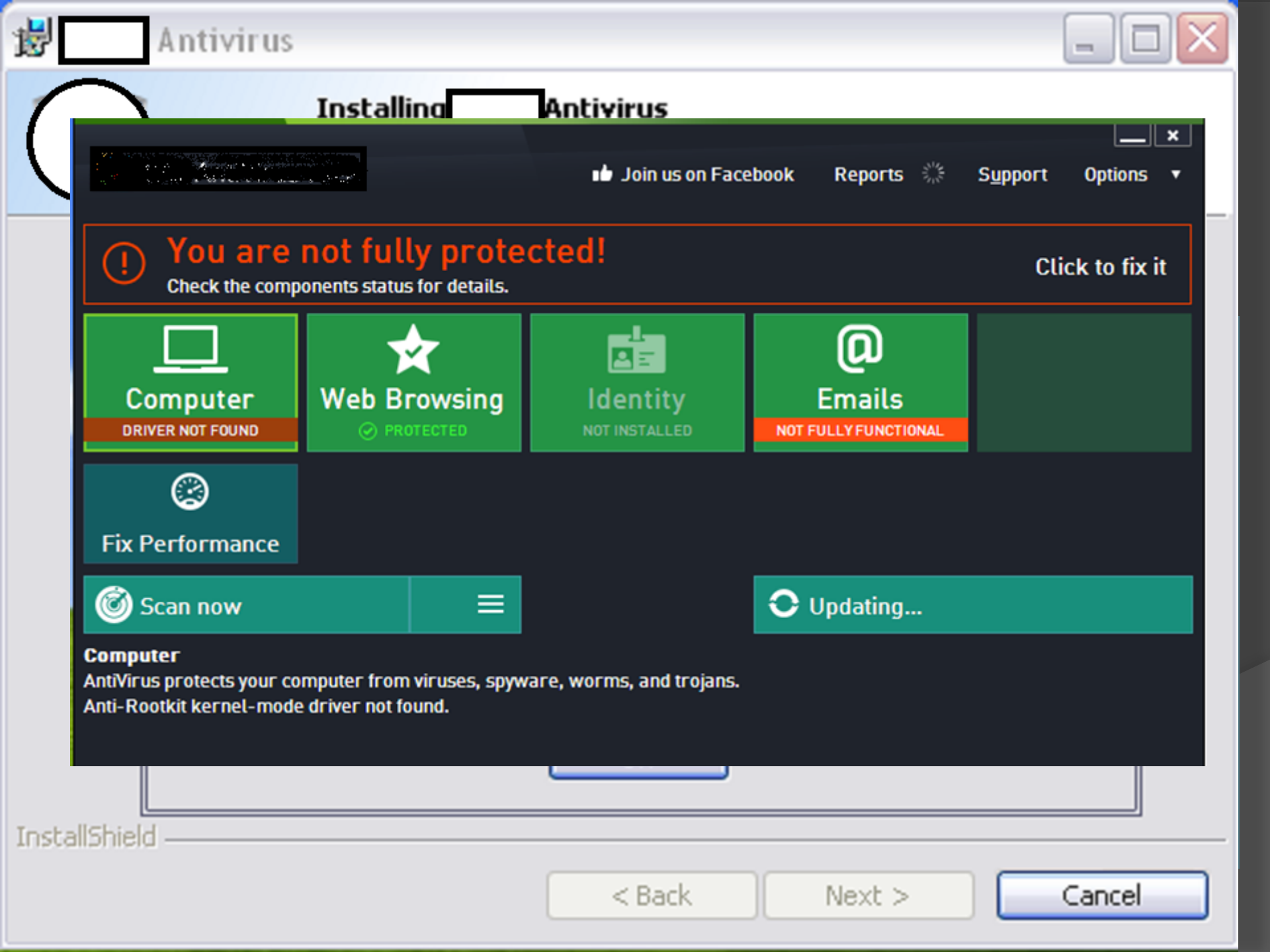
Why Necurs?

- Infected 80,000+ during December 2012

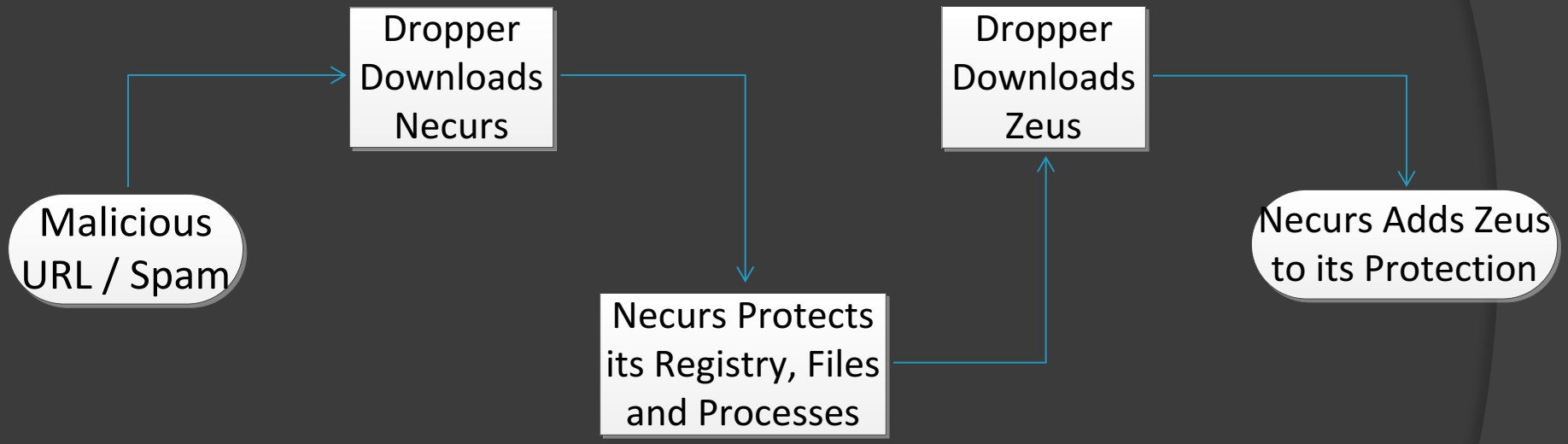


What is a Rootkit?

- Stealthy type of software
- Activated at boot up
- Removal can be complicat
  practically impossible


Antivirus
Installing Antivirus
Join us on Facebook
Reports
Support
Options
You are not fully protected!
Check the components status for details.
Click to fix it
Computer
DRIVER NOT FOUND
Web Browsing
PROTECTED
Identity
NOT INSTALLED
Emails
NOT FULLY FUNCTIONAL
Fix Performance
Scan now
Updating...
Computer
AntiVirus protects your computer from viruses, spyware, worms, and trojans.
Anti-Rootkit kernel-mode driver not found.
InstallShield
< Back
Next >
Cancel

Basic Flow


Malicious URL / Spam
Dropper Downloads Necurs
Necurs Protects its Registry, Files and Processes
Dropper Downloads Zeus
Necurs Adds Zeus to its Protection

The Components

- The Dropper (Executable .exe)
  - Infection Symptoms, The Executable, Rootkit Installation
- The Rootkit (Driver .sys)
  - The Driver, Access Denial, AV and Application Blocking

The Dropper

Infected by Necurs?

- Windows Platform (32 bit / 64 bit)
- Query ‘Syshost32’ Service.

The Dropper - Symptoms

Query ‘Syshost32’ Service

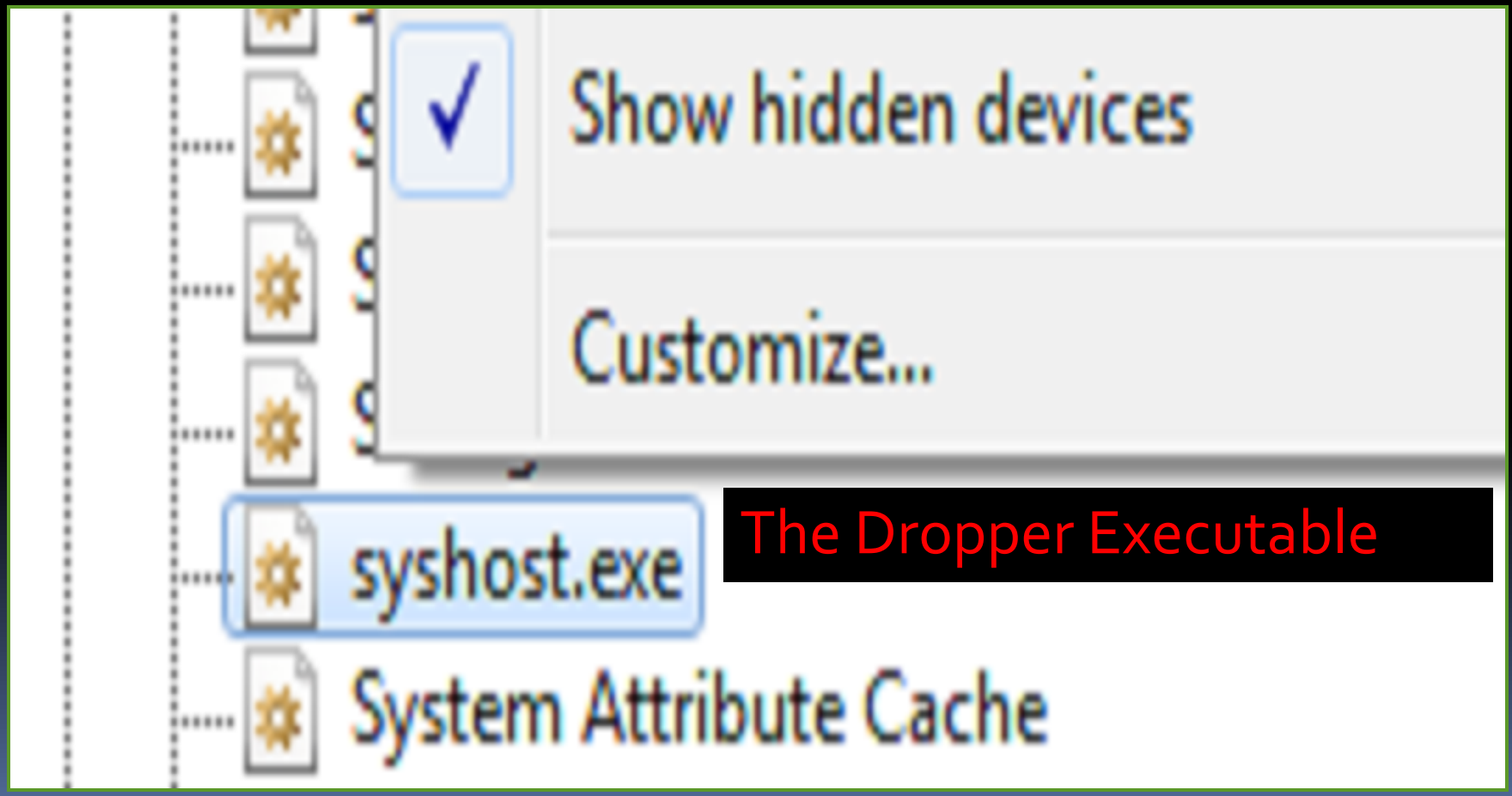
The Dropper

Infected by Necurs?

- Windows Platform (32 bit / 64 bit)
- Query ‘Syshost32’ Service.
- ‘Syshost.exe’ in Device Manager

The Dropper - Symptoms

‘Syshost.exe’ in Device Manager



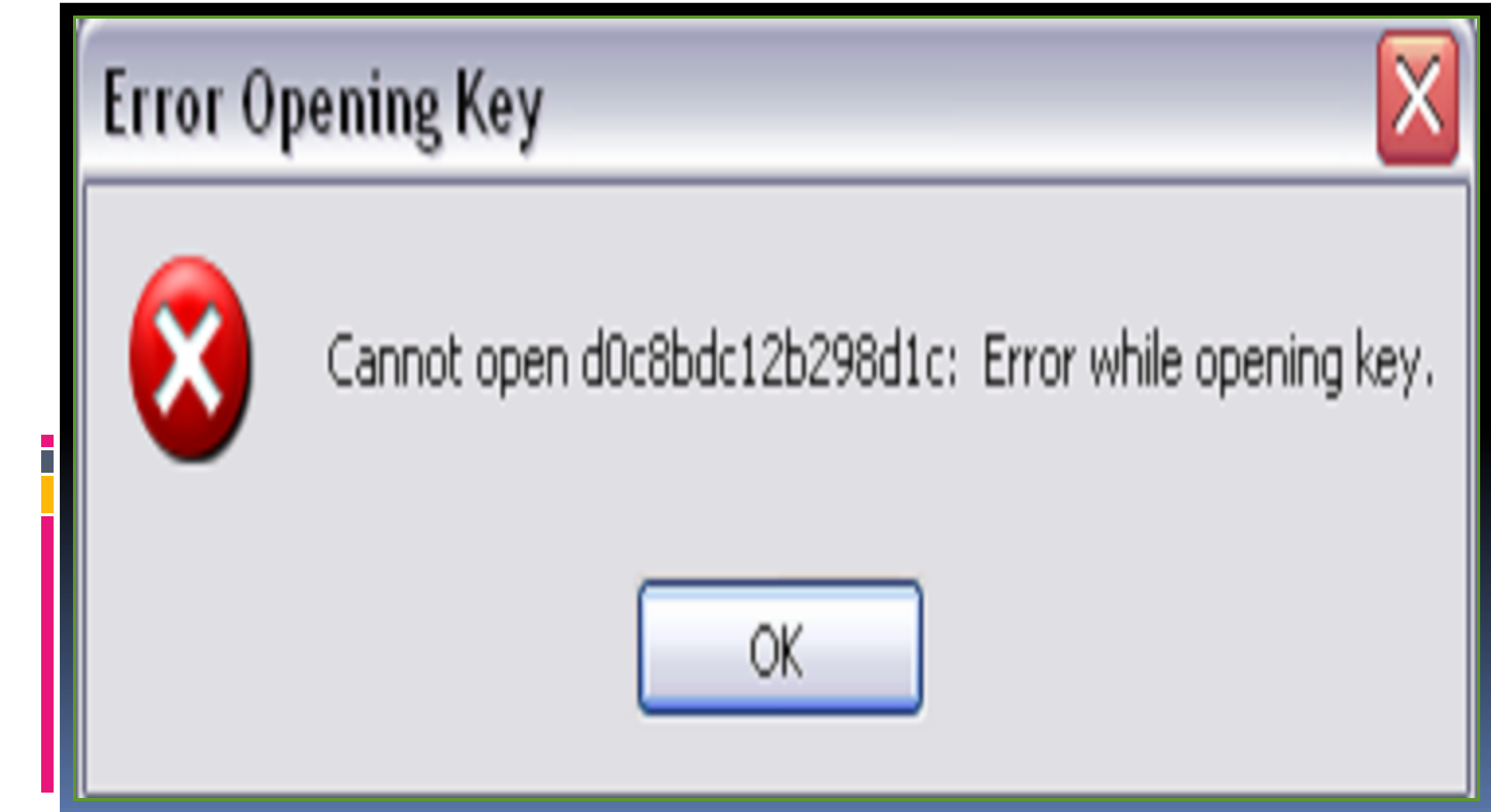
The Dropper

Infected by Necurs?

- Windows Platform (32 bit / 64 bit)
- Query ‘Syshost32’ Service.
- ‘Syshost.exe’ in Device Manager
- Parse “HKLM\ System\ CurrentControlSet\ Services”

The Dropper - Symptoms

Parse “HKLM\System\CurrentControlSet\Services”



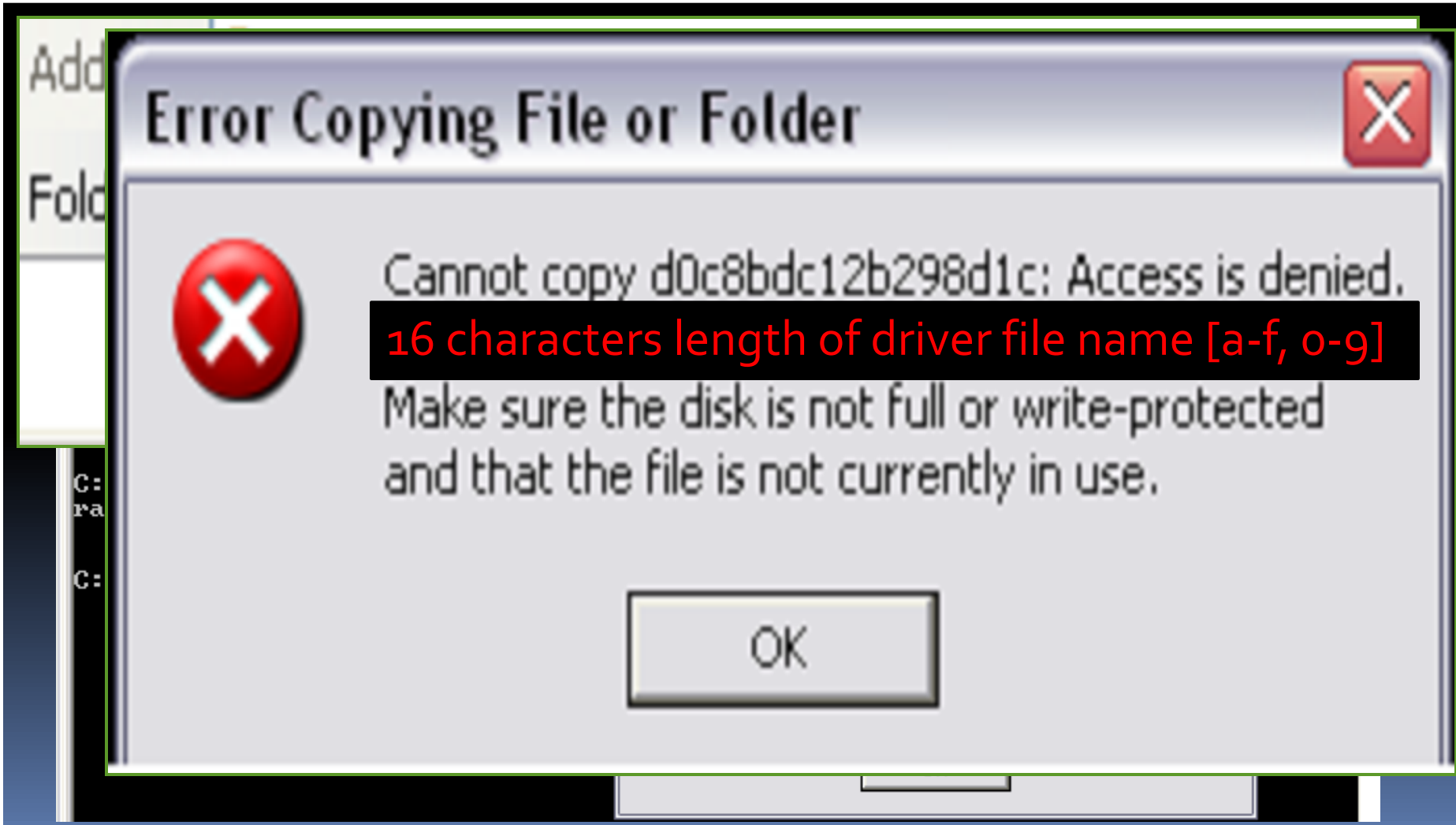
The Dropper

Infected by Necurs?

- Windows Platform (32 bit / 64 bit)
- Query ‘Syshost32’ Service.
- ‘Syshost.exe’ in Device Manager
- Parse “HKLM\ System\ CurrentControlSet\ Services”
- Verify Driver File Access Denial

The Dropper - Symptoms

Verify Driver File Access Denial



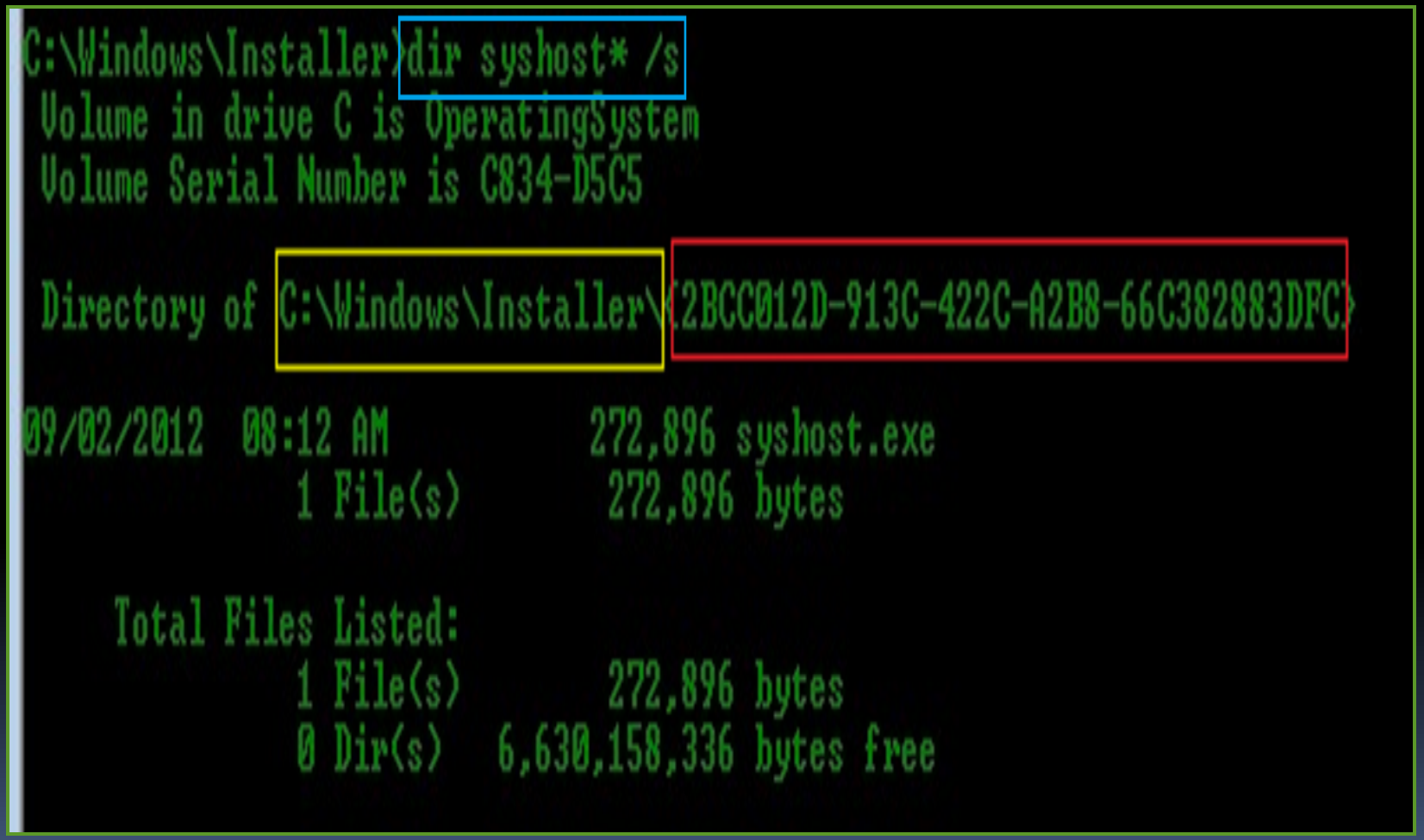
The Dropper

Infected by Necurs?

- Windows Platform (32 bit / 64 bit)
- Query ‘Syshost32’ Service.
- ‘Syshost.exe’ in Device Manager
- Parse “HKLM\ System\ CurrentControlSet\ Services”
- Verify Driver File Access Denial

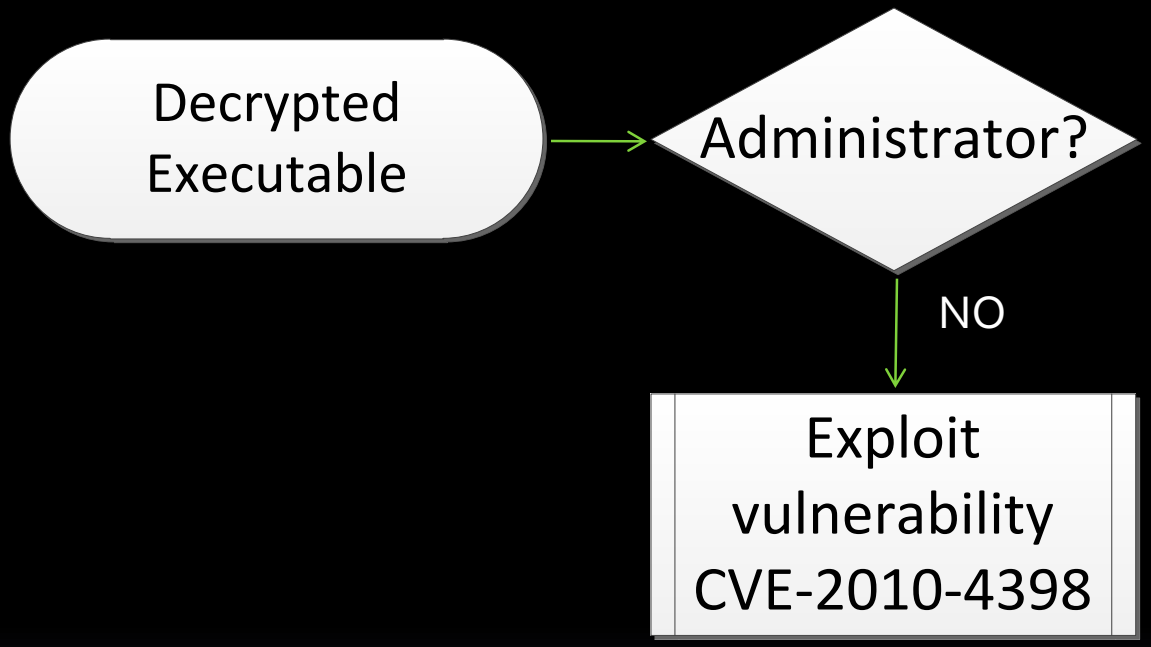
The Dropper

The Executable



The Dropper

Rootkit Installation



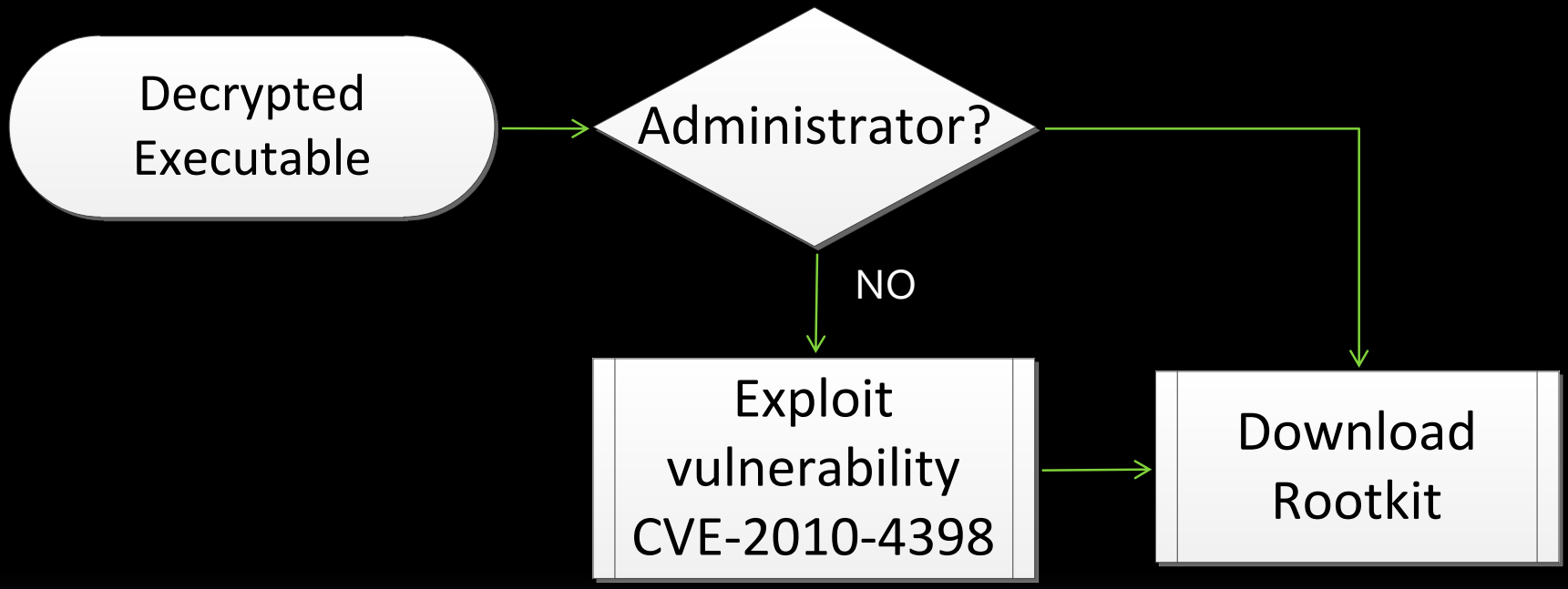
The Dropper

Privilege Escalation

- Vulnerability listed as CVE-2010-4398
- allows local users to gain admin privileges
- bypass the User Account Control (UAC)

The Dropper

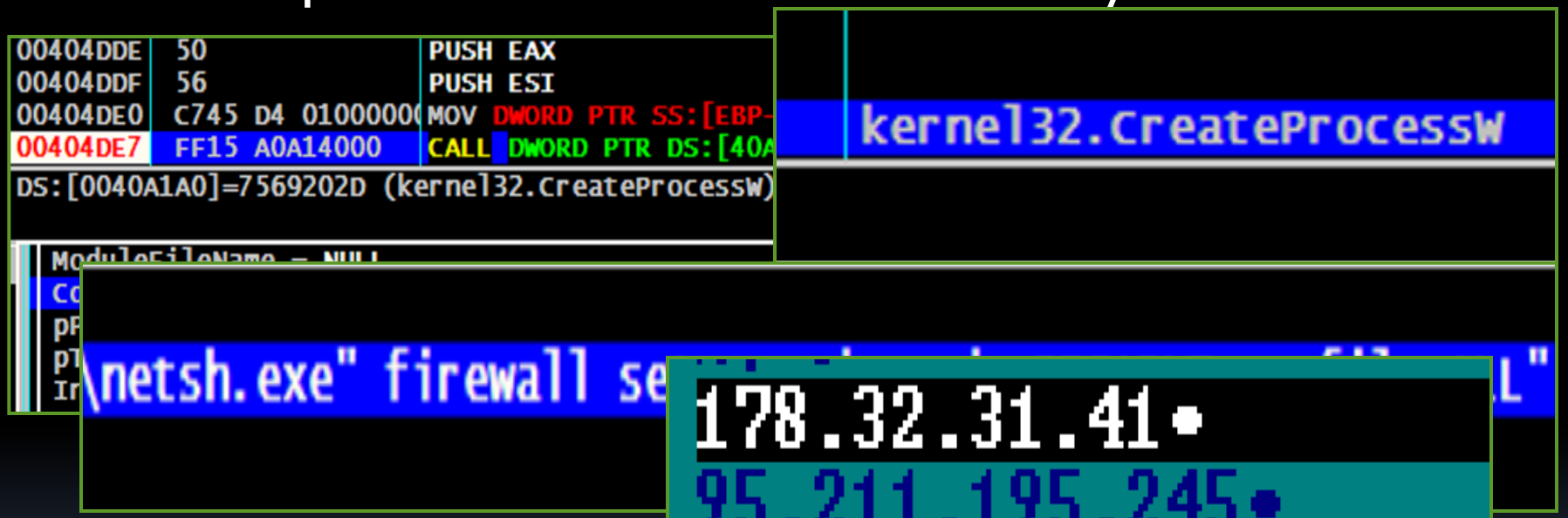
Rootkit Installation



The Dropper

Rootkit Download

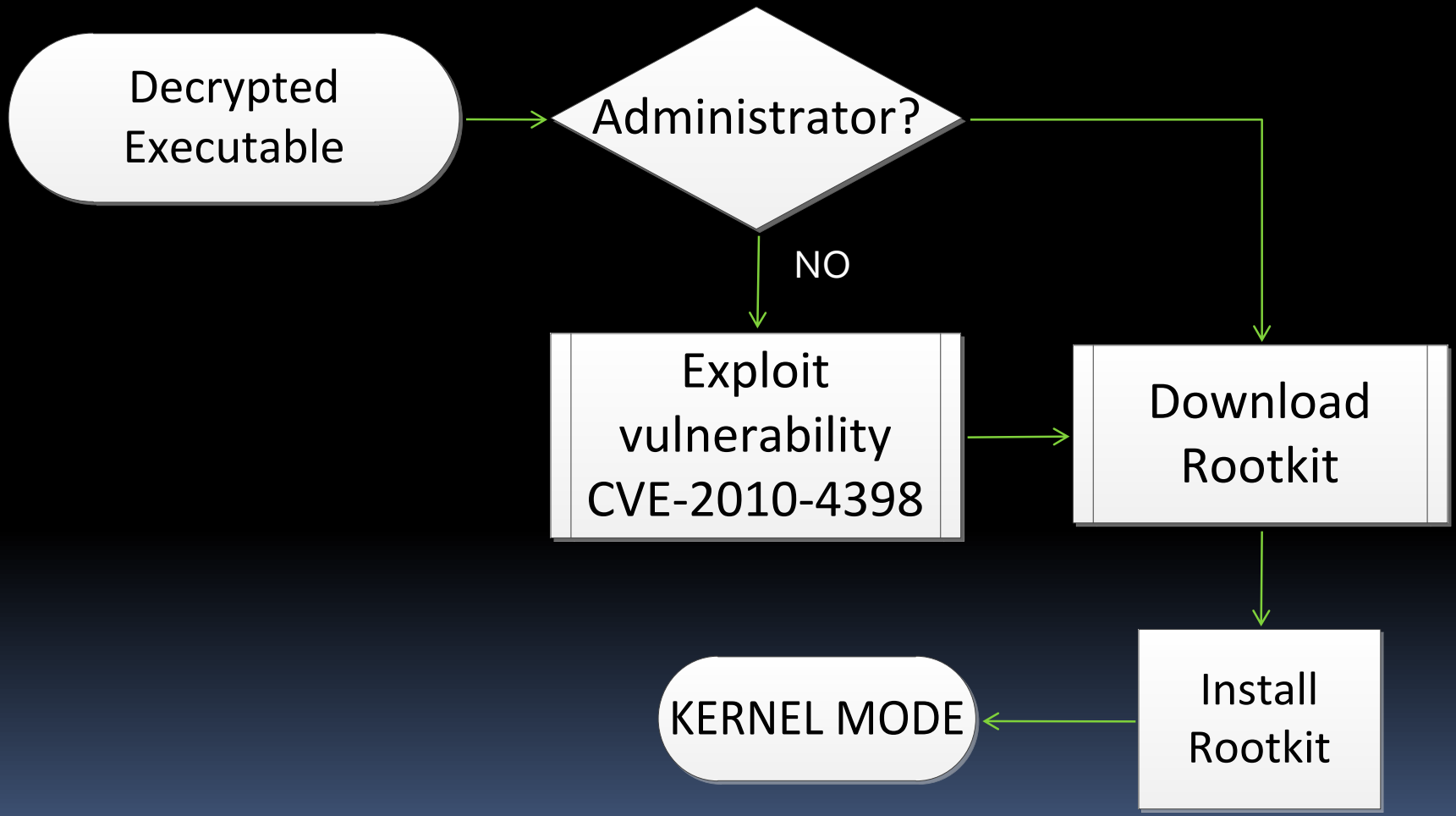
- Manipulate Windows Firewall by netsh.exe



- Decrypt a List of

The Dropper

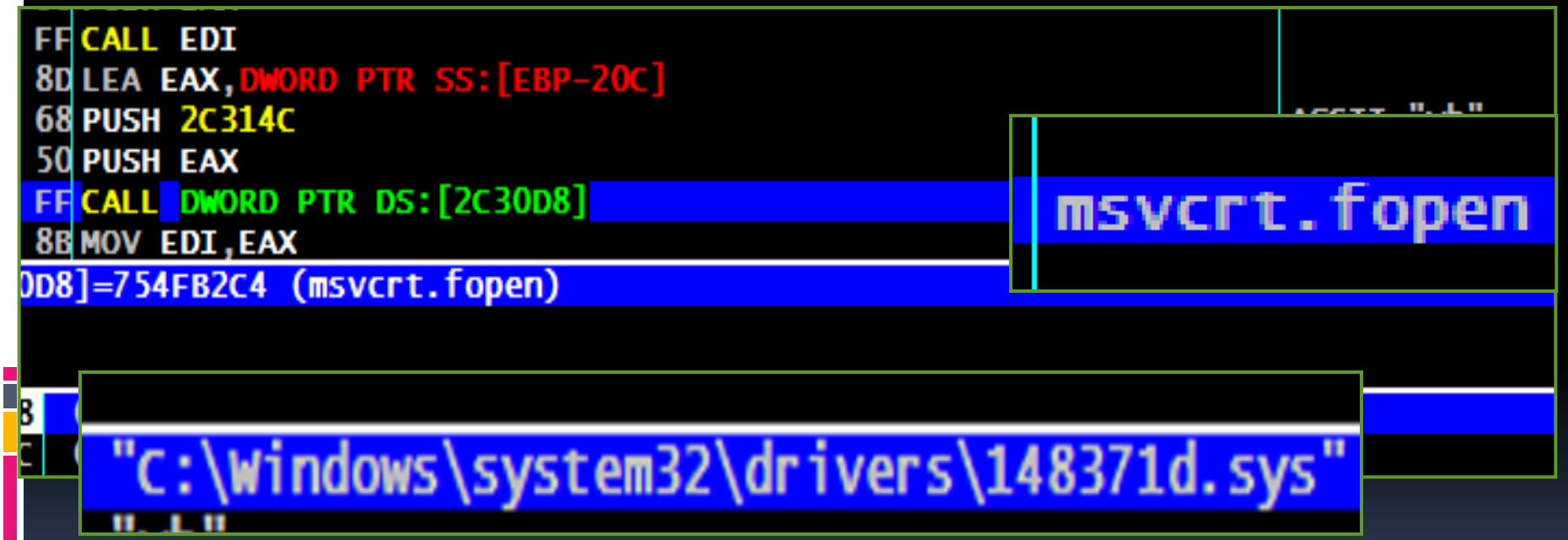
Rootkit Installation



The Dropper

Rootkit Installation

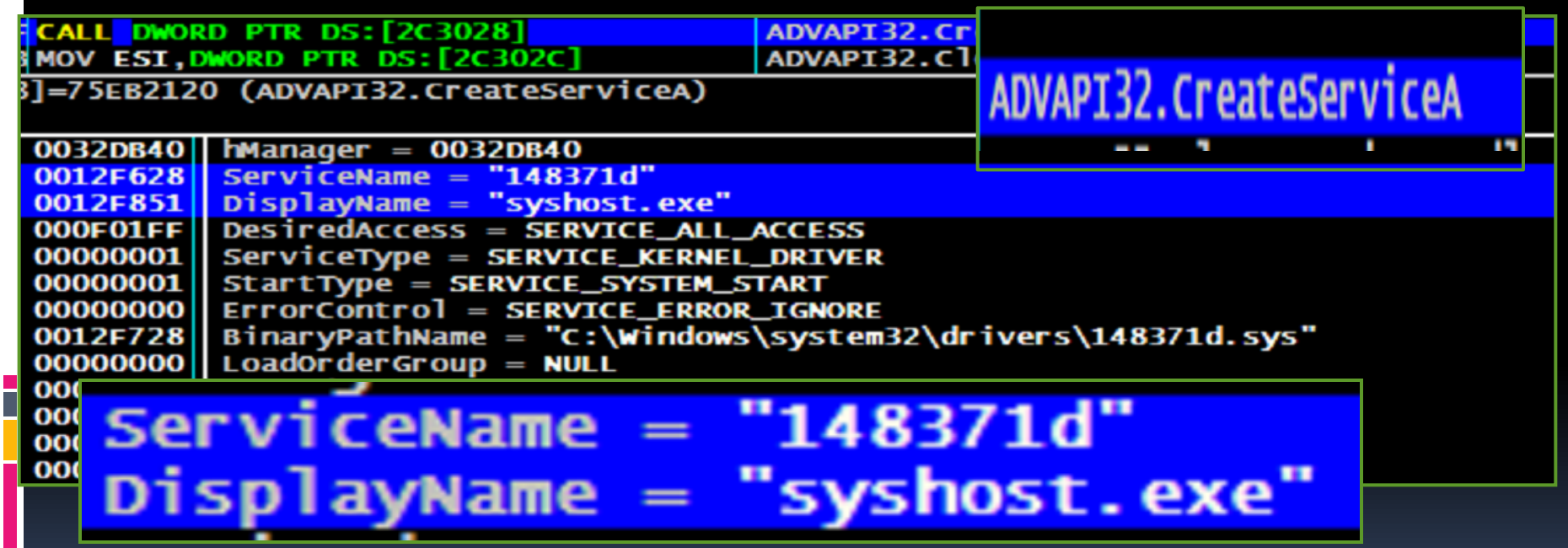
- Create System file



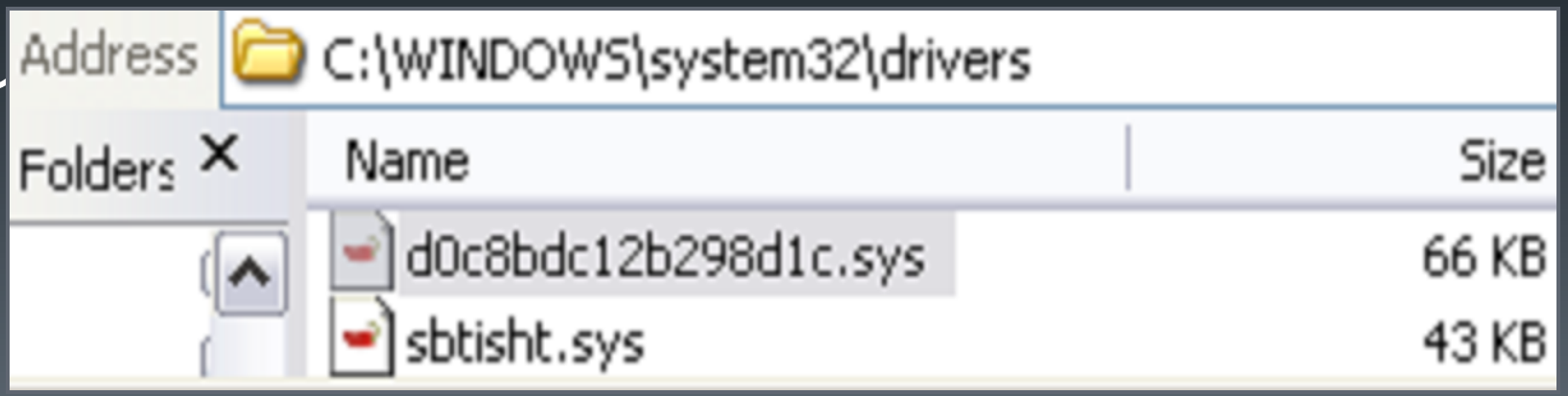
The Dropper

Rootkit Installation

- Load Rootkit as a Service

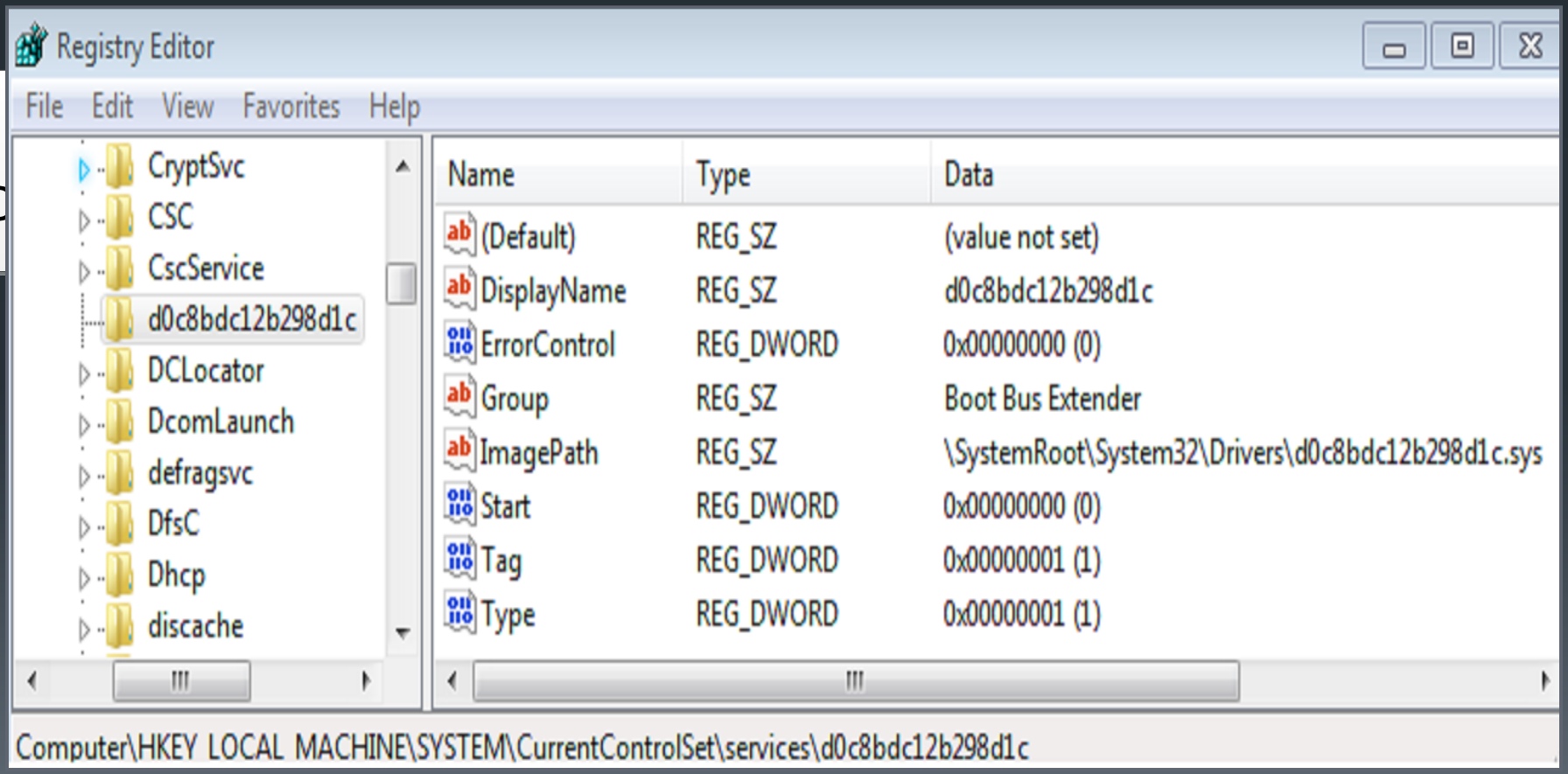


The Driver

- MD5 : eaa43802c3801389911b6ad35c0ee71
- Sample was Downloaded June 2014
- Obfuscated and will eventually decrypt a new file : 787328fa36df1ce151eebf44fe07c0a6
- 

The Driver

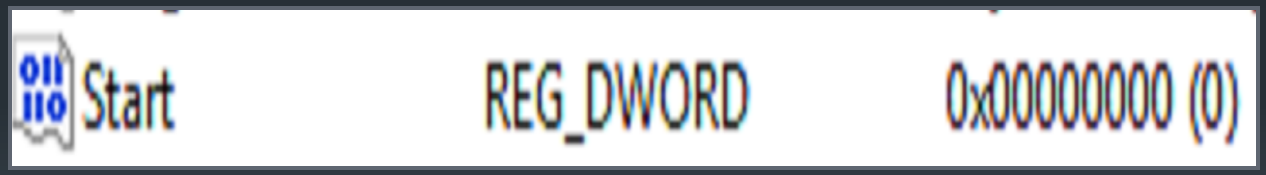
- Registry Entry at “\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services”



The Driver

- Registry Entry at “\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services”

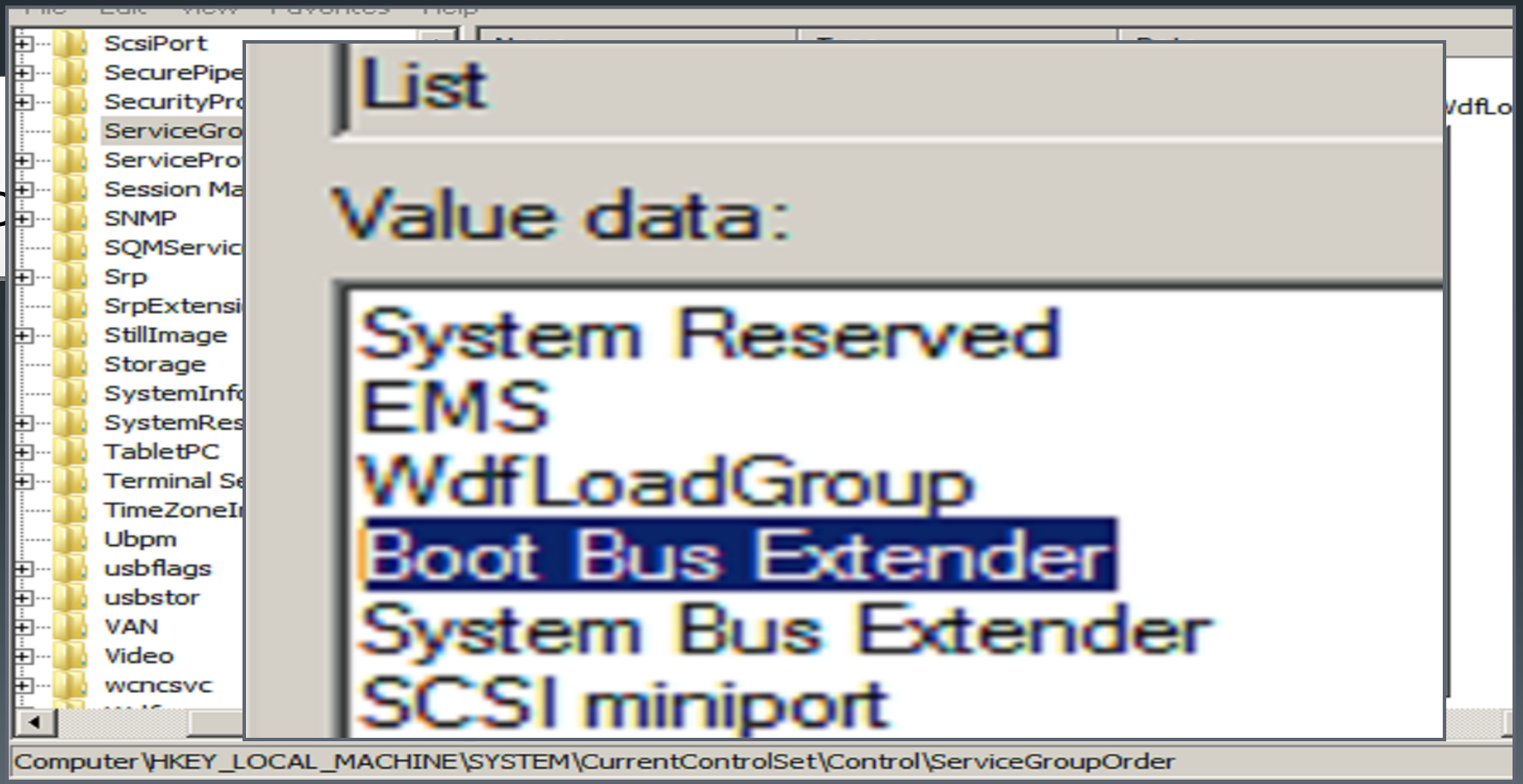
Load Boot Device Drivers



SERVICE_BOOT_START

The Driver

- “\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Control\ServiceGroupOrder”



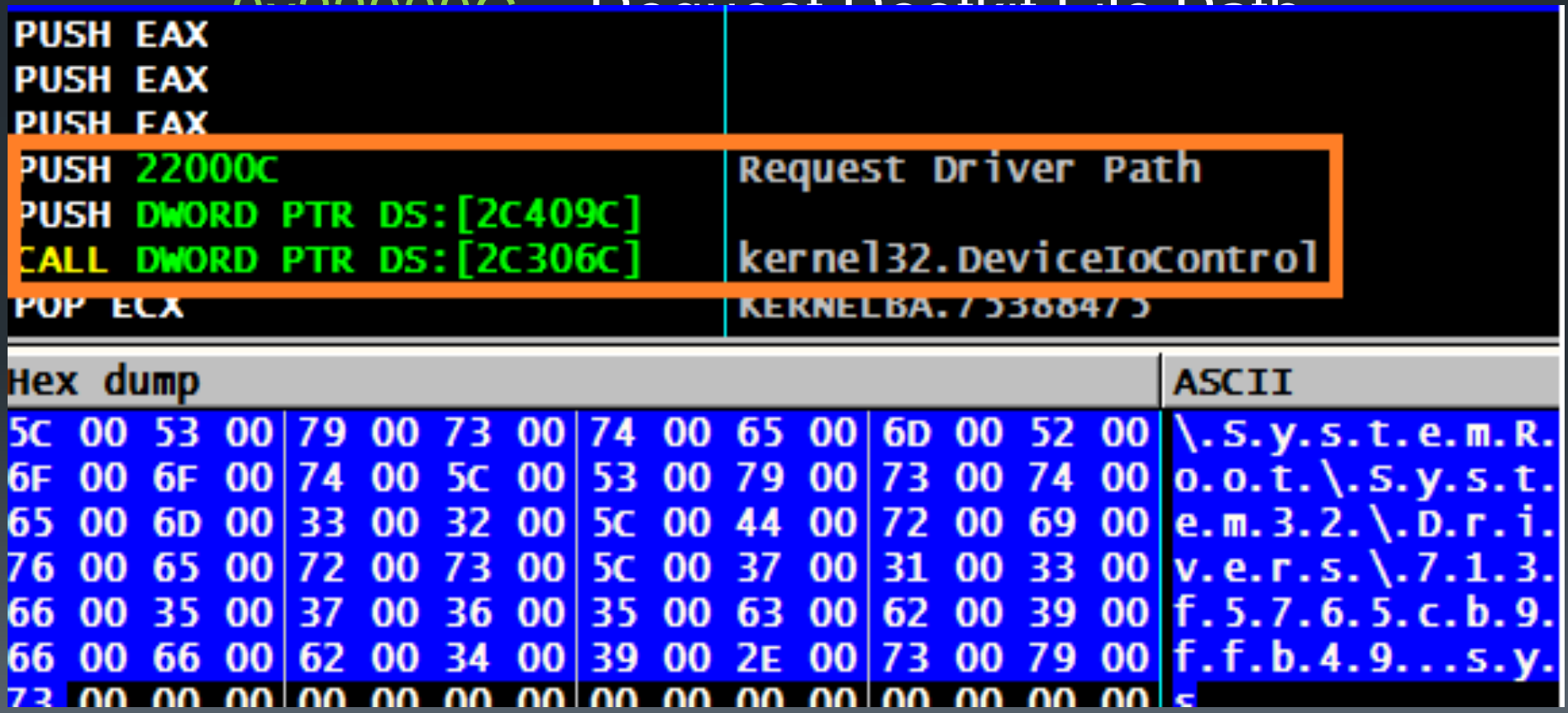
The Driver

- Registry Entry at "\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services"

- Able to load in Safe Mode
- Load before other Drivers

Driver – Dropper Communication

- Create device object "NtSecureSys" and a Symbolic link "\??\NtSecureSys"



Access Denial

- Registry - CmRegisterCallback API

```
.000140E5: 50                push        eax
```

A filter driver's *RegistryCallback* routine can monitor, block, or modify a registry operation.

Syntax

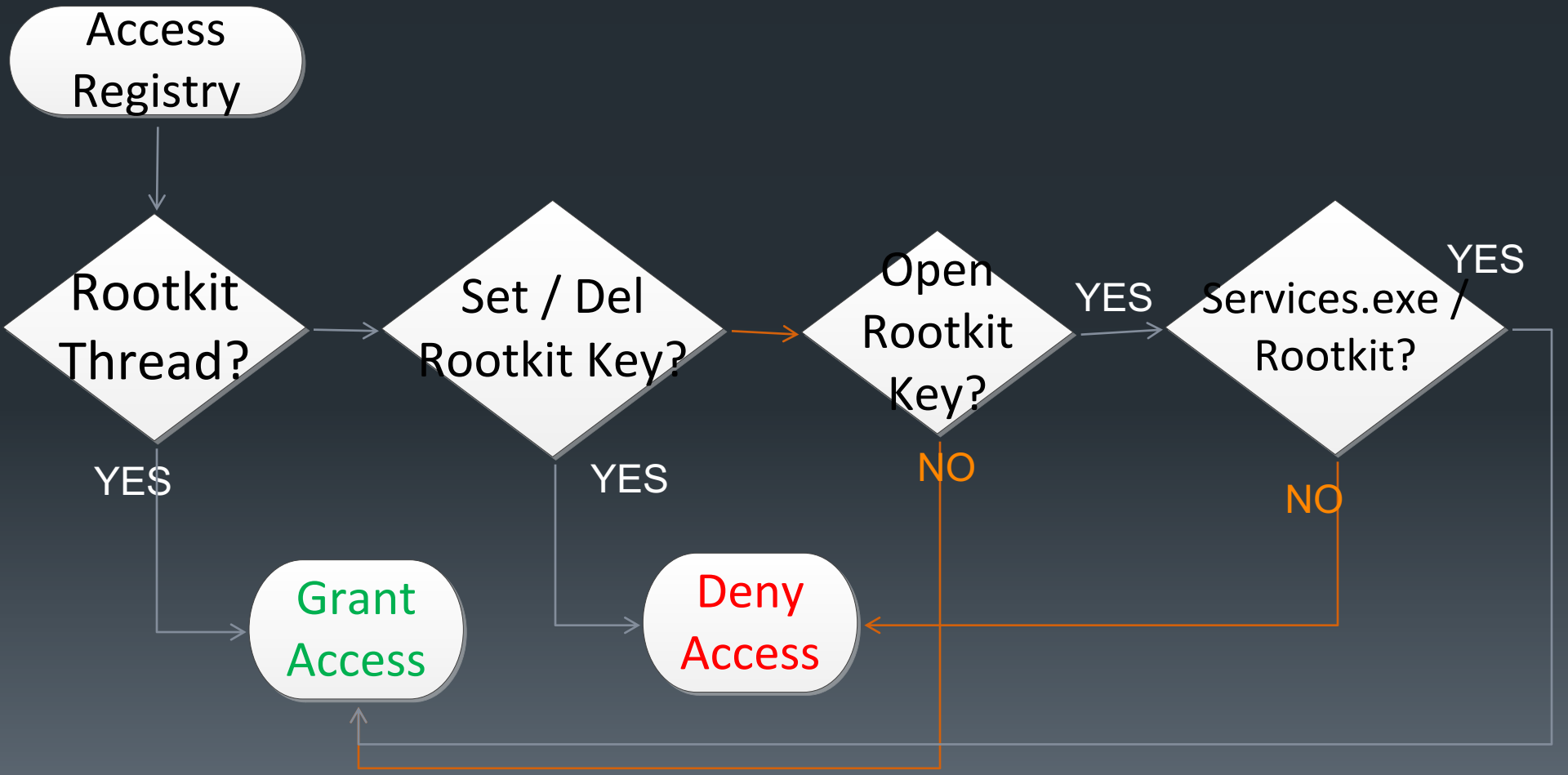
C++

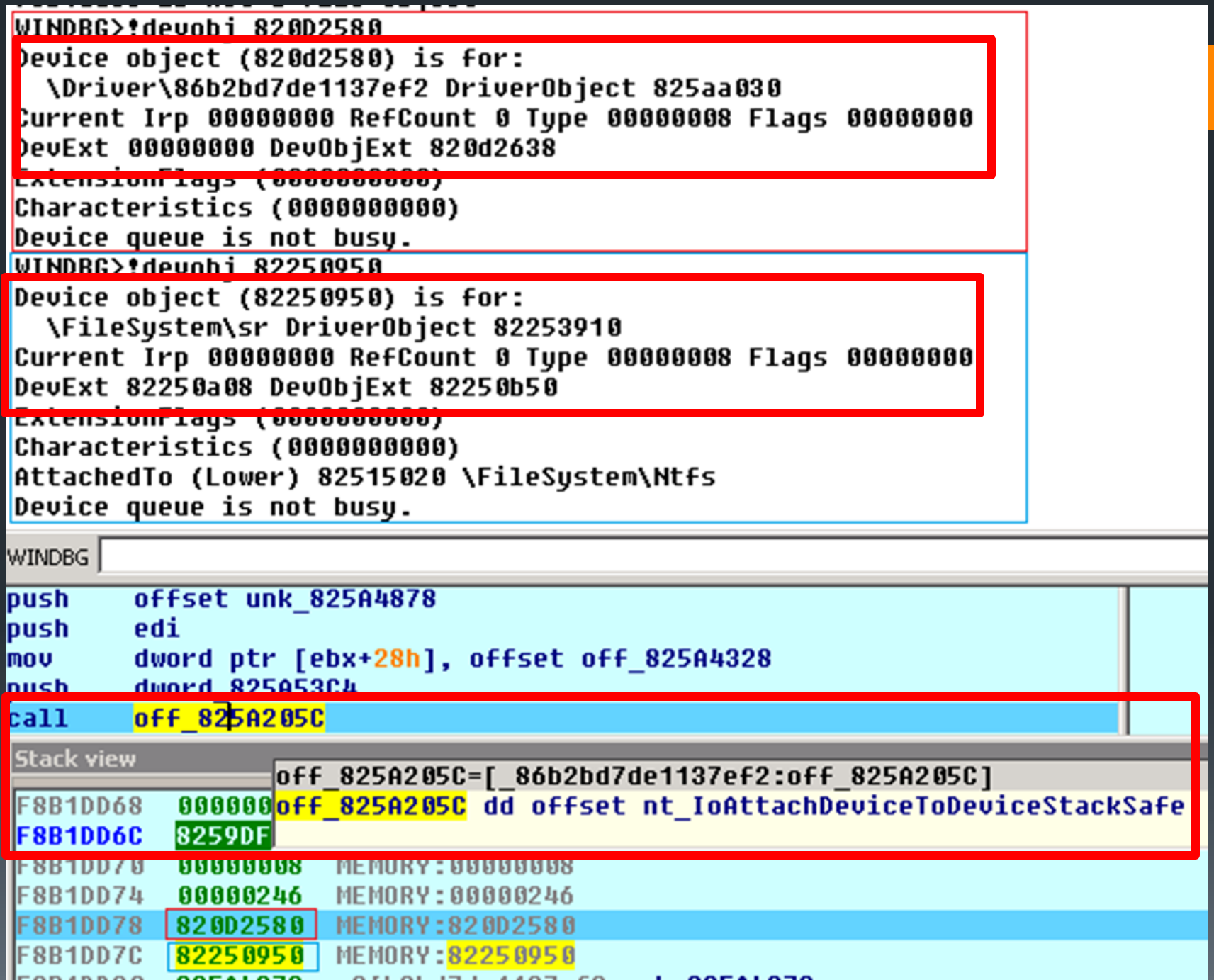
```
EX_CALLBACK_FUNCTION RegistryCallback;

NTSTATUS RegistryCallback(
  _In_       PVOID CallbackContext,
  _In_opt_   PVOID Argument1,
  _In_opt_   PVOID Argument2
)
{ ... }
```

Access Denial

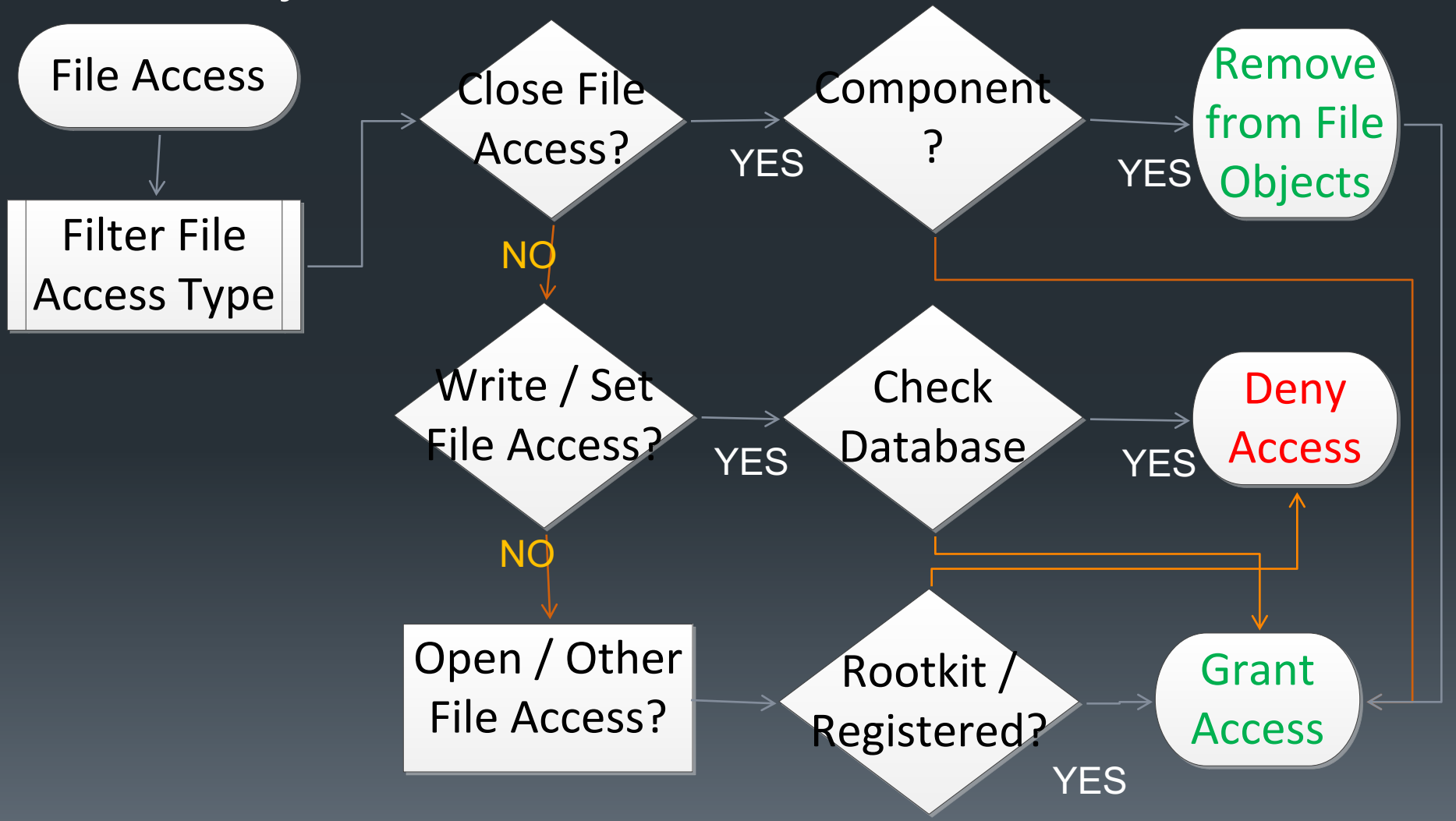
- Registry CallBack Flow




WINDBG>!devobj 820D2580
Device object (820d2580) is for:
\Driver\86b2bd7de1137ef2 DriverObject 825aa030
Current Irp 00000000 RefCount 0 Type 00000008 Flags 00000000
DevExt 00000000 DevObjExt 820d2638
Characteristics (0000000000)
Device queue is not busy.
WINDBG>!devobj 82250950
Device object (82250950) is for:
\FileSystem\sr DriverObject 82253910
Current Irp 00000000 RefCount 0 Type 00000008 Flags 00000000
DevExt 82250a08 DevObjExt 82250b50
Characteristics (0000000000)
AttachedTo (Lower) 82515020 \FileSystem\Ntfs
Device queue is not busy.
WINDBG
push offset unk_825A4878
push edi
mov dword ptr [ebx+28h], offset off_825A4328
call off_825A205C
Stack view
off_825A205C=[_86b2bd7de1137ef2:off_825A205C]
F8B1DD68 000000 off_825A205C dd offset nt_IoAttachDeviceToDeviceStackSafe
F8B1DD6C 8259DF
F8B1DD74 00000246 MEMORY:00000246
F8B1DD78 820D2580 MEMORY:820D2580
F8B1DD7C 82250950 MEMORY:82250950

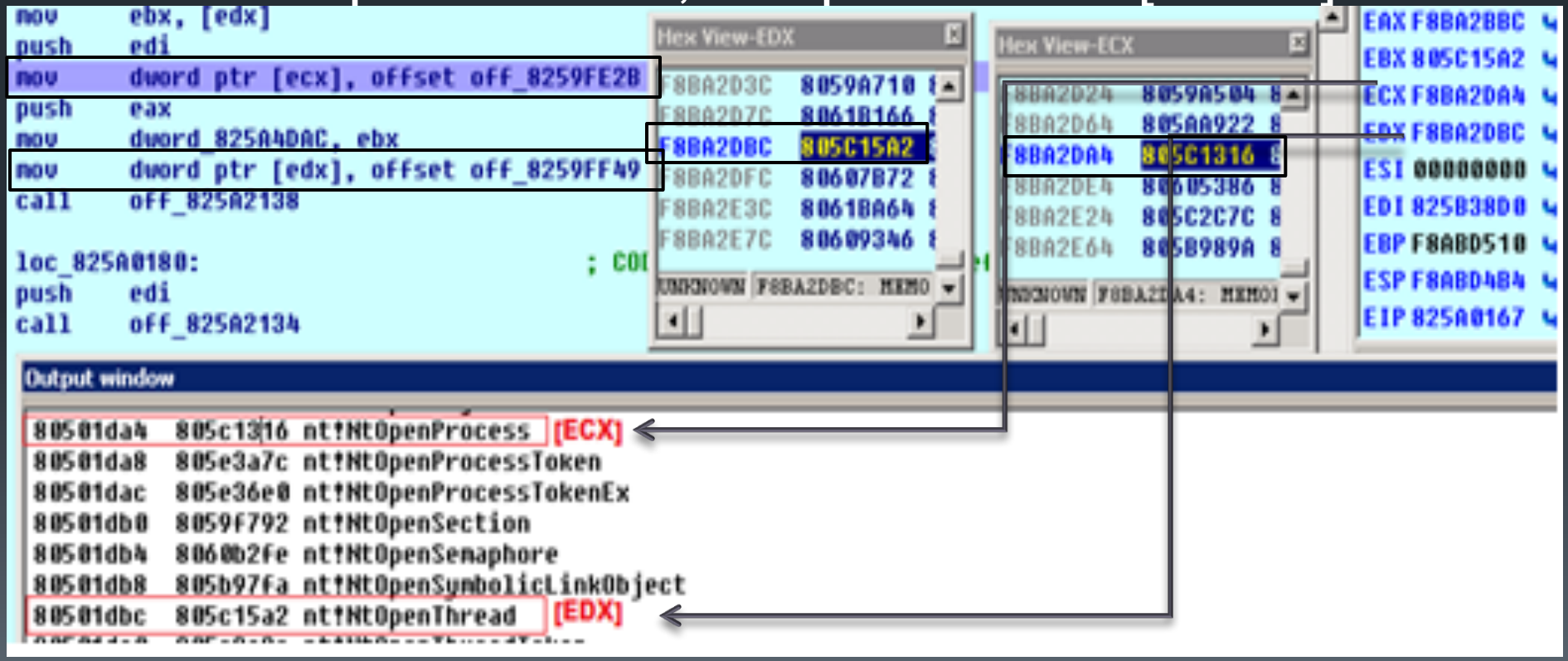
Access Denial

- FileSystem Filter Flow



Access Denial

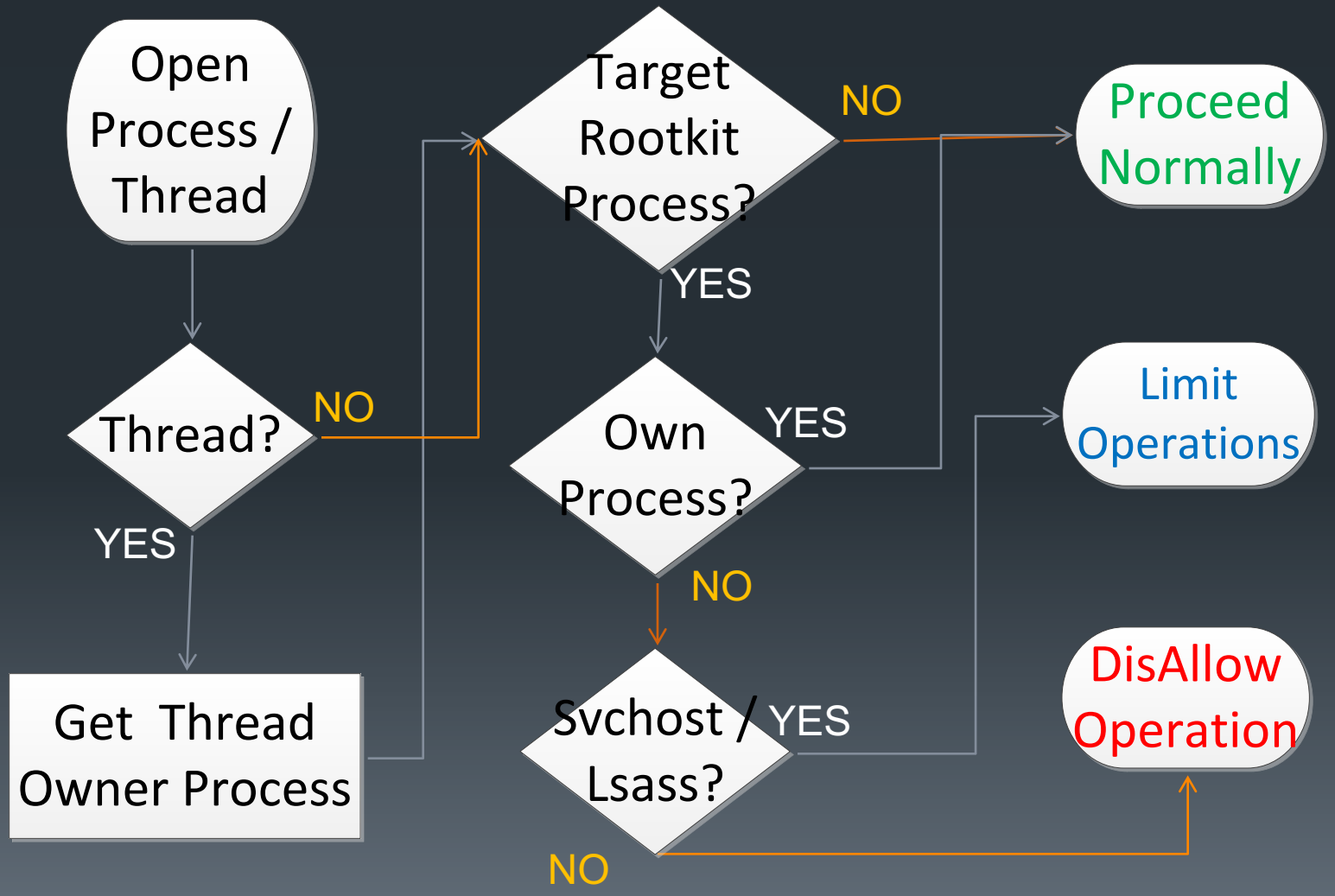
- Process / Thread
  - API ObRegisterCallbacks
  - NtOpenProcess, NtOpenThread [SSDT]



The Rootkit

Access Denial

- Process / Thread Call Back



The Ro

Appli

- Blac
  - V

C

Parse Registry
"ImagePat

Parse PE file
System32 a
System32\Dr

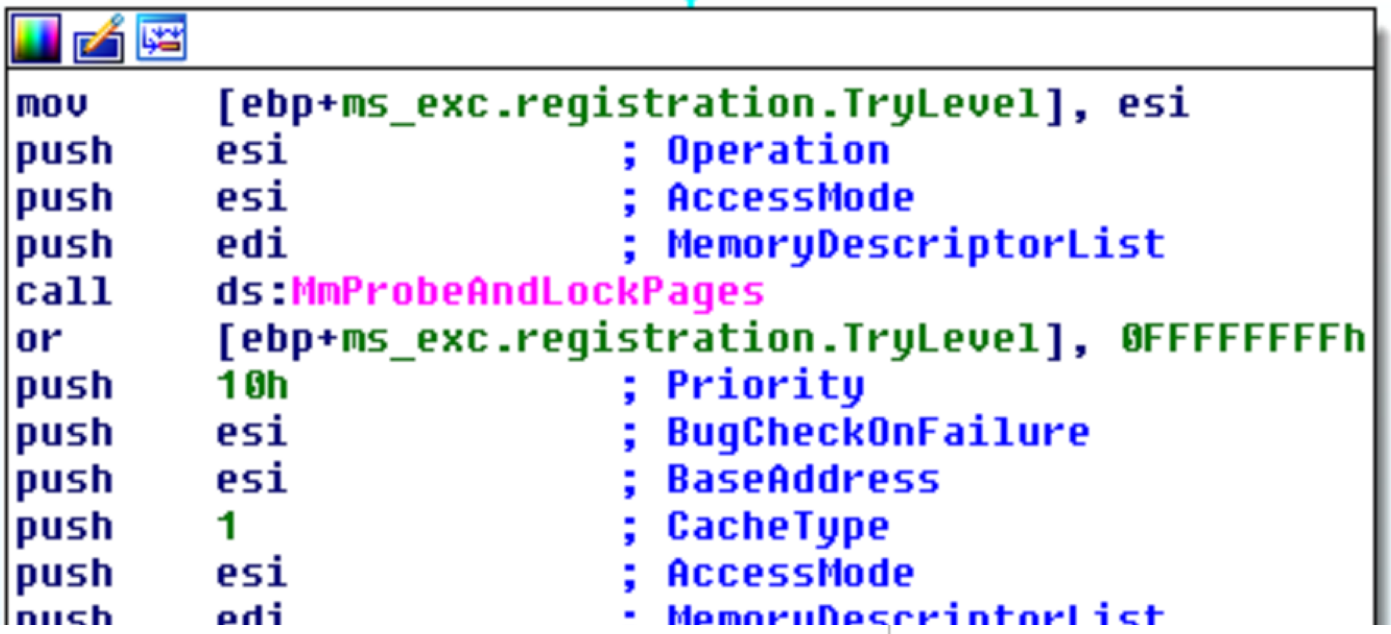
te list

Compute File
Name FMV –
1 Hash

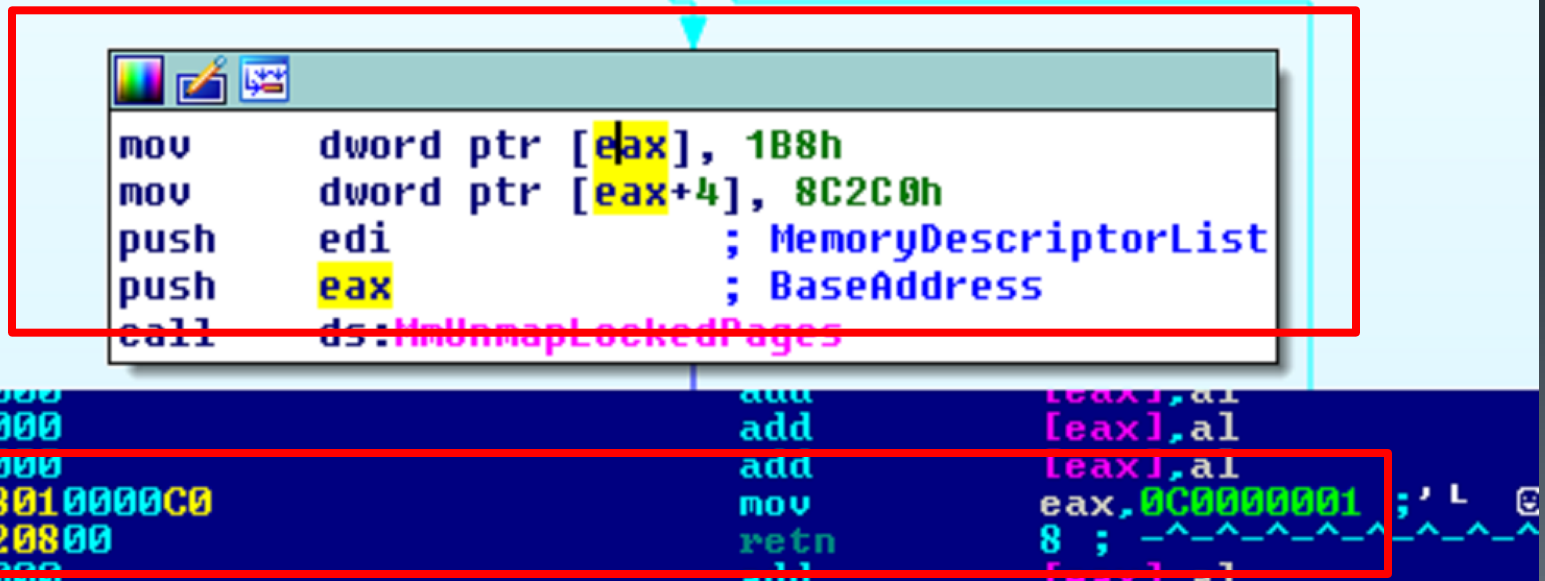
tore at
32 / DB5

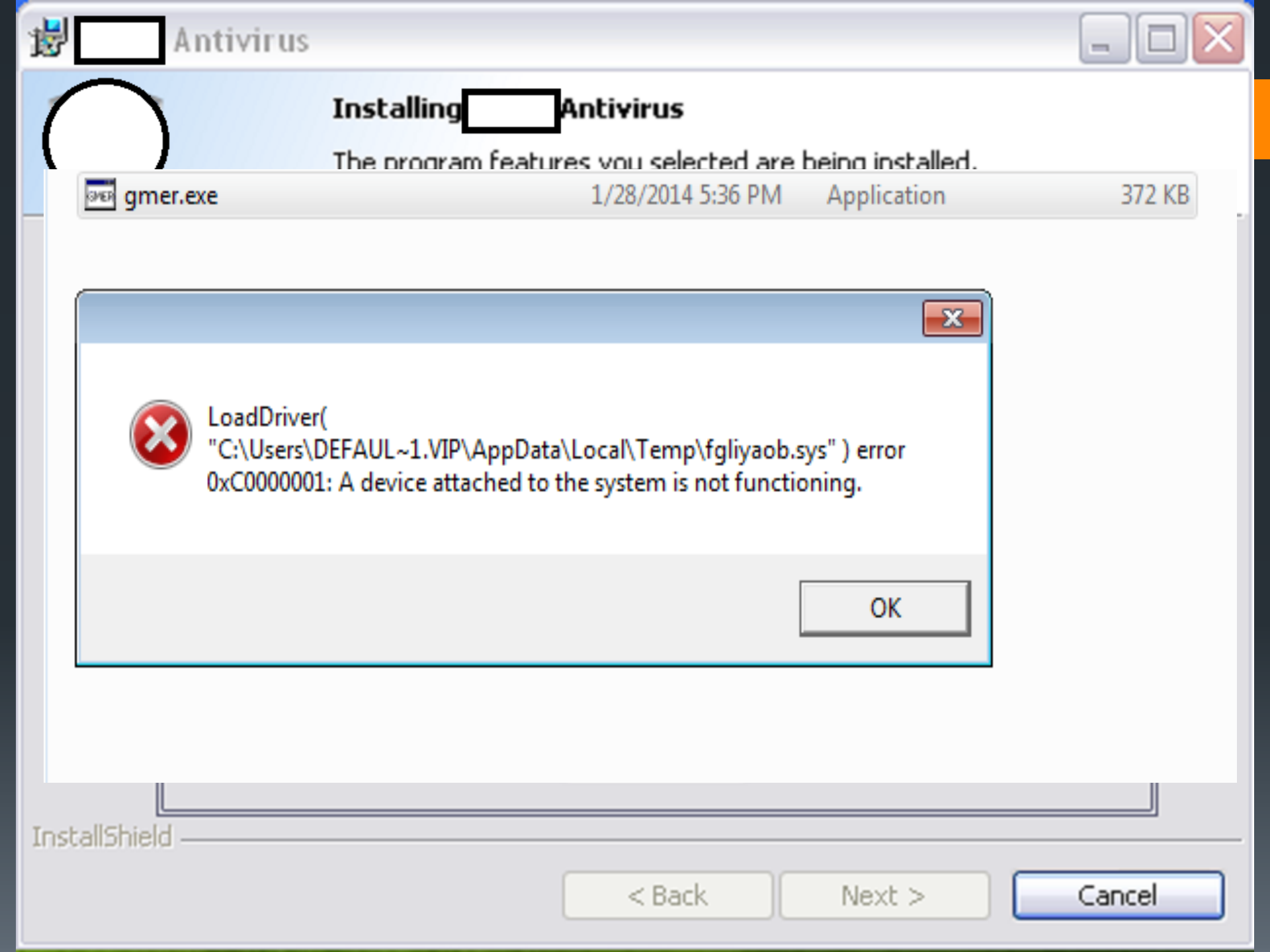
SUNBELT SOFTWARE•
Sunbelt Software•
K7 Computing•
Immunet Corporation•
Beijing Rising•
G DATA Software•
Quick Heal Technologies•
Comodo Security Solutions•
Sophos Plc•
Anti-Virus•
CJSC Returnil Software•
NovaShield Inc•
antimalware•
BullGuard Ltd•
Check Point Software Technologies Ltd•
Panda Software International•
Kaspersky Lab•
FRISK Software International Ltd•
ESET, spol. s r.o.•
Doctor Web Ltd•
Comodo Inc•
BitDefender SRL•
BITDEFENDER LLC•
Avira GmbH•
GRISOFT, s.r.o.•
PC Tools•
ALWIL Software•
Agnitum Ltd•
dkprocesshacker.sys•

App



0xC0000001 STATUS_UNSUCCESSFUL	{Operation Failed} The requested operation was unsuccessful.




[redacted] Antivirus
Installing [redacted] Antivirus
The program features you selected are being installed.
gmer.exe 1/28/2014 5:36 PM Application 372 KB
LoadDriver(
"C:\Users\DEFAUL~1.VIP\AppData\Local\Temp\fgliyaob.sys") error
0xC0000001: A device attached to the system is not functioning.
OK
InstallShield
< Back
Next >
Cancel

GameOver Zeus

- Resurrected as of July 2014
- Used to install CryptoLocker ransomware.
- Blamed for more than $100 million theft from banks, businesses and consumers worldwide.

Removal Tips

- Use a Boot CD e.g. [Hiren's]
- Demonstration

References

- http://stopmalvertising.com/rootkits/analysis-of-zeus-gameover-with-necurs.html
- http://www.f-secure.com/weblog/archives/00002717.html
- http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4398
- http://www.infosecurity-magazine.com/view/29806/necurs-rootkit-not-new-but-spreading-fast-warns-microsoft
- krebsonsecurity.com/tag/gameover-zeus/
- MSDN
- Peter Ferrie http://pferrie.host22.com/papers/