

Nico Yturriaga

September 27, 2014

THE NECURS ROOTKIT

Why Necurs?

- Infected 80,000+ during December 2012



What is a Rootkit?

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



Installing Antivirus



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

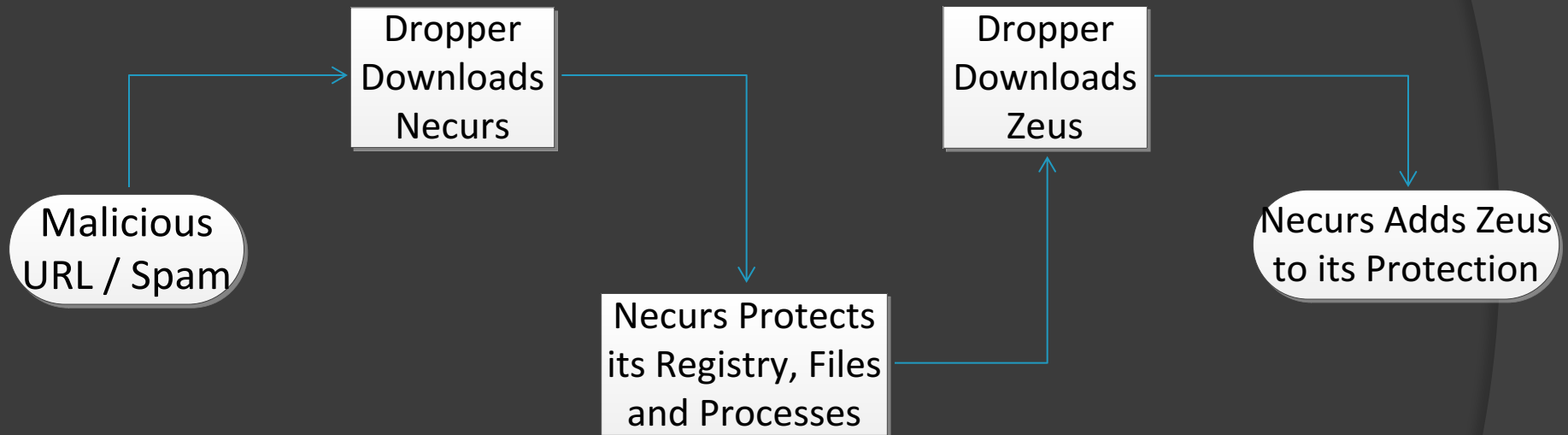
AntiVirus protects your computer from viruses, spyware, worms, and trojans.
Anti-Rootkit kernel-mode driver not found.

< Back

Next >

Cancel

Basic Flow



The Components

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



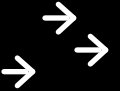
The Dropper

Infected by Necurs?

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

The Dropper - Symptoms

Query 'SysHost32' Service



```
...an732test>sc query sysHost32  
  
C:\Use...  
SERV...  
SERVICE_NAME: sysHost32  
        TYPE               : 10  WIN32_OWN_PROCESS  
        STATE                : 4   RUNNING  
        (NOT_STOPPABLE, NO...  
        WIN32_EXIT_CODE       : 0    (0x0)  
        SERVICE_EXIT_CODE   : 0    (0x0)
```

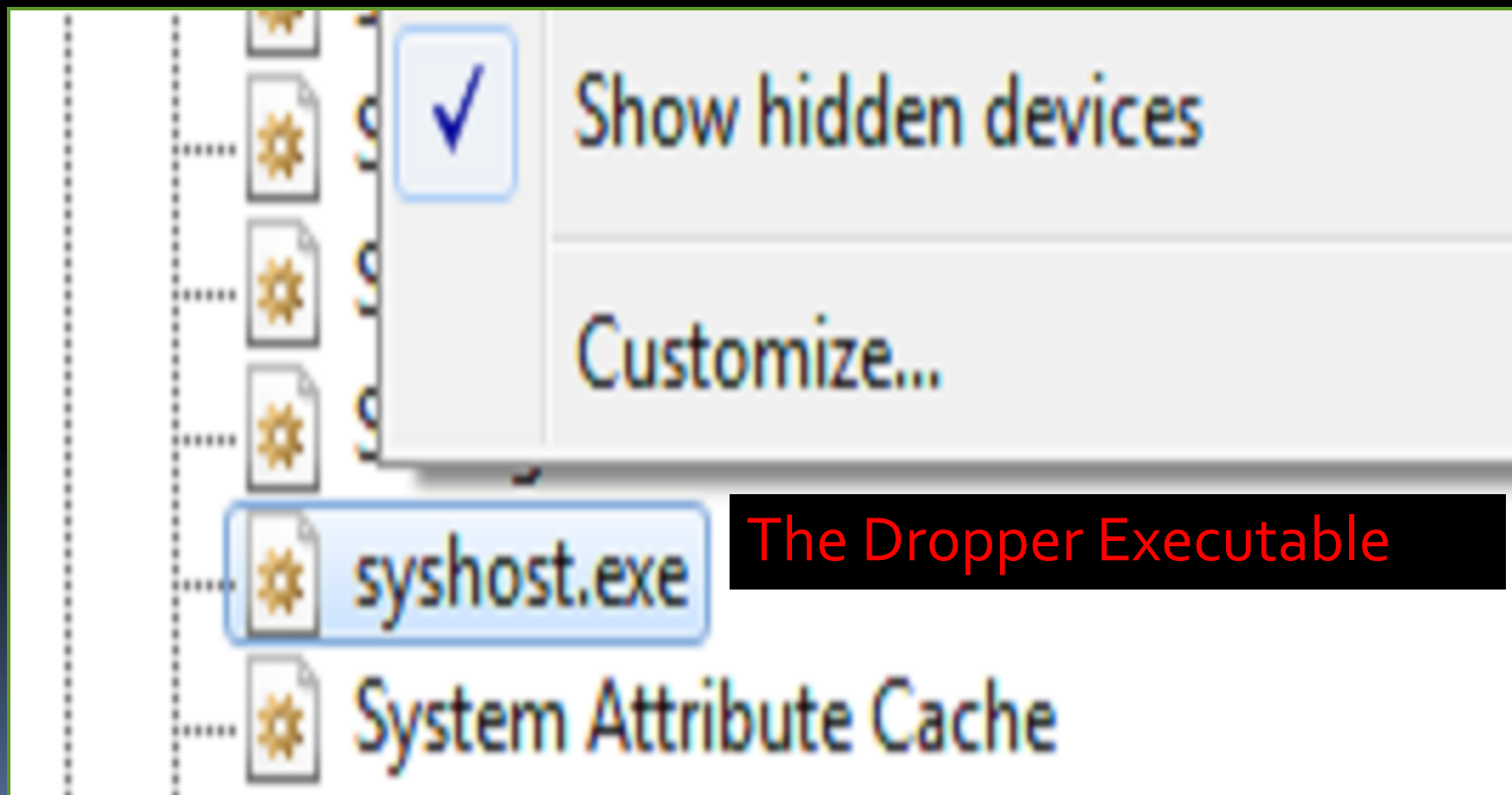

The Dropper

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



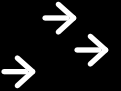
The Dropper

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”

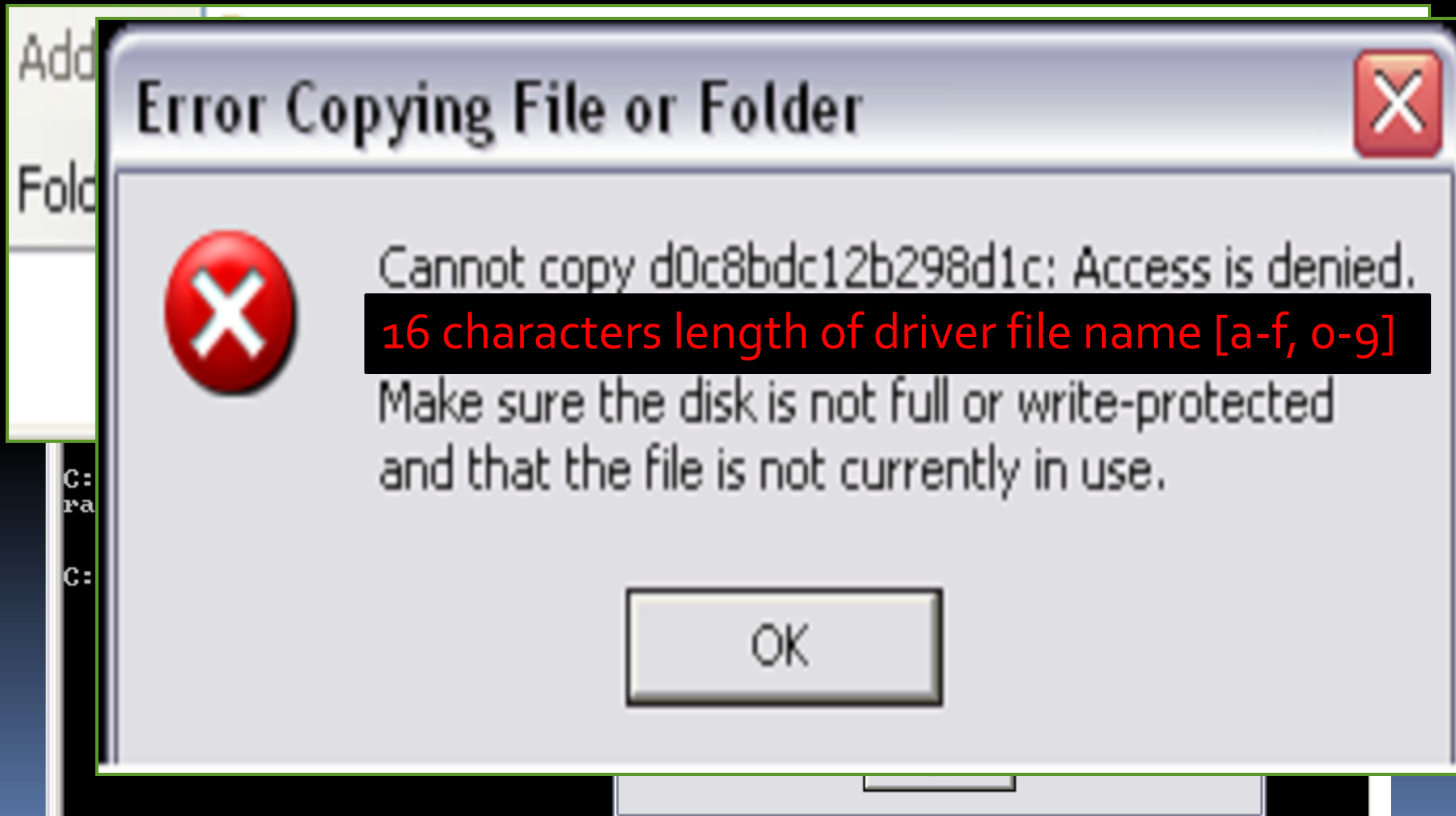
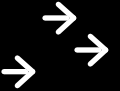


Infected by Necurs?

- 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



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

```
C:\Windows\Installer>dir syshost* /s
Volume in drive C is OperatingSystem
Volume Serial Number is C834-D5C5

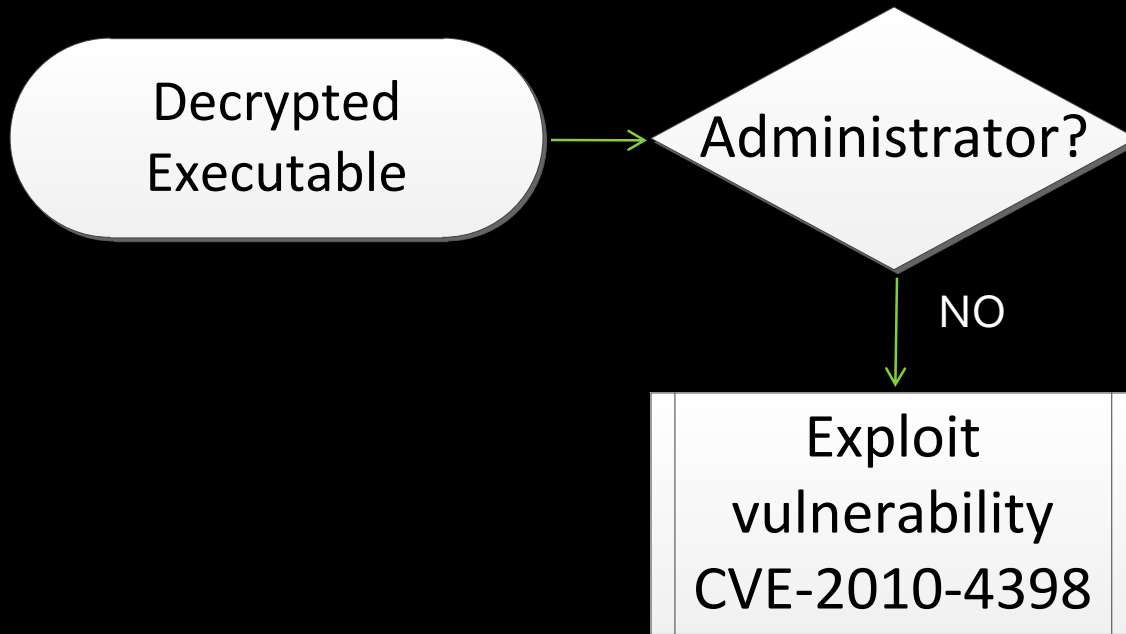
Directory of C:\Windows\Installer\{2BCC012D-913C-422C-A2B8-66C382883DFC}

09/02/2012  08:12 AM                272,896 syshost.exe
                1 File(s)                272,896 bytes

Total Files Listed:
                1 File(s)                272,896 bytes
                0 Dir(s)  6,630,158,336 bytes free
```


The Dropper

Rootkit Installation



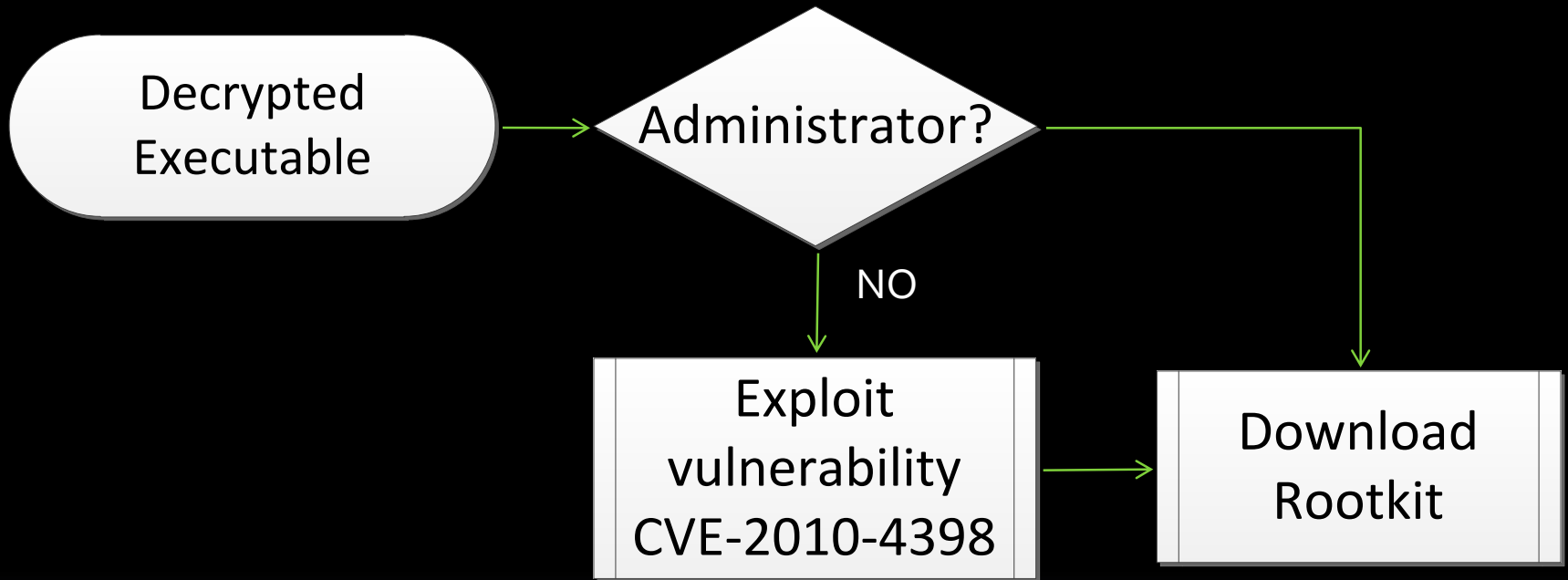
The Dropper

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

```
00404DDE  50          PUSH EAX
00404DDF  56          PUSH ESI
00404DE0  C745 D4 01000000 MOV DWORD PTR SS:[EBP-
00404DE7  FF15 A0A14000 CALL DWORD PTR DS:[40A
DS:[0040A1A0]=7569202D (kernel32.CreateProcessW)
```

kernel32.CreateProcessW

ModuleFileName = NULL

Co

PF

PT

Ir

netsh.exe" firewall se

178.32.31.41•

95.211.195.245•

94.231.81.24•

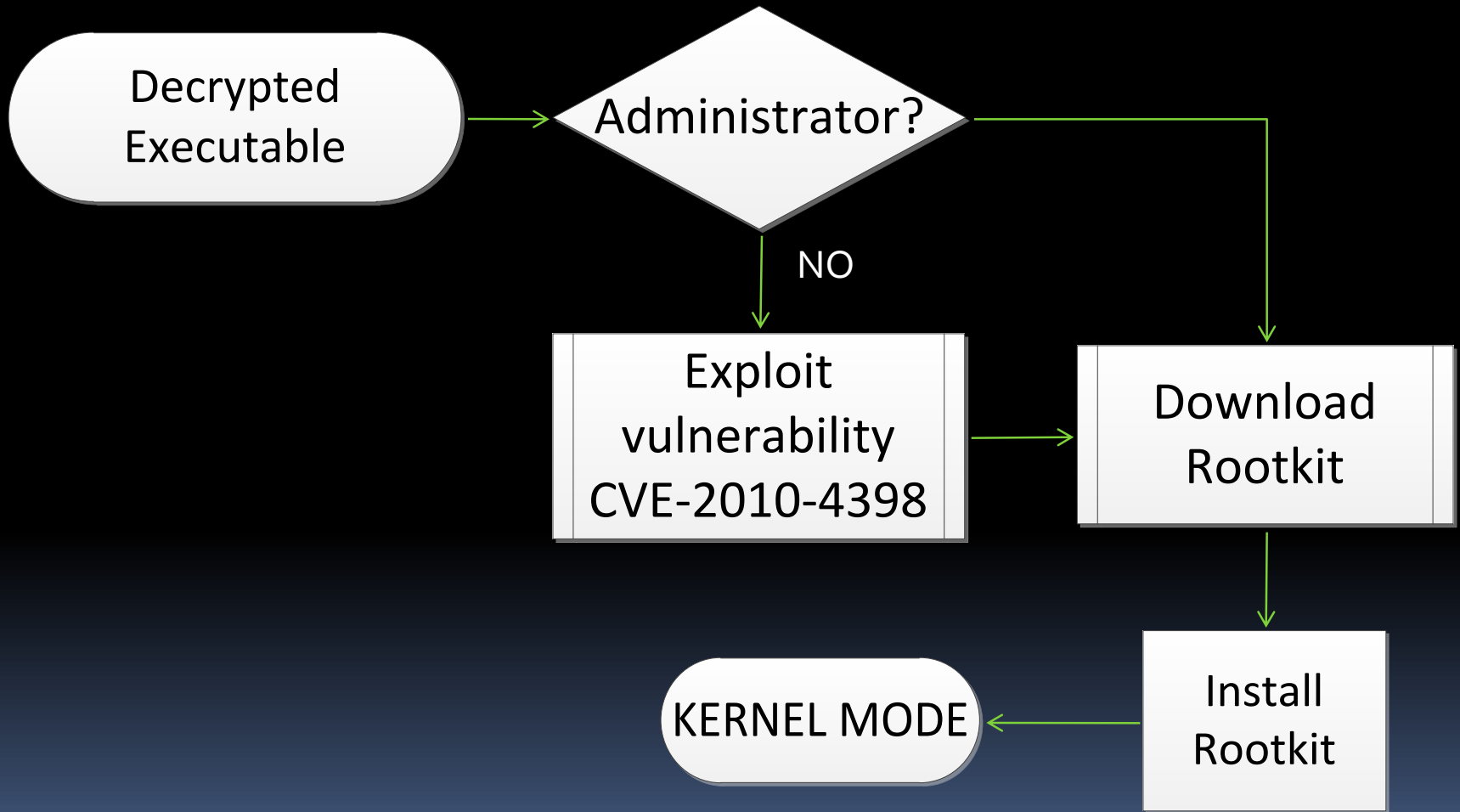
162.243.56.54•

91.213.8.35•

- Decrypt a List of

The Dropper

Rootkit Installation



The Dropper

Rootkit Installation

- Create System file

```
FF CALL EDI
8D LEA EAX, DWORD PTR SS:[EBP-20C]
68 PUSH 2C314C
50 PUSH EAX
FF CALL DWORD PTR DS:[2C30D8]
8B MOV EDI, EAX
0D8]=754FB2C4 (msvcrt.fopen)
```

msvcrt.fopen

"C:\windows\system32\drivers\148371d.sys"

The Dropper

Rootkit Installation

- Load Rootkit as a Service

```
CALL DWORD PTR DS:[2C3028] ADVAPI32.Cr
MOV ESI,DWORD PTR DS:[2C302C] ADVAPI32.C1
] = 75EB2120 (ADVAPI32.CreateServiceA)
0032DB40 | hManager = 0032DB40
0012F628 | ServiceName = "148371d"
0012F851 | DisplayName = "syshost.exe"
000F01FF | DesiredAccess = SERVICE_ALL_ACCESS
00000001 | ServiceType = SERVICE_KERNEL_DRIVER
00000001 | StartType = SERVICE_SYSTEM_START
00000000 | ErrorControl = SERVICE_ERROR_IGNORE
0012F728 | BinaryPathName = "C:\windows\system32\drivers\148371d.sys"
00000000 | LoaderOrderGroup = NULL
000
000
000
000
```

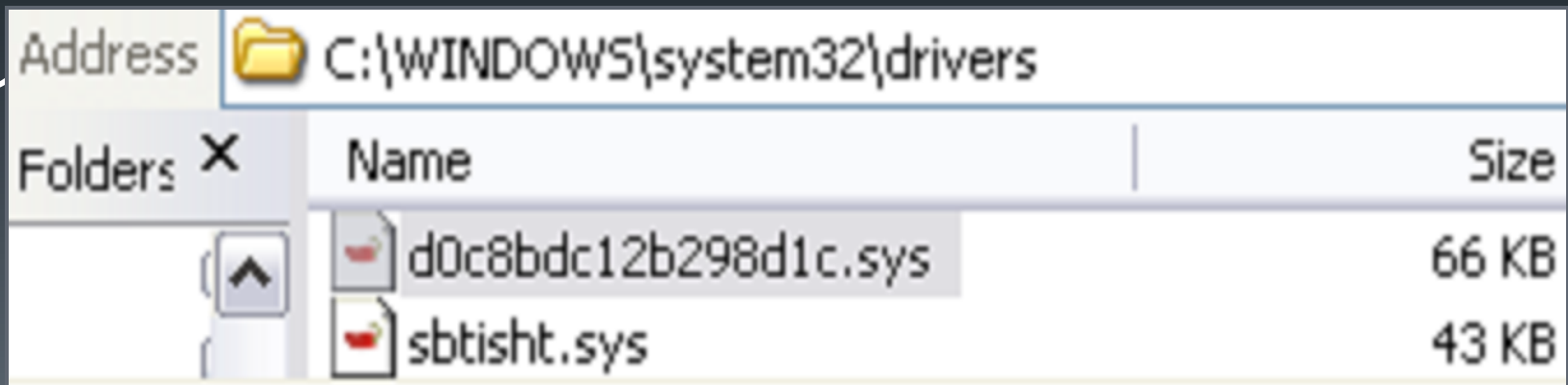
ADVAPI32.CreateServiceA


ServiceName = "148371d"
DisplayName = "syshost.exe"





The Rootkit

The Driver

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



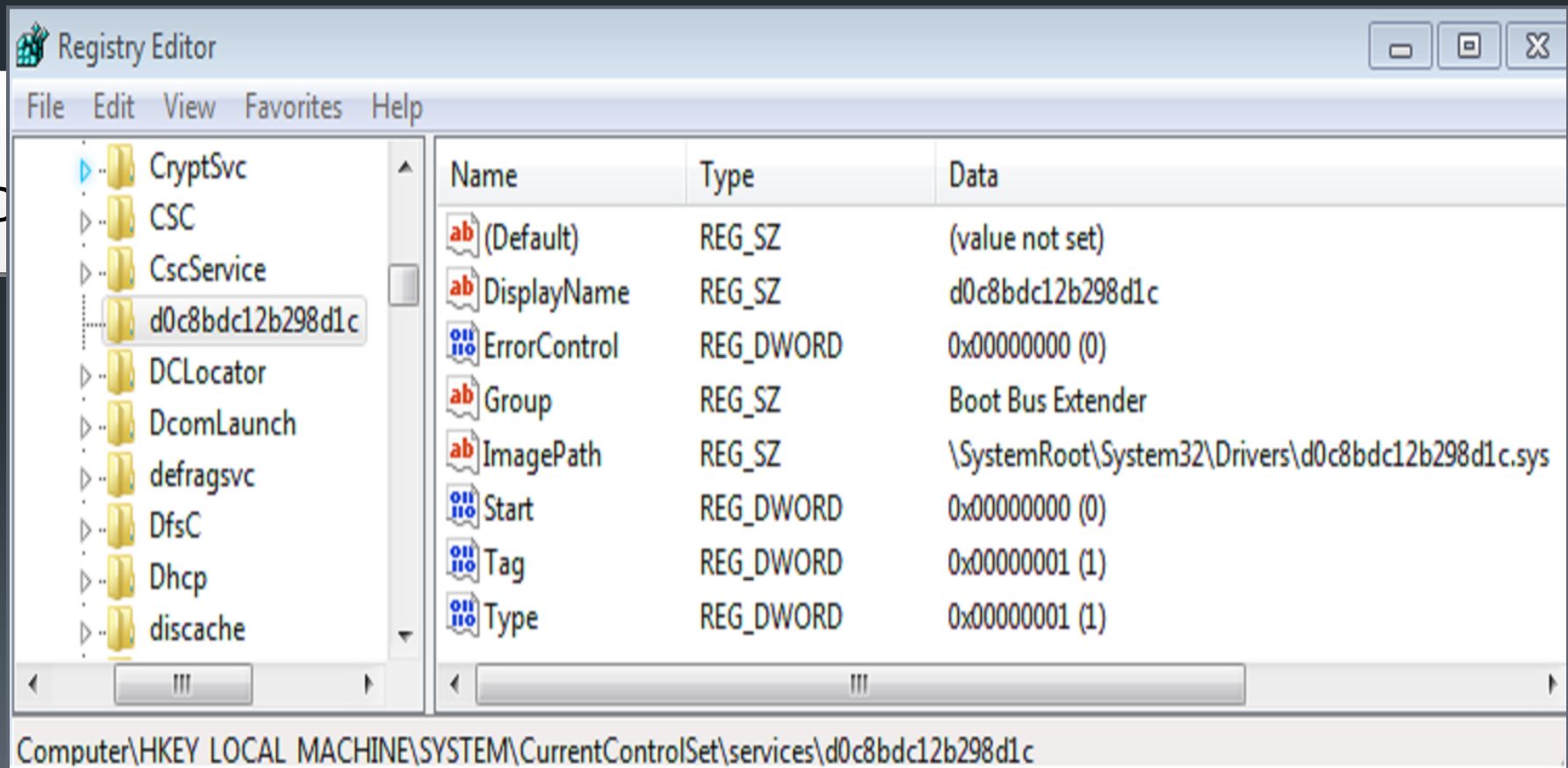
Address  C:\WINDOWS\system32\drivers

Folders 	Name	Size
	 d0c8bdc12b298d1c.sys	66 KB
	 sbtisht.sys	43 KB

The Rootkit

The Driver

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



The screenshot shows the Windows Registry Editor window. The left pane displays a tree view of the registry, with the path `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\d0c8bdc12b298d1c` selected. The right pane shows a list of registry values for this service.

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayName	REG_SZ	d0c8bdc12b298d1c
ErrorControl	REG_DWORD	0x00000000 (0)
Group	REG_SZ	Boot Bus Extender
ImagePath	REG_SZ	\SystemRoot\System32\Drivers\d0c8bdc12b298d1c.sys
Start	REG_DWORD	0x00000000 (0)
Tag	REG_DWORD	0x00000001 (1)
Type	REG_DWORD	0x00000001 (1)


Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\d0c8bdc12b298d1c

The Rootkit

The Driver

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

Load Boot
Device Drivers

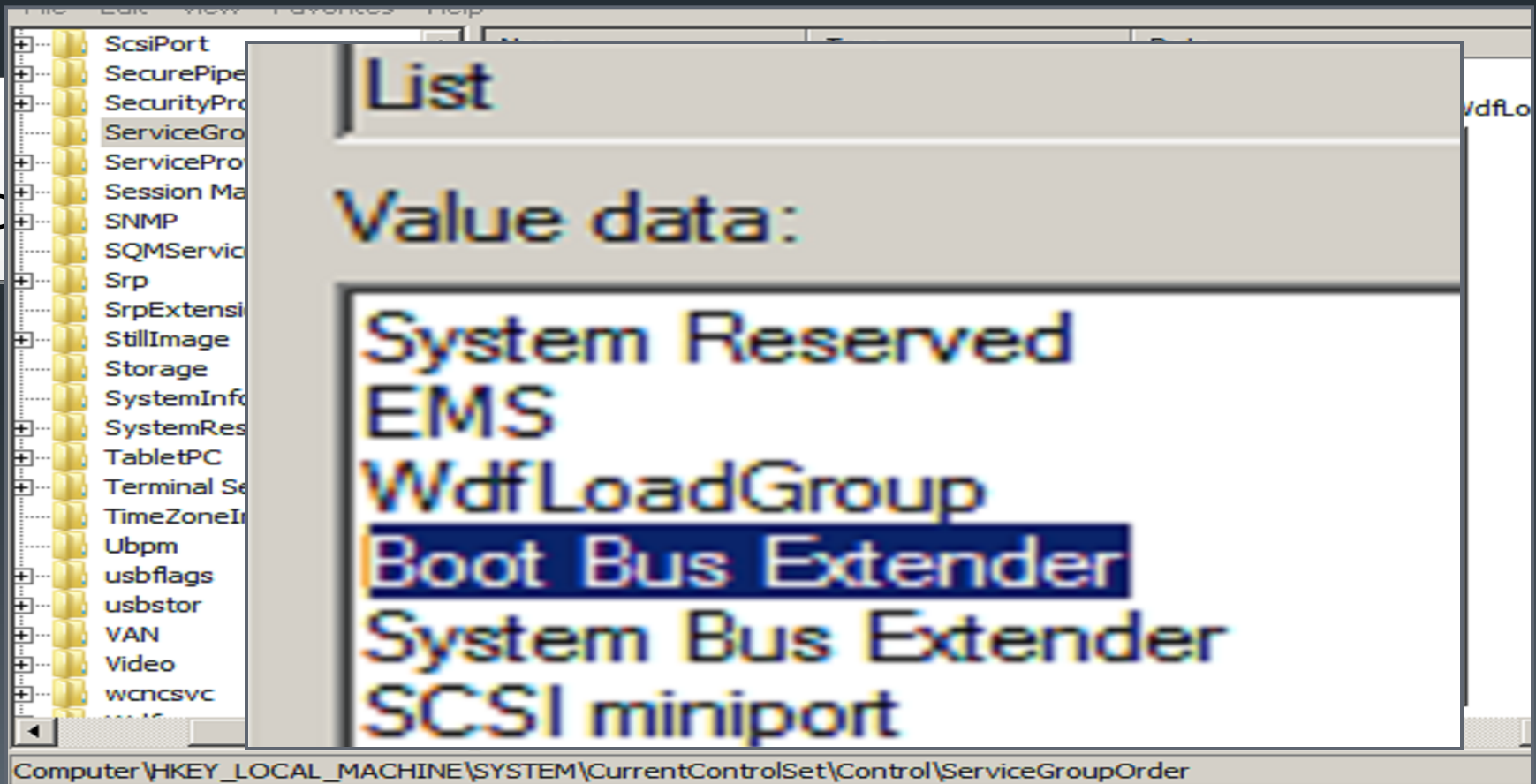
 Start	REG_DWORD	0x00000000 (0)
---	-----------	----------------

SERVICE_BOOT_START

The Rootkit

The Driver

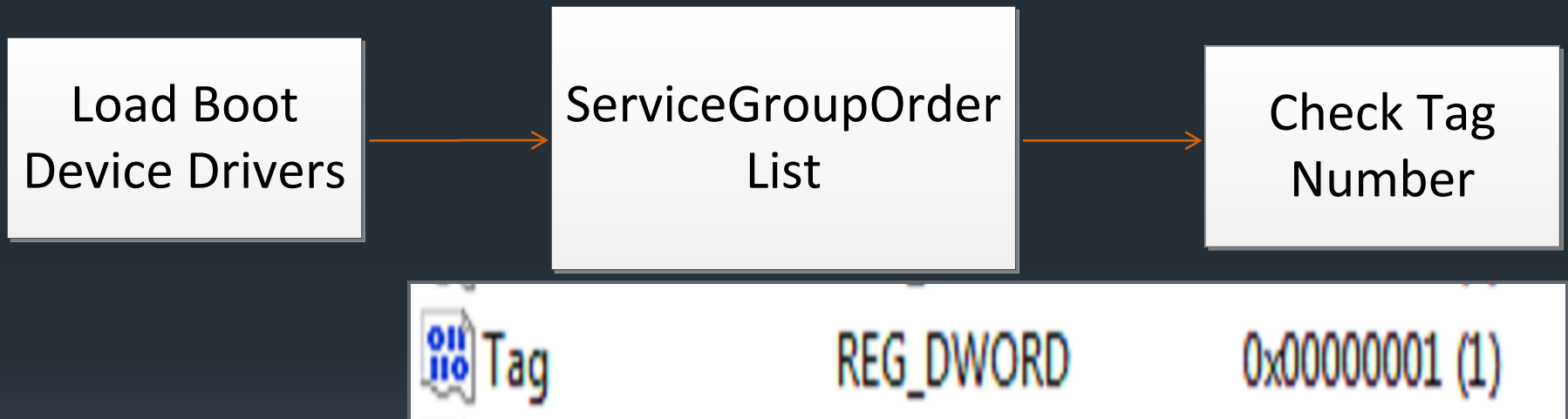
- “\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Control\ServiceGroupOrder”



The Rootkit

The Driver

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



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

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++

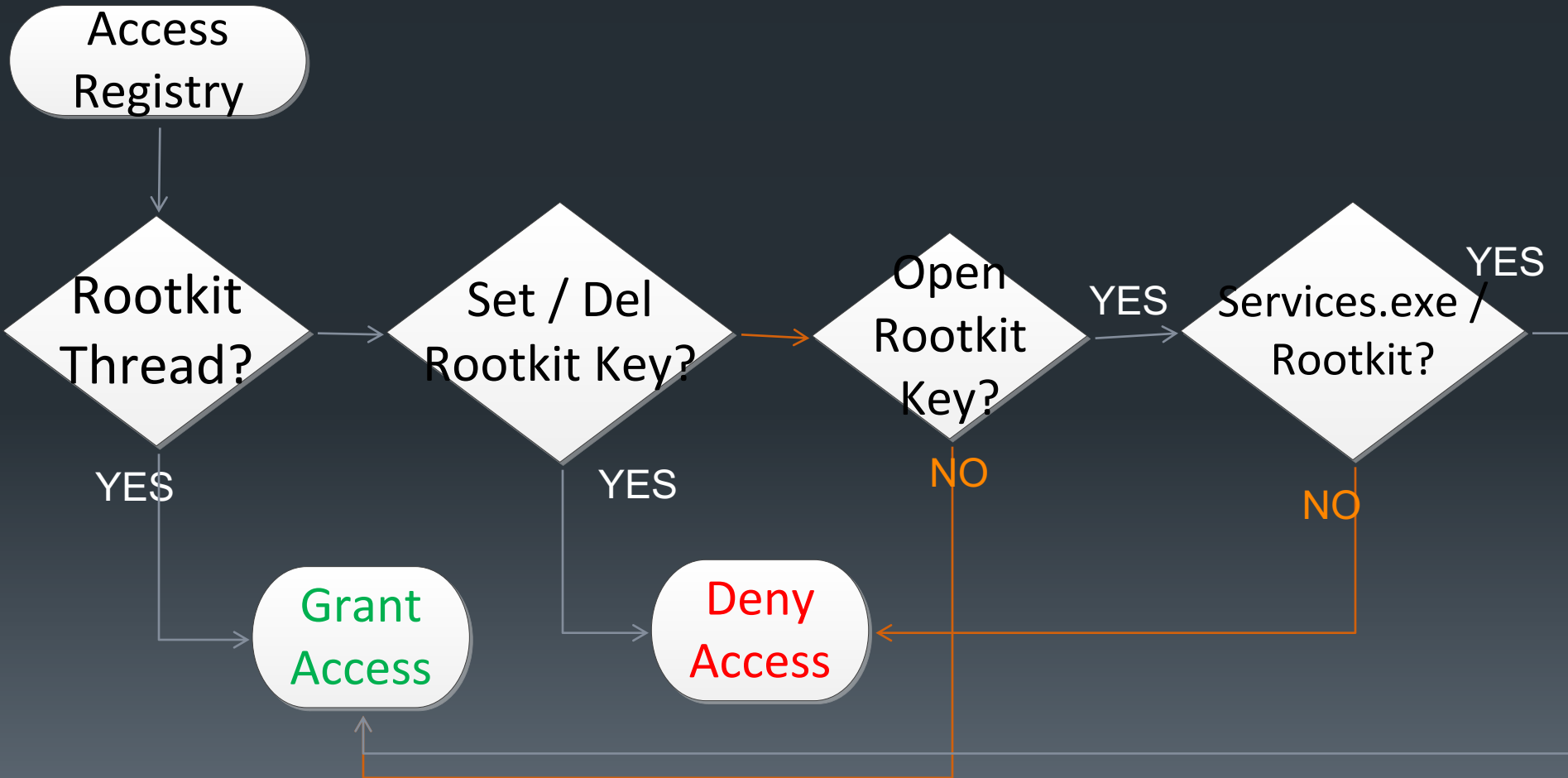
```
EX_CALLBACK_FUNCTION RegistryCallback;
```

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

The Rootkit

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
```

```
ExtensionFlags (00000000)
```

```
Characteristics (00000000)
```

```
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
```

```
ExtensionFlags (00000000)
```

```
Characteristics (00000000)
```

```
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
```

```
push dword 825A53C4
```

```
call off_825A205C
```

```
Stack view
```

```
off_825A205C=[_86b2bd7de1137ef2:off_825A205C]
```

```
F8B1DD68 00000000 off_825A205C dd offset nt_IoAttachDeviceToDeviceStackSafe
```

```
F8B1DD6C 8259DF
```

```
F8B1DD70 00000008 MEMORY:00000008
```

```
F8B1DD74 00000246 MEMORY:00000246
```

```
F8B1DD78 820D2580 MEMORY:820D2580
```

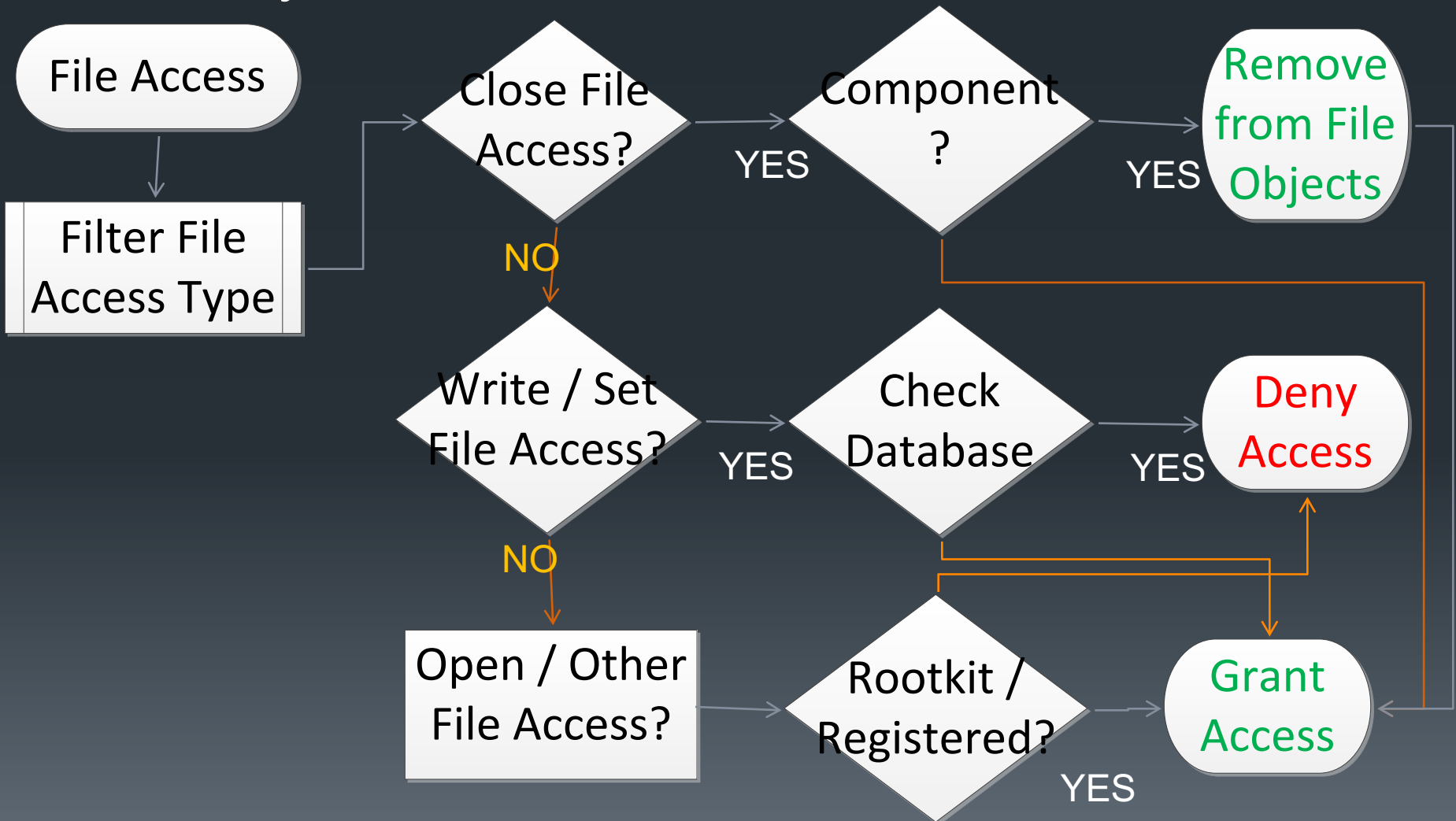
```
F8B1DD7C 82250950 MEMORY:82250950
```

```
F8B1DD80 005A1070 00000000 00000000 00000000 005A1070
```


The Rootkit

Access Denial

- FileSystem Filter Flow



The Rootkit

Access Denial

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

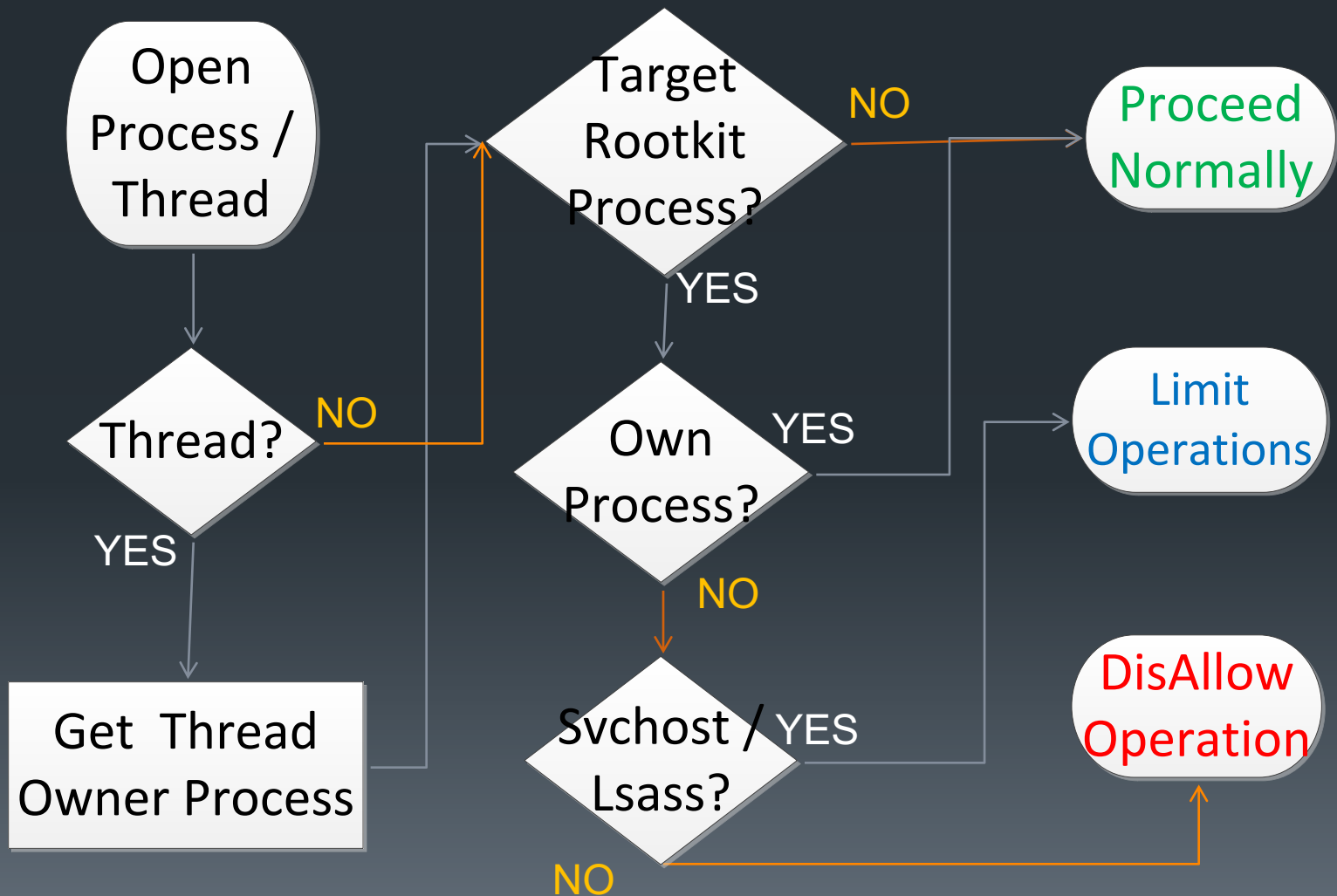
The screenshot displays a debugger interface with several components:

- Assembly View:** Shows assembly instructions. A call instruction `call off_825A2138` is highlighted. Below it, `loc_825A0180:` contains `push edi` and `call off_825A2134`.
- Hex View-EDX:** Shows memory addresses and values. The value `805C15A2` at address `F8BA208C` is highlighted in blue.
- Hex View-ECX:** Shows memory addresses and values. The value `805C1316` at address `8BA2DA4` is highlighted in blue.
- Output window:** Lists the System Service Description Table (SSDT) entries. Two entries are highlighted with red boxes:
 - `80501da4 805c1316 nt!NtOpenProcess [ECX]`
 - `80501dbc 805c15a2 nt!NtOpenThread [EDX]`Arrows point from the highlighted values in the hex views to these entries in the SSDT table.

The Rootkit

Access Denial

- Process / Thread Call Back



The Role

Application

- Blacksnake

 - VM

 - OS

Parse Registry
"ImagePath"



Parse PE file
System32 and
System32\Drivers



Compute File
Name FMV –
1 Hash



Store 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•
```

ITEM\

File list



App

```
mov    [ebp+ms_exc.registration.TryLevel], esi
push   esi                ; Operation
push   esi                ; AccessMode
push   edi                ; MemoryDescriptorList
call   ds:MmProbeAndLockPages
or     [ebp+ms_exc.registration.TryLevel], 0FFFFFFFFh
push   10h               ; Priority
push   esi                ; BugCheckOnFailure
push   esi                ; BaseAddress
push   1                  ; CacheType
push   esi                ; AccessMode
push   edi                ; MemoryDescriptorList
```

0xC0000001
STATUS_UNSUCCESSFUL

{Operation Failed} The requested operation was unsuccessful.

```
mov    dword ptr [eax], 1B8h
mov    dword ptr [eax+4], 8C2C0h
push   edi                ; MemoryDescriptorList
push   eax                ; BaseAddress
call   ds:MmUnmapLockedPages
```

```
0000 add     eax, al
0000 add     [eax], al
0000 add     leax, al
B8010000C0 mov    eax, 0C0000001 ; L
C20800 retn   8 ; ^-^-^-^-^-^-^-^-^-^-
```

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

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/>