NYU Poly Reverse Engineering Lecture

Aaron Portnoy
TippingPoint Security Research

Peter Silberman
Mandiant Engineering and Research

Outline

Agenda

- Software auditing and reverse engineering on Windows
- **SESSION ONE**
  - Auditing methodologies
  - Tools of the trade
  - Disassembling and IDA Pro
- **SESSION TWO**
  - Reversing styles and techniques
  - Vulnerability classes
  - Vulnerability analysis and debugging
  - Automation (if time permits)

Focus on vulnerability discovery and analysis

Introduction to RE

Why is this skill set valuable?

- Source is not often available for Windows applications
- Eliteness factor
  - Often exponentially more difficult than source auditing
  - Find bugs where few others are comfortable
- Homebrew patches
- Patch analysis
  - e.g. Reversing Microsoft patches to discover root cause
  - 1st with a new exploit or Metasploit module?
  - 1st with a new signature for an AV or IPS?

<u>Binary code is a $ goldmine $</u>

- Bugs exist for long periods of time in binary code

Introduction to RE (cont.)

Why is this skill set valuable (cont.)?

- Knowledge is portable
  - Apply techniques to wide array of tasks
  - New architectures become approachable
- Developing countries rely on it
  - Why engineer from scratch when you can copy
  - Reverse for security, ensure there are no backdoors
  - In the US we take these things for granted

Introduction to RE (cont.)

It's not always about the assembly

Reversing is the process by which you attempt to understand the system

- Operating system
- Software
- Hardware
- Plane, train, auto, anything that was engineered

Reverse the *system* as a whole, helps locate trust boundaries

Malkovich malkovich, malkovich?

GOAL: Get inside the developer's head

Reverse engineer intentional behavior to determine how to deviate execution from that intention

Overview of Approach

General Steps, pre-disassembling

- Examine system behavior
- Enumerate components
- Determine relationships
- Determine trust
- Locate and probe inputs

Many tools to aid in this process

We'll cover some of these

Step by step

Examining system behavior

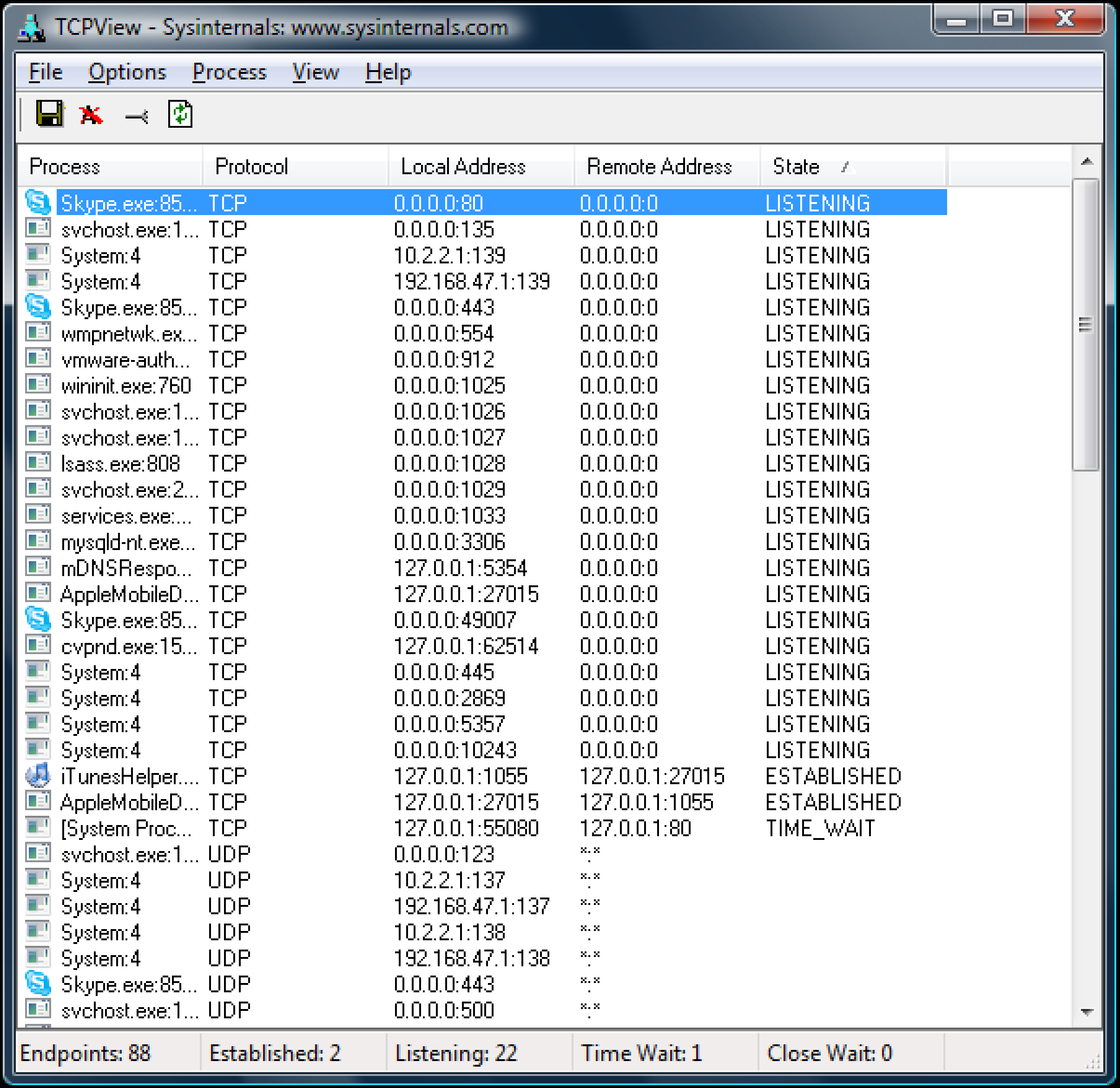
- <u>Documentation</u>
- Install & use the product!
- Support forums
  - Exploitable bugs might be “annoyances” to regular users

Step by step (cont.)

Enumerating components

- Documentation
  - Product prerequisites (Java, .NET, …)
- MSRPC
  - Process Explorer
  - rpcdump, rpcinfo
  - mIDA
- ActiveX, Codecs, File formats, Protocol Handlers, …
  - RegMon
  - FileMon
  - ProcessMon
- Services
  - services.msc / TCPView

TCP View from MS

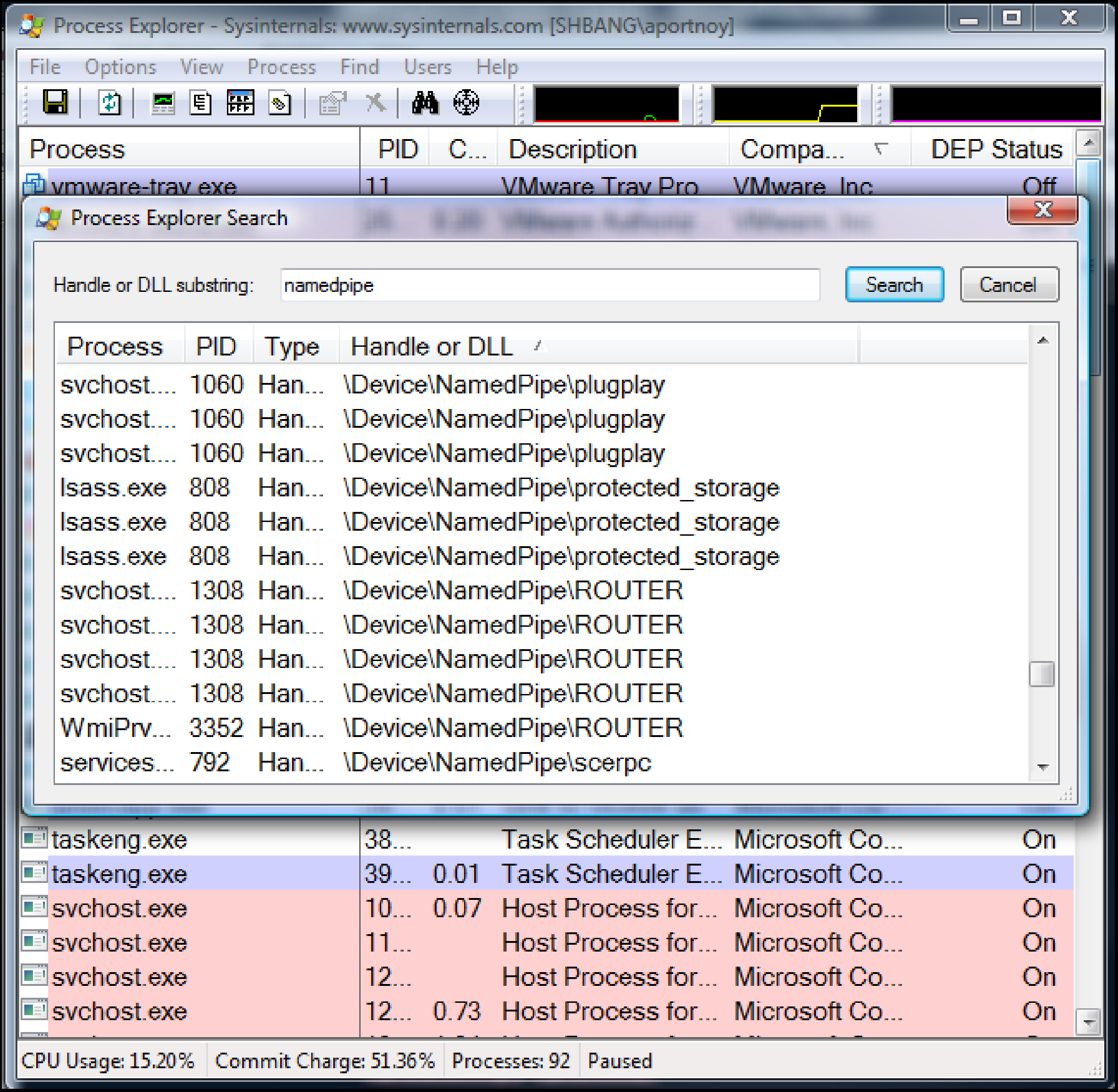


TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help

Process	Protocol	Local Address	Remote Address	State
Skype.exe:85...	TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
svchost.exe:1...	TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
System:4	TCP	10.2.2.1:139	0.0.0.0:0	LISTENING
System:4	TCP	192.168.47.1:139	0.0.0.0:0	LISTENING
Skype.exe:85...	TCP	0.0.0.0:443	0.0.0.0:0	LISTENING
wmpnetwk.ex...	TCP	0.0.0.0:554	0.0.0.0:0	LISTENING
vmware-auth...	TCP	0.0.0.0:912	0.0.0.0:0	LISTENING
wininit.exe:760	TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
svchost.exe:1...	TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING
svchost.exe:1...	TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING
lsass.exe:808	TCP	0.0.0.0:1028	0.0.0.0:0	LISTENING
svchost.exe:2...	TCP	0.0.0.0:1029	0.0.0.0:0	LISTENING
services.exe:...	TCP	0.0.0.0:1033	0.0.0.0:0	LISTENING
mysqld-nt.exe...	TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
mDNSRespo...	TCP	127.0.0.1:5354	0.0.0.0:0	LISTENING
AppleMobileD...	TCP	127.0.0.1:27015	0.0.0.0:0	LISTENING
Skype.exe:85...	TCP	0.0.0.0:49007	0.0.0.0:0	LISTENING
cvpnd.exe:15...	TCP	127.0.0.1:62514	0.0.0.0:0	LISTENING
System:4	TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
System:4	TCP	0.0.0.0:2869	0.0.0.0:0	LISTENING
System:4	TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING
System:4	TCP	0.0.0.0:10243	0.0.0.0:0	LISTENING
iTunesHelper....	TCP	127.0.0.1:1055	127.0.0.1:27015	ESTABLISHED
AppleMobileD...	TCP	127.0.0.1:27015	127.0.0.1:1055	ESTABLISHED
[System Proc...	TCP	127.0.0.1:55080	127.0.0.1:80	TIME_WAIT
svchost.exe:1...	UDP	0.0.0.0:123	*:*	
System:4	UDP	10.2.2.1:137	*:*	
System:4	UDP	192.168.47.1:137	*:*	
System:4	UDP	10.2.2.1:138	*:*	
System:4	UDP	192.168.47.1:138	*:*	
Skype.exe:85...	UDP	0.0.0.0:443	*:*	
svchost.exe:1...	UDP	0.0.0.0:500	*:*	

Endpoints: 88 Established: 2 Listening: 22 Time Wait: 1 Close Wait: 0

Process Explorer from MS

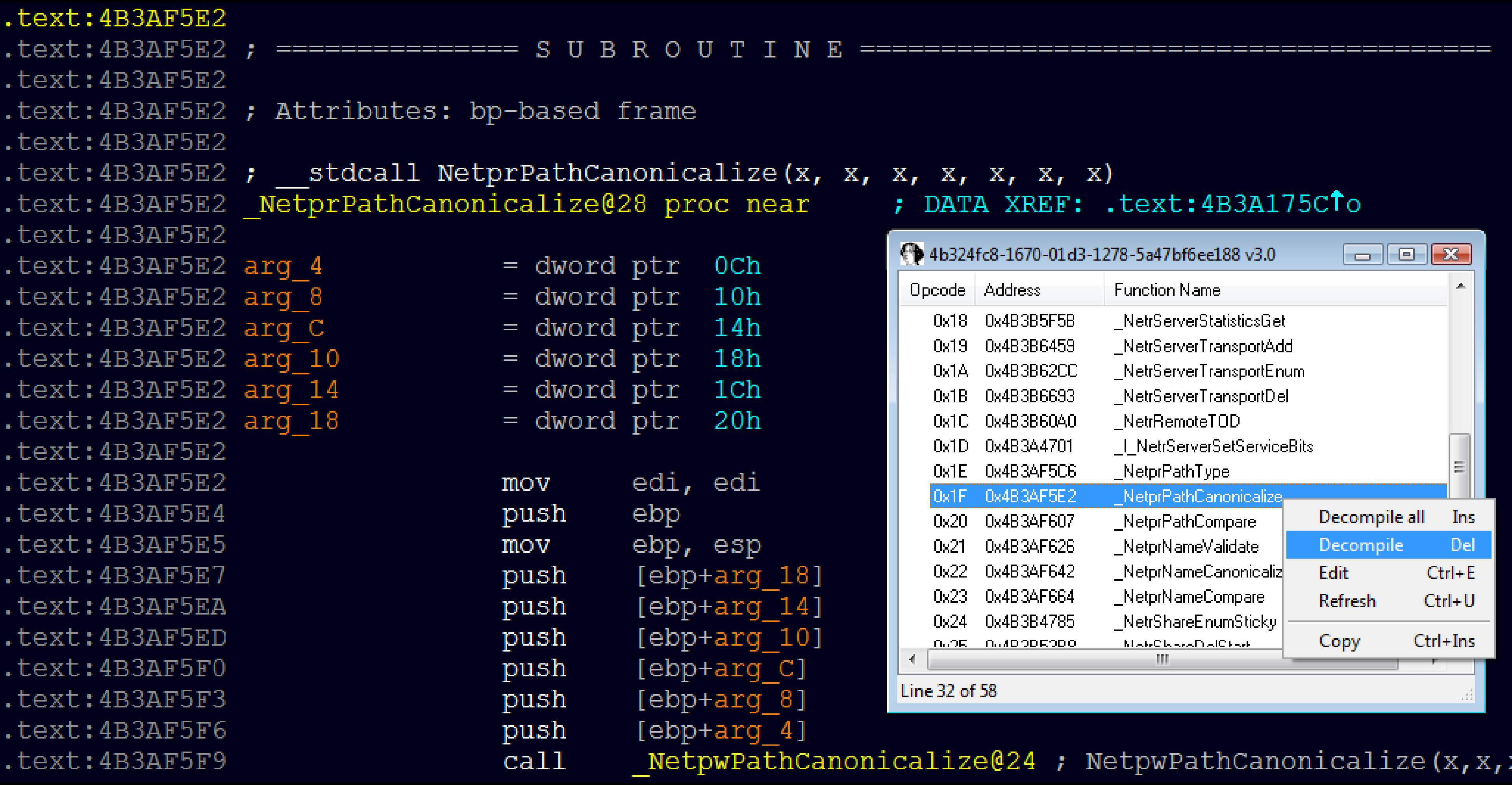

Process Explorer - Sysinternals: www.sysinternals.com [SHBANG\aportnoy]
File Options View Process Find Users Help
Process Explorer Search
Handle or DLL substring: namedpipe
Search
Cancel

Process	PID	Type	Handle or DLL
svchost....	1060	Han...	\Device\NamedPipe\plugplay
svchost....	1060	Han...	\Device\NamedPipe\plugplay
svchost....	1060	Han...	\Device\NamedPipe\plugplay
lsass.exe	808	Han...	\Device\NamedPipe\protected_storage
lsass.exe	808	Han...	\Device\NamedPipe\protected_storage
lsass.exe	808	Han...	\Device\NamedPipe\protected_storage
svchost....	1308	Han...	\Device\NamedPipe\ROUTER
svchost....	1308	Han...	\Device\NamedPipe\ROUTER
svchost....	1308	Han...	\Device\NamedPipe\ROUTER
svchost....	1308	Han...	\Device\NamedPipe\ROUTER
WmiPrv...	3352	Han...	\Device\NamedPipe\ROUTER
services...	792	Han...	\Device\NamedPipe\scerpc

Process	PID	C...	Description	Compa...	DEP Status
vmware-tray.exe	11		VMware Tray Pro	VMware, Inc	Off
taskeng.exe	38...		Task Scheduler E...	Microsoft Co...	On
taskeng.exe	39...	0.01	Task Scheduler E...	Microsoft Co...	On
svchost.exe	10...	0.07	Host Process for...	Microsoft Co...	On
svchost.exe	11...		Host Process for...	Microsoft Co...	On
svchost.exe	12...		Host Process for...	Microsoft Co...	On
svchost.exe	12...	0.73	Host Process for...	Microsoft Co...	On

CPU Usage: 15.20% | Commit Charge: 51.36% | Processes: 92 | Paused

mIDA from Tenable (MSRPC)

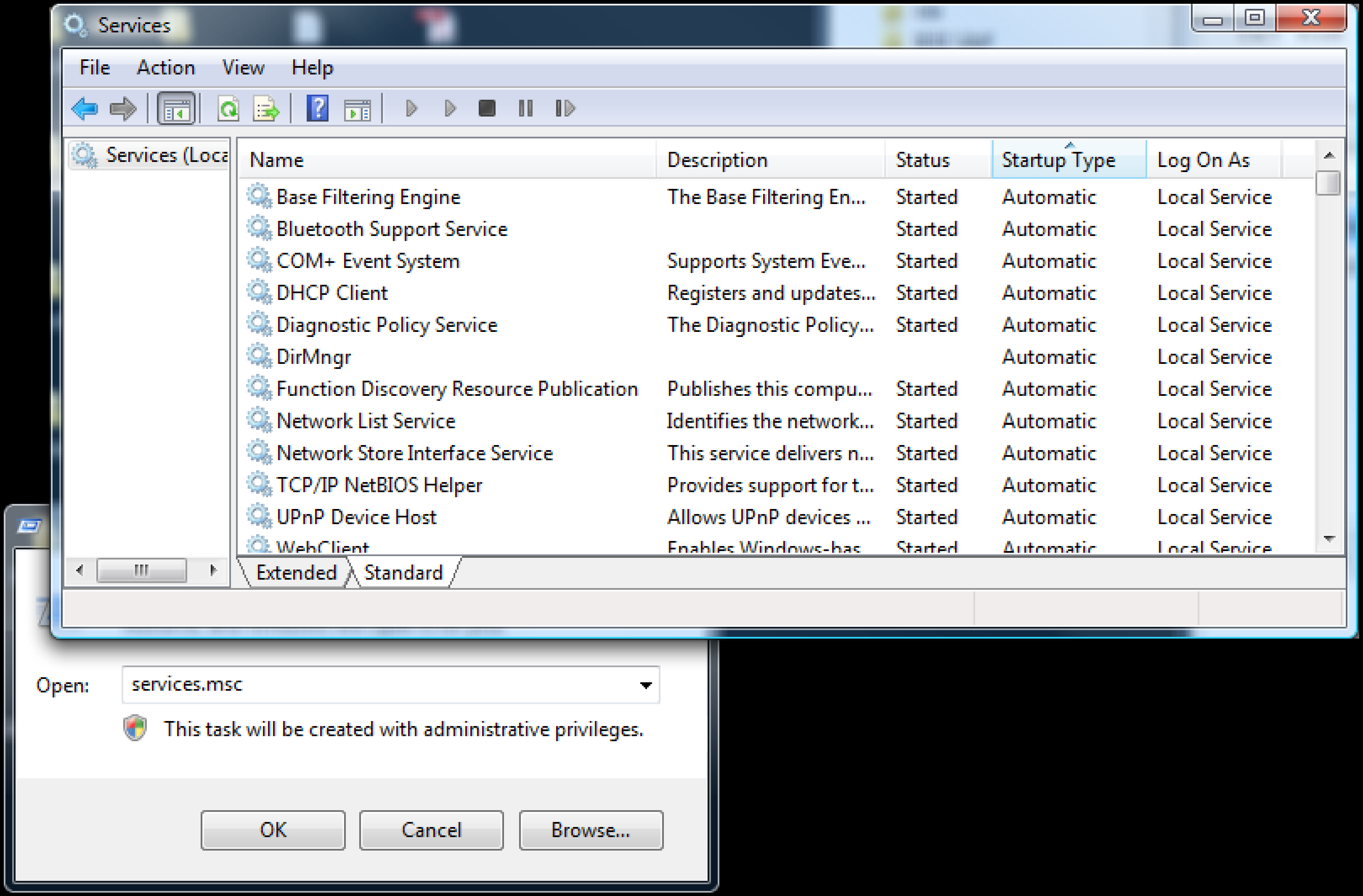


```
.text:4B3AF5E2
.text:4B3AF5E2 ; =============== S U B R O U T I N E =======================================
.text:4B3AF5E2
.text:4B3AF5E2 ; Attributes: bp-based frame
.text:4B3AF5E2
.text:4B3AF5E2 ; __stdcall NetprPathCanonicalize(x, x, x, x, x, x, x)
.text:4B3AF5E2 _NetprPathCanonicalize@28 proc near     ; DATA XREF: .text:4B3A175C↑o
.text:4B3AF5E2
.text:4B3AF5E2 arg_4           = dword ptr  0Ch
.text:4B3AF5E2 arg_8           = dword ptr  10h
.text:4B3AF5E2 arg_C           = dword ptr  14h
.text:4B3AF5E2 arg_10          = dword ptr  18h
.text:4B3AF5E2 arg_14          = dword ptr  1Ch
.text:4B3AF5E2 arg_18          = dword ptr  20h
.text:4B3AF5E2
.text:4B3AF5E2                 mov     edi, edi
.text:4B3AF5E4                 push    ebp
.text:4B3AF5E5                 mov     ebp, esp
.text:4B3AF5E7                 push    [ebp+arg_18]
.text:4B3AF5EA                 push    [ebp+arg_14]
.text:4B3AF5ED                 push    [ebp+arg_10]
.text:4B3AF5F0                 push    [ebp+arg_C]
.text:4B3AF5F3                 push    [ebp+arg_8]
.text:4B3AF5F6                 push    [ebp+arg_4]
.text:4B3AF5F9                 call    _NetpwPathCanonicalize@24 ; NetpwPathCanonicalize(x,x,
```

4b324fc8-1670-01d3-1278-5a47bf6ee188 v3.0

Opcode	Address	Function Name
0x18	0x4B3B5F5B	_NetrServerStatisticsGet
0x19	0x4B3B6459	_NetrServerTransportAdd
0x1A	0x4B3B62CC	_NetrServerTransportEnum
0x1B	0x4B3B6693	_NetrServerTransportDel
0x1C	0x4B3B60A0	_NetrRemoteTOD
0x1D	0x4B3A4701	_I_NetrServerSetServiceBits
0x1E	0x4B3AF5C6	_NetprPathType
0x1F	0x4B3AF5E2	_NetprPathCanonicalize
0x20	0x4B3AF607	_NetprPathCompare
0x21	0x4B3AF626	_NetprNameValidate
0x22	0x4B3AF642	_NetprNameCanonicaliz
0x23	0x4B3AF664	_NetprNameCompare
0x24	0x4B3B4785	_NetrShareEnumSticky

Services

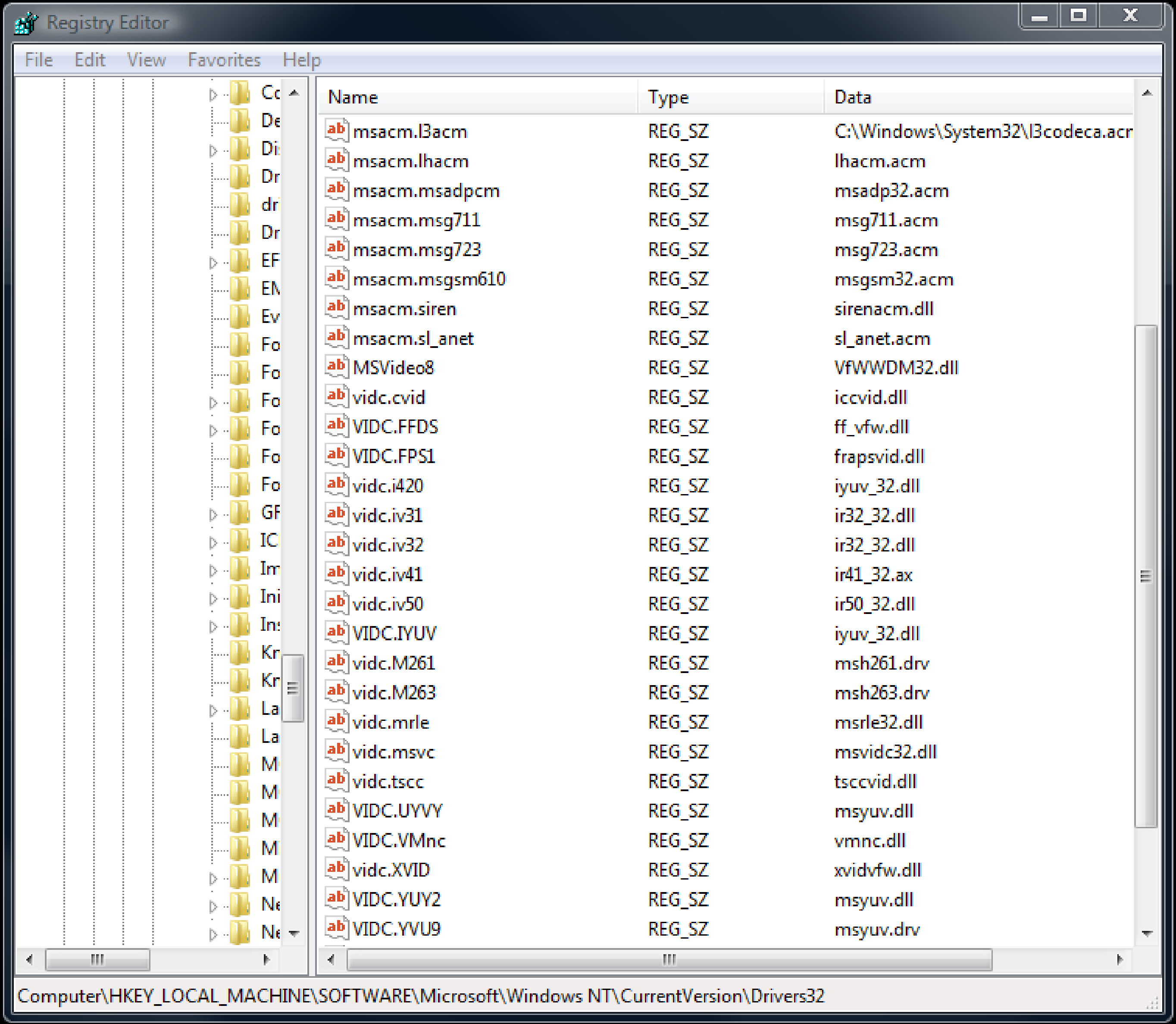


Name	Description	Status	Startup Type	Log On As
Base Filtering Engine	The Base Filtering En...	Started	Automatic	Local Service
Bluetooth Support Service		Started	Automatic	Local Service
COM+ Event System	Supports System Eve...	Started	Automatic	Local Service
DHCP Client	Registers and updates...	Started	Automatic	Local Service
Diagnostic Policy Service	The Diagnostic Policy...	Started	Automatic	Local Service
DirMngr			Automatic	Local Service
Function Discovery Resource Publication	Publishes this compu...	Started	Automatic	Local Service
Network List Service	Identifies the network...	Started	Automatic	Local Service
Network Store Interface Service	This service delivers n...	Started	Automatic	Local Service
TCP/IP NetBIOS Helper	Provides support for t...	Started	Automatic	Local Service
UPnP Device Host	Allows UPnP devices ...	Started	Automatic	Local Service
WebClient	Enables Windows-bas	Started	Automatic	Local Service

Open: services.msc

This task will be created with administrative privileges.

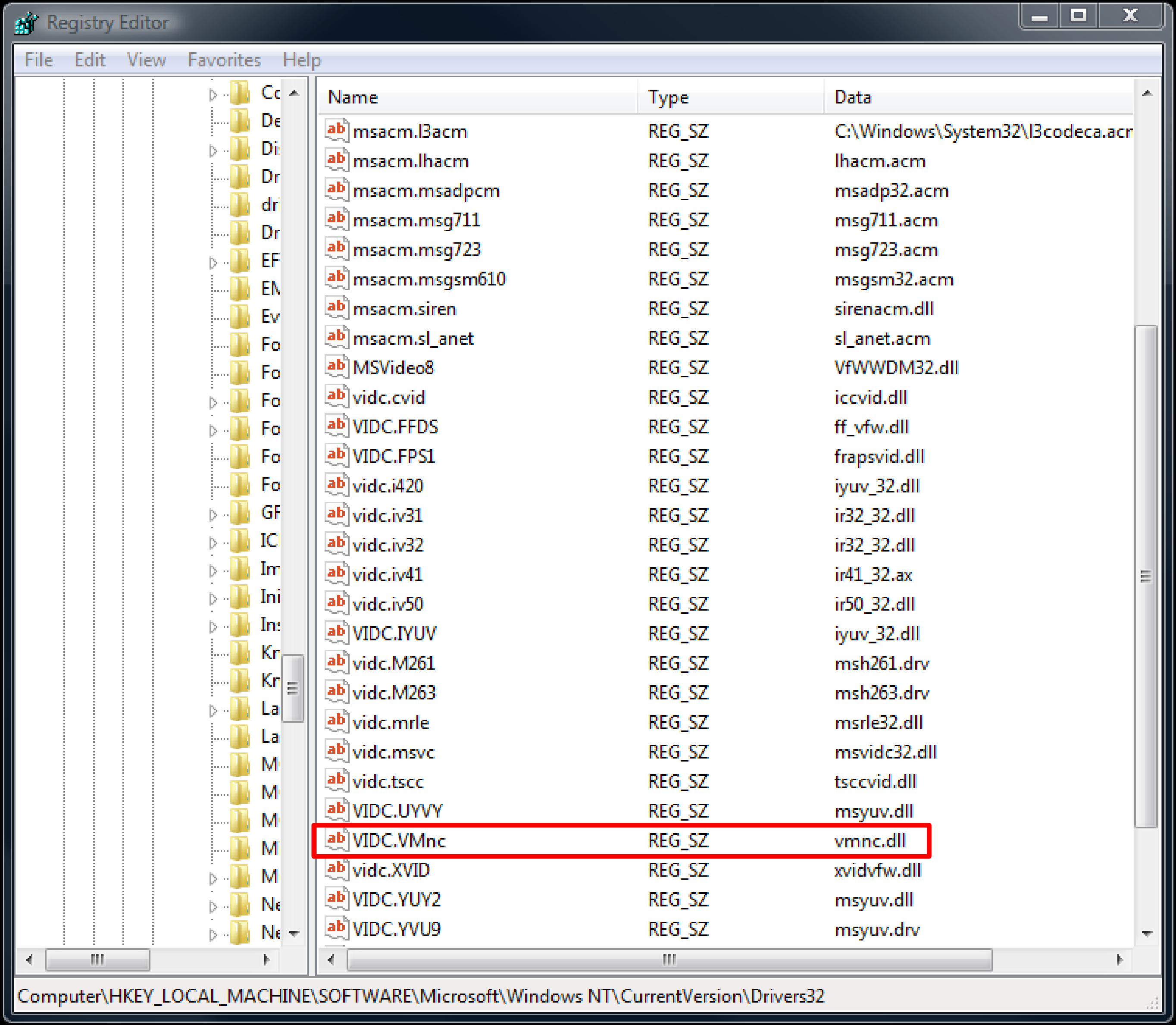
Registered Codecs



Name	Type	Data
msacm.l3acm	REG_SZ	C:\Windows\System32\l3codeca.acr
msacm.lhacm	REG_SZ	lhacm.acm
msacm.msadpcm	REG_SZ	msadp32.acm
msacm.msg711	REG_SZ	msg711.acm
msacm.msg723	REG_SZ	msg723.acm
msacm.msgsm610	REG_SZ	msgsm32.acm
msacm.siren	REG_SZ	sirenacm.dll
msacm.sl_anet	REG_SZ	sl_anet.acm
MSVideo8	REG_SZ	VfWWDM32.dll
vidc.cvid	REG_SZ	iccvid.dll
VIDC.FFDS	REG_SZ	ff_vfw.dll
VIDC.FPS1	REG_SZ	frapsvid.dll
vidc.i420	REG_SZ	iyuv_32.dll
vidc.iv31	REG_SZ	ir32_32.dll
vidc.iv32	REG_SZ	ir32_32.dll
vidc.iv41	REG_SZ	ir41_32.ax
vidc.iv50	REG_SZ	ir50_32.dll
VIDC.IYUV	REG_SZ	iyuv_32.dll
vidc.M261	REG_SZ	msh261.drv
vidc.M263	REG_SZ	msh263.drv
vidc.mrle	REG_SZ	msrle32.dll
vidc.msvc	REG_SZ	msvidc32.dll
vidc.tscc	REG_SZ	tsccvid.dll
VIDC.UYVY	REG_SZ	msyuv.dll
VIDC.VMnc	REG_SZ	vmnc.dll
vidc.XVID	REG_SZ	xvidvfw.dll
VIDC.YUY2	REG_SZ	msyuv.dll
VIDC.YVU9	REG_SZ	msyuv.drv

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32

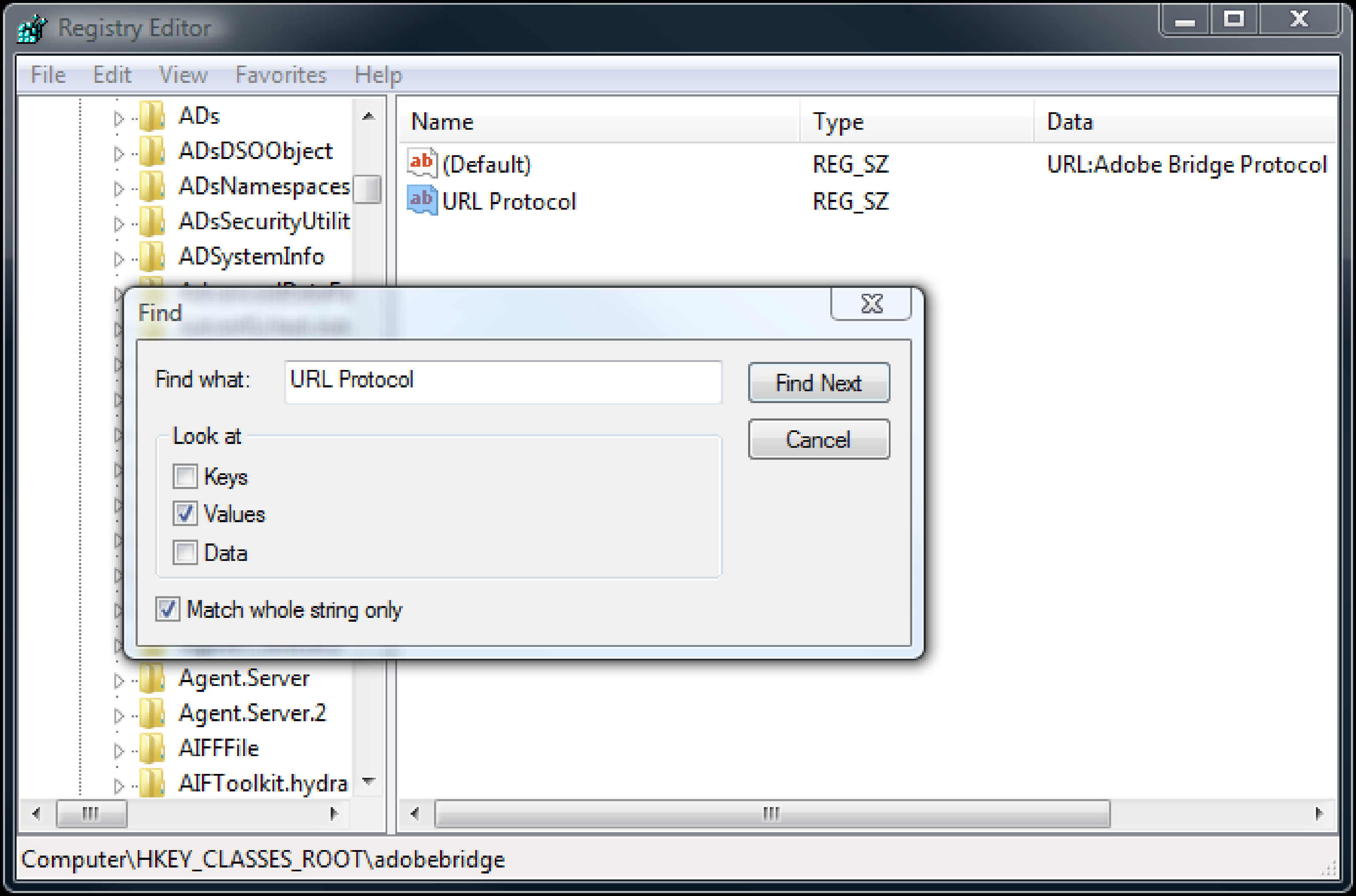
Registered Codecs



Name	Type	Data
msacm.l3acm	REG_SZ	C:\Windows\System32\l3codeca.acm
msacm.lhacm	REG_SZ	lhacm.acm
msacm.msadpcm	REG_SZ	msadp32.acm
msacm.msg711	REG_SZ	msg711.acm
msacm.msg723	REG_SZ	msg723.acm
msacm.msgsm610	REG_SZ	msgsm32.acm
msacm.siren	REG_SZ	sirenacm.dll
msacm.sl_anet	REG_SZ	sl_anet.acm
MSVideo8	REG_SZ	VfWWDM32.dll
vidc.cvid	REG_SZ	iccvid.dll
VIDC.FFDS	REG_SZ	ff_vfw.dll
VIDC.FPS1	REG_SZ	frapsvid.dll
vidc.i420	REG_SZ	iyuv_32.dll
vidc.iv31	REG_SZ	ir32_32.dll
vidc.iv32	REG_SZ	ir32_32.dll
vidc.iv41	REG_SZ	ir41_32.ax
vidc.iv50	REG_SZ	ir50_32.dll
VIDC.IYUV	REG_SZ	iyuv_32.dll
vidc.M261	REG_SZ	msh261.drv
vidc.M263	REG_SZ	msh263.drv
vidc.mrle	REG_SZ	msrle32.dll
vidc.msvc	REG_SZ	msvidc32.dll
vidc.tscc	REG_SZ	tsccvid.dll
VIDC.UYVY	REG_SZ	msyuv.dll
VIDC.VMnc	REG_SZ	vmnc.dll
vidc.XVID	REG_SZ	xvidvfw.dll
VIDC.YUY2	REG_SZ	msyuv.dll
VIDC.YVU9	REG_SZ	msyuv.drv

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32

Registered Protocol Handlers



Name	Type	Data
(Default)	REG_SZ	URL:Adobe Bridge Protocol
URL Protocol	REG_SZ	

Find

Find what: URL Protocol

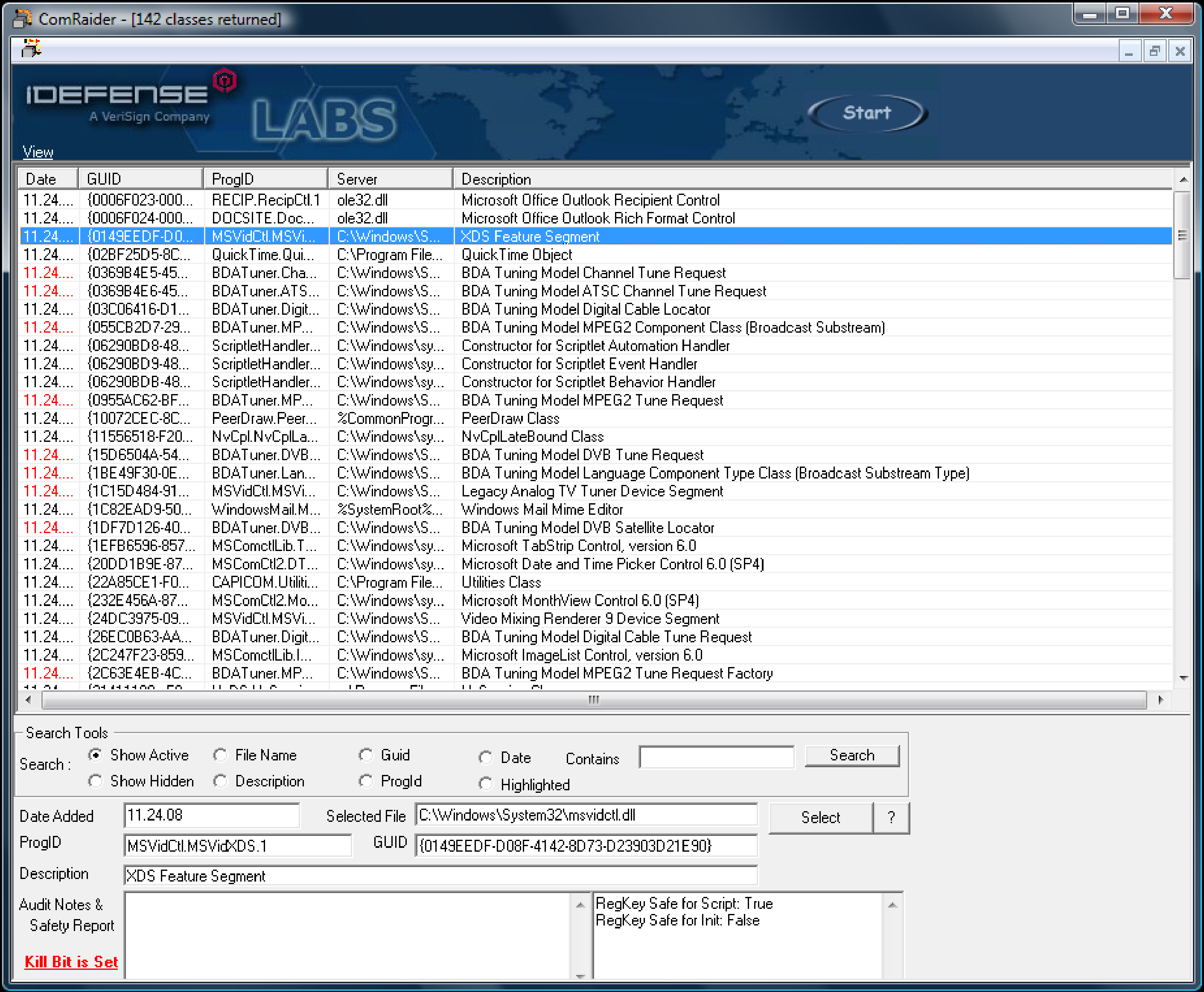
Look at

- [ ] Keys
- [x] Values
- [ ] Data

- [x] Match whole string only

Computer\HKEY_CLASSES_ROOT\adobebridge

ActiveX Controls


ComRaider - [142 classes returned]

Date	GUID	ProgID	Server	Description
11.24....	{0006F023-000...	RECIP.RecipCtl.1	ole32.dll	Microsoft Office Outlook Recipient Control
11.24....	{0006F024-000...	DOCSITE.Doc...	ole32.dll	Microsoft Office Outlook Rich Format Control
11.24....	{0149EEDF-D0...	MSVidCtl.MSVi...	C:\Windows\S...	XDS Feature Segment
11.24....	{02BF25D5-8C...	QuickTime.Qui...	C:\Program File...	QuickTime Object
11.24....	{0369B4E5-45...	BDATuner.Cha...	C:\Windows\S...	BDA Tuning Model Channel Tune Request
11.24....	{0369B4E6-45...	BDATuner.ATS...	C:\Windows\S...	BDA Tuning Model ATSC Channel Tune Request
11.24....	{03C06416-D1...	BDATuner.Digit...	C:\Windows\S...	BDA Tuning Model Digital Cable Locator
11.24....	{055CB2D7-29...	BDATuner.MP...	C:\Windows\S...	BDA Tuning Model MPEG2 Component Class (Broadcast Substream)
11.24....	{06290BD8-48...	ScriptletHandler...	C:\Windows\sy...	Constructor for Scriptlet Automation Handler
11.24....	{06290BD9-48...	ScriptletHandler...	C:\Windows\sy...	Constructor for Scriptlet Event Handler
11.24....	{06290BDB-48...	ScriptletHandler...	C:\Windows\sy...	Constructor for Scriptlet Behavior Handler
11.24....	{0955AC62-BF...	BDATuner.MP...	C:\Windows\S...	BDA Tuning Model MPEG2 Tune Request
11.24....	{10072CEC-8C...	PeerDraw.Peer...	%CommonProgr...	PeerDraw Class
11.24....	{11556518-F20...	NvCpl.NvCplLa...	C:\Windows\sy...	NvCplLateBound Class
11.24....	{15D6504A-54...	BDATuner.DVB...	C:\Windows\S...	BDA Tuning Model DVB Tune Request
11.24....	{1BE49F30-0E...	BDATuner.Lan...	C:\Windows\S...	BDA Tuning Model Language Component Type Class (Broadcast Substream Type)
11.24....	{1C15D484-91...	MSVidCtl.MSVi...	C:\Windows\S...	Legacy Analog TV Tuner Device Segment
11.24....	{1C82EAD9-50...	WindowsMail.M...	%SystemRoot%...	Windows Mail Mime Editor
11.24....	{1DF7D126-40...	BDATuner.DVB...	C:\Windows\S...	BDA Tuning Model DVB Satellite Locator
11.24....	{1EFB6596-857...	MSComctlLib.T...	C:\Windows\sy...	Microsoft TabStrip Control, version 6.0
11.24....	{20DD1B9E-87...	MSComCtl2.DT...	C:\Windows\sy...	Microsoft Date and Time Picker Control 6.0 (SP4)
11.24....	{22A85CE1-F0...	CAPICOM.Utiliti...	C:\Program File...	Utilities Class
11.24....	{232E456A-87...	MSComCtl2.Mo...	C:\Windows\sy...	Microsoft MonthView Control 6.0 (SP4)
11.24....	{24DC3975-09...	MSVidCtl.MSVi...	C:\Windows\S...	Video Mixing Renderer 9 Device Segment
11.24....	{26EC0B63-AA...	BDATuner.Digit...	C:\Windows\S...	BDA Tuning Model Digital Cable Tune Request
11.24....	{2C247F23-859...	MSComctlLib.I...	C:\Windows\sy...	Microsoft ImageList Control, version 6.0
11.24....	{2C63E4EB-4C...	BDATuner.MP...	C:\Windows\S...	BDA Tuning Model MPEG2 Tune Request Factory

Search Tools

Search : [✓ Show Active] Show Hidden File Name Description Guid ProgId Date Highlighted Contains Search

Date Added	11.24.08	Selected File	C:\Windows\System32\msvidctl.dll	Select	?
ProgID	MSVidCtl.MSVidXDS.1	GUID	{0149EEDF-D08F-4142-8D73-D23903D21E90}		
Description	XDS Feature Segment				

Audit Notes & Safety Report

RegKey Safe for Script: True
RegKey Safe for Init: False

Kill Bit is Set

Step by step (cont.)

Determining relationships

- <u>Documentation</u>

- Loaded modules
  - Do different processes share 3rd party DLL files?

- Local ports, Named pipes
  - IPC
  - Check shared handles

- Wireshark
  - Use the product, sniff

Step by step (cont.)

Determining trust

<u>Documentation</u>

- Ethernet interfaces bound
  - Local? Remote? TCP? UDP? …
- Named pipe restrictions
  - Authentication
- ActiveX
  - Safe for scripting
  - Safe for init
- Privileges of users running processes
- Permissions on resources, directories, handles, …

Step by step (cont.)

Locating inputs

- Documentation
- Registry entries
  - File formats, codecs, protocol handlers
- TCP View /Process Explorer

Probing inputs

- Create your own "clients"
  - MSRPC
    - Impacket (Core), PyMSRPC (Myself and Cody Pierce)
  - ActiveX
    - COMRaider (David Zimmer), Axman (HD Moore)
  - TCP/UDP/…
    - Socket code (py, pl, C, take your pick)
- Subverting client code
  - Don't bother implementing an encryption if you can steal theirs

Questions?

Disassembling and IDA Pro

Intro to binary code structure

Modules

process.exe, library.dll

Functions

At least one basic block, can be called

Basic Blocks

Groups of instructions terminated at a branch or return

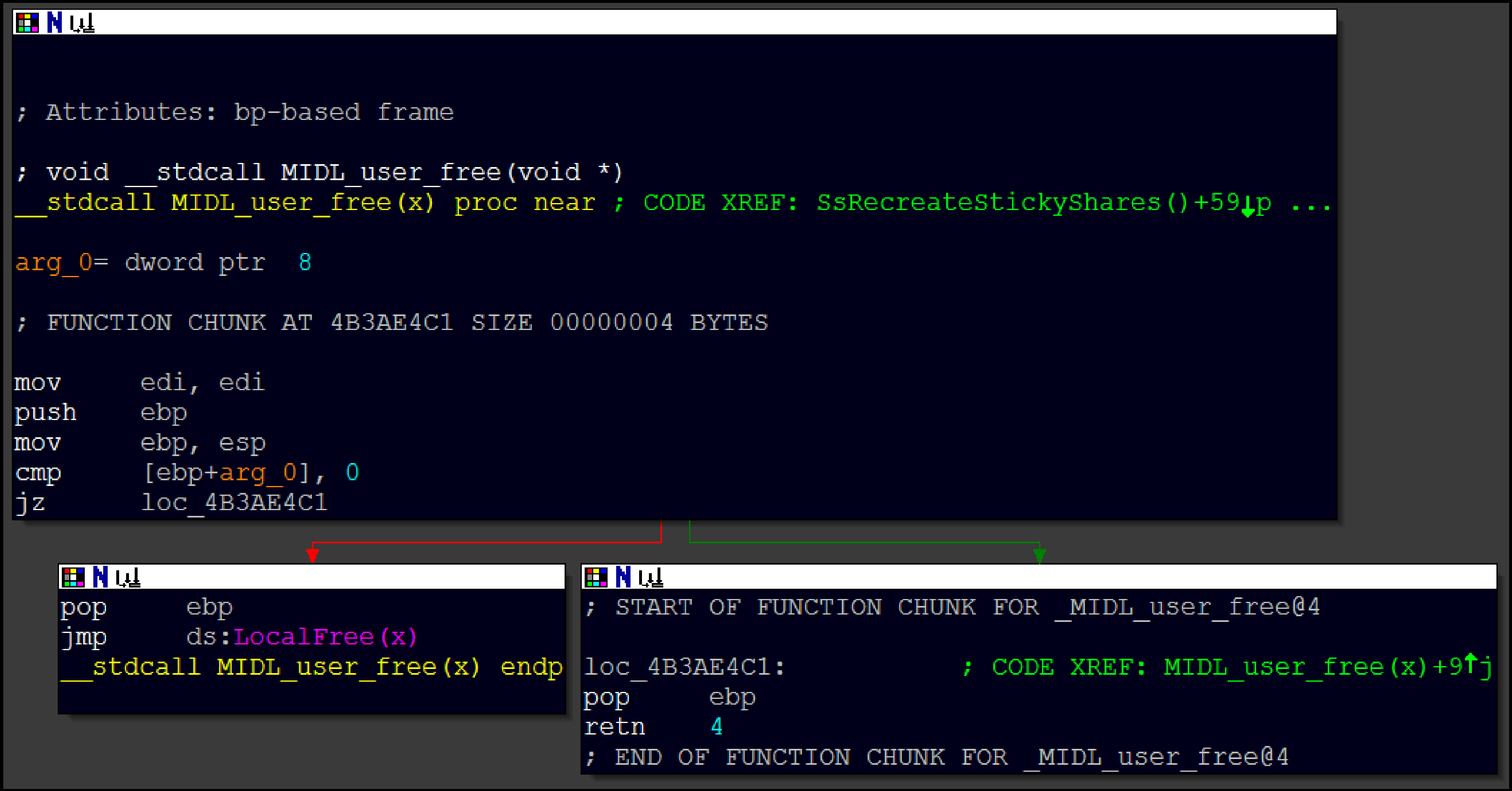
```
mov  ebx, dword_0x400400
test ebx, ebx
jz   fail
```

Instructions

Atomic

```
mov  eax, [ebp+0x4c]
```

Func/Basic block/Instruction

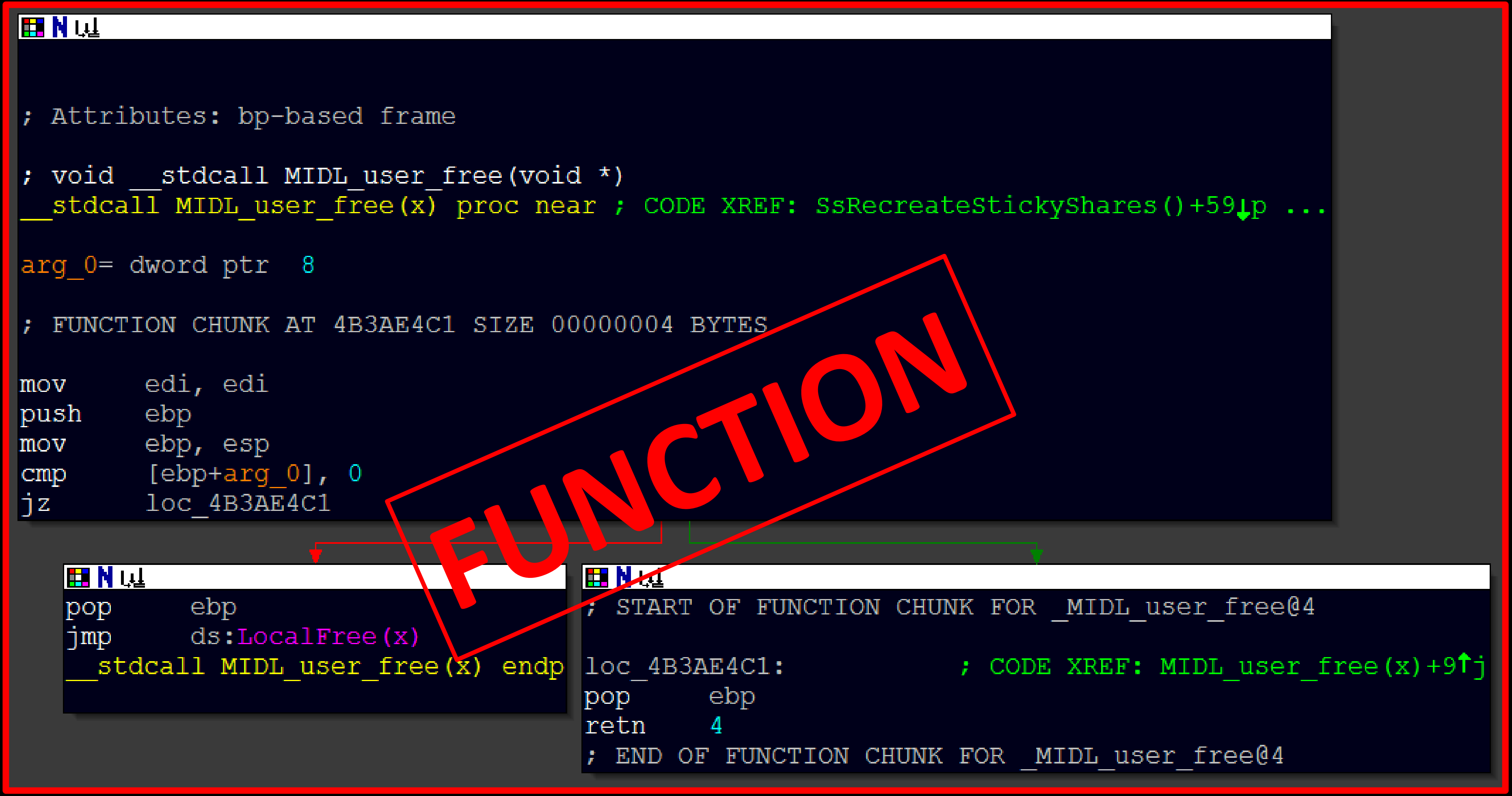


```
; Attributes: bp-based frame

; void __stdcall MIDL_user_free(void *)
__stdcall MIDL_user_free(x) proc near ; CODE XREF: SsRecreateStickyShares()+59↓p ...

arg_0= dword ptr  8

; FUNCTION CHUNK AT 4B3AE4C1 SIZE 00000004 BYTES

mov     edi, edi
push    ebp
mov     ebp, esp
cmp     [ebp+arg_0], 0
jz      loc_4B3AE4C1
```

```
pop     ebp
jmp     ds:LocalFree(x)
__stdcall MIDL_user_free(x) endp
```

```
; START OF FUNCTION CHUNK FOR _MIDL_user_free@4

loc_4B3AE4C1:           ; CODE XREF: MIDL_user_free(x)+9↑j
pop     ebp
retn    4
; END OF FUNCTION CHUNK FOR _MIDL_user_free@4
```

Func/Basic block/Instruction

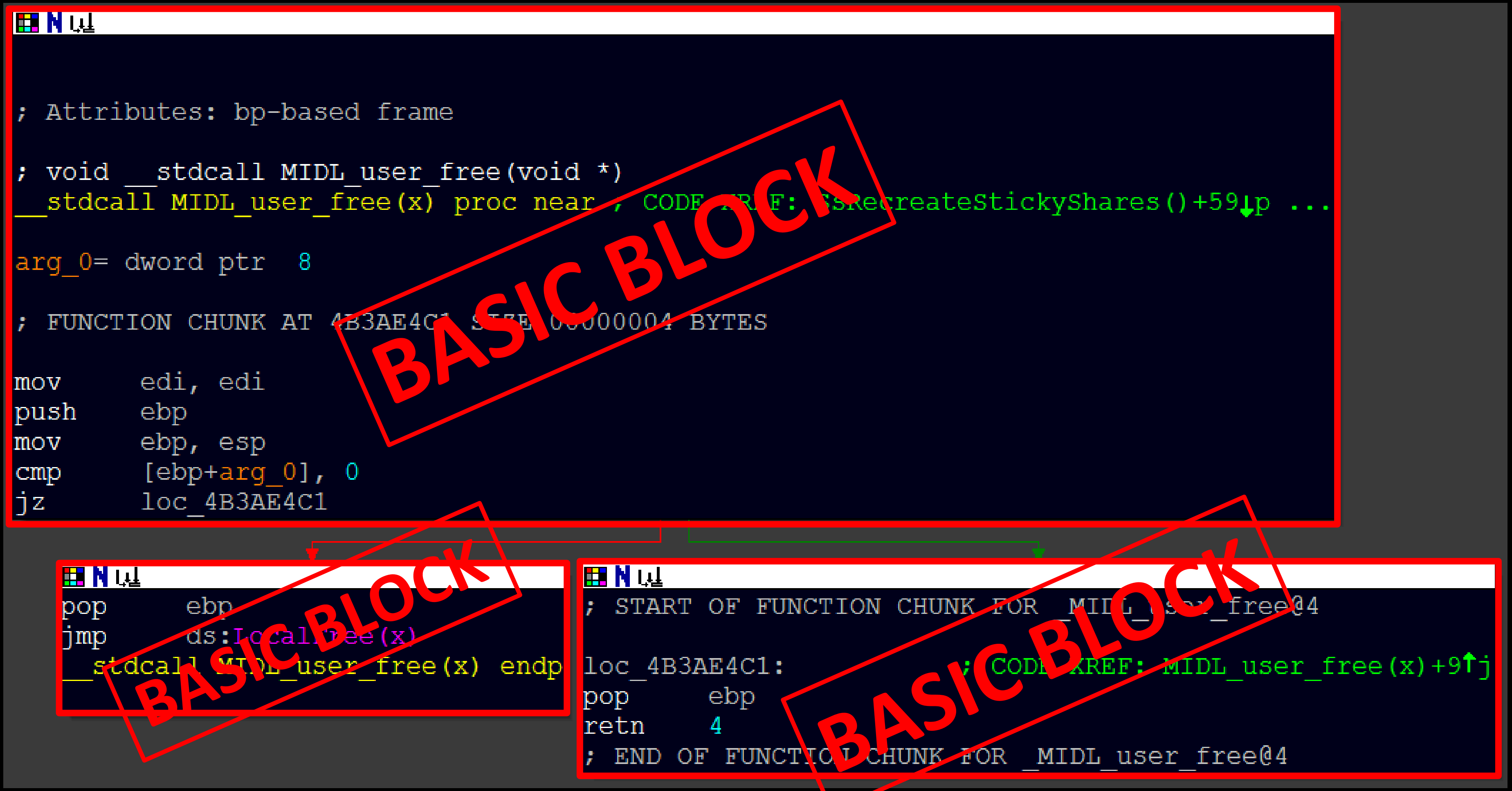


```
; Attributes: bp-based frame

; void __stdcall MIDL_user_free(void *)
__stdcall MIDL_user_free(x) proc near ; CODE XREF: SsRecreateStickyShares()+59↓p ...

arg_0= dword ptr  8

; FUNCTION CHUNK AT 4B3AE4C1 SIZE 00000004 BYTES

mov     edi, edi
push    ebp
mov     ebp, esp
cmp     [ebp+arg_0], 0
jz      loc_4B3AE4C1
```

```
pop     ebp
jmp     ds:LocalFree(x)
__stdcall MIDL_user_free(x) endp
```

```
; START OF FUNCTION CHUNK FOR _MIDL_user_free@4

loc_4B3AE4C1:             ; CODE XREF: MIDL_user_free(x)+9↑j
pop     ebp
retn    4
; END OF FUNCTION CHUNK FOR _MIDL_user_free@4
```

Func/Basic block/Instruction

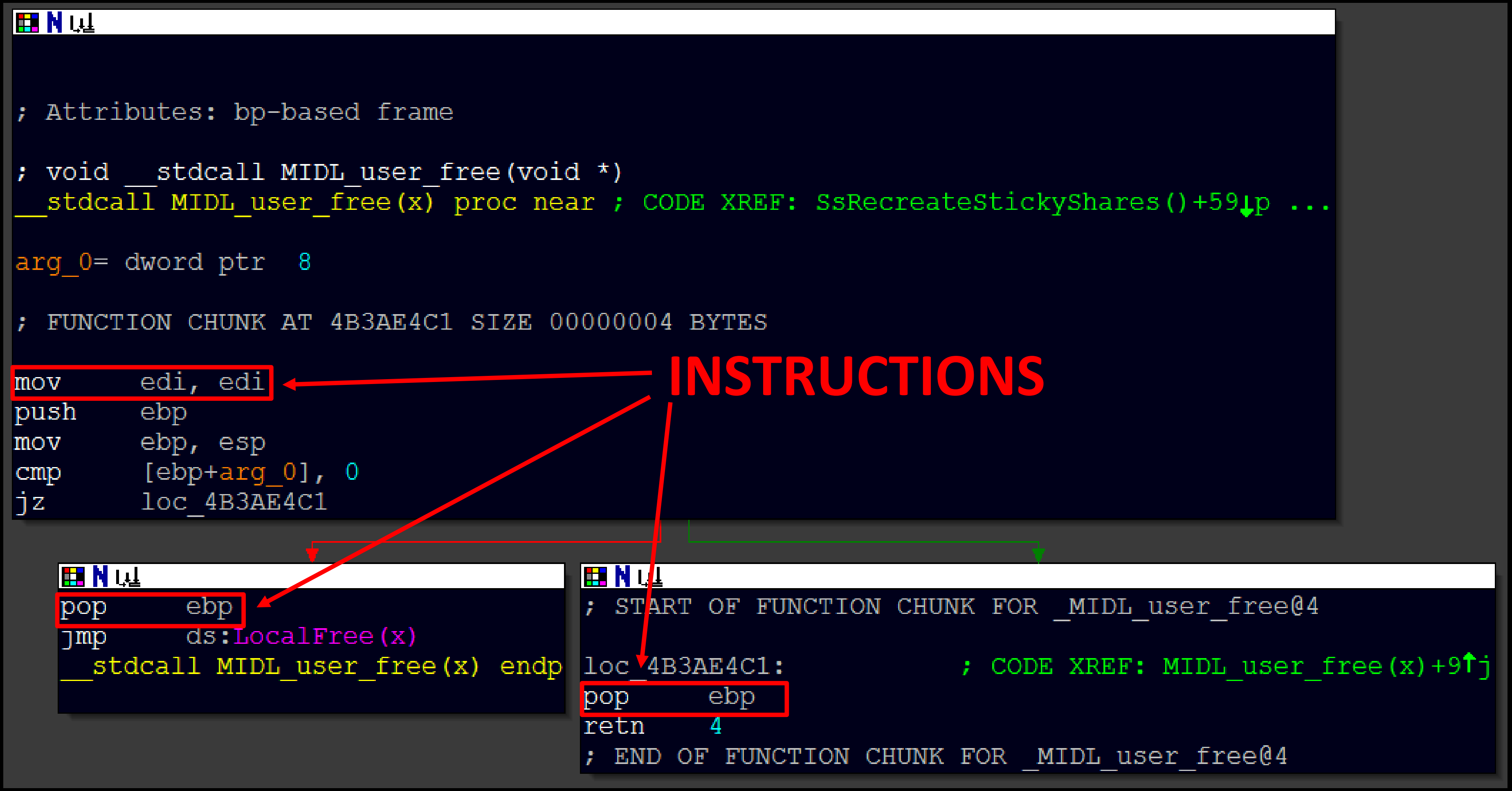


```
; Attributes: bp-based frame

; void __stdcall MIDL_user_free(void *)
__stdcall MIDL_user_free(x) proc near ; CODE XREF: SsRecreateStickyShares()+59↓p ...

arg_0= dword ptr  8

; FUNCTION CHUNK AT 4B3AE4C1 SIZE 00000004 BYTES

mov     edi, edi
push    ebp
mov     ebp, esp
cmp     [ebp+arg_0], 0
jz      loc_4B3AE4C1
```

```
pop     ebp
jmp     ds:LocalFree(x)
__stdcall MIDL_user_free(x) endp
```

```
; START OF FUNCTION CHUNK FOR _MIDL_user_free@4

loc_4B3AE4C1:                ; CODE XREF: MIDL_user_free(x)+9↑j
pop     ebp
retn    4
; END OF FUNCTION CHUNK FOR _MIDL_user_free@4
```

Func/Basic block/Instruction



```
; Attributes: bp-based frame

; void __stdcall MIDL_user_free(void *)
__stdcall MIDL_user_free(x) proc near ; CODE XREF: SsRecreateStickyShares()+59↓p ...

arg_0= dword ptr  8

; FUNCTION CHUNK AT 4B3AE4C1 SIZE 00000004 BYTES

mov     edi, edi
push    ebp
mov     ebp, esp
cmp     [ebp+arg_0], 0
jz      loc_4B3AE4C1
```

```
pop     ebp
jmp     ds:LocalFree(x)
__stdcall MIDL_user_free(x) endp
```

```
; START OF FUNCTION CHUNK FOR _MIDL_user_free@4

loc_4B3AE4C1:                ; CODE XREF: MIDL_user_free(x)+9↑j
pop     ebp
retn    4
; END OF FUNCTION CHUNK FOR _MIDL_user_free@4
```

Graphing

Code can be represented as a graph, as shown previously

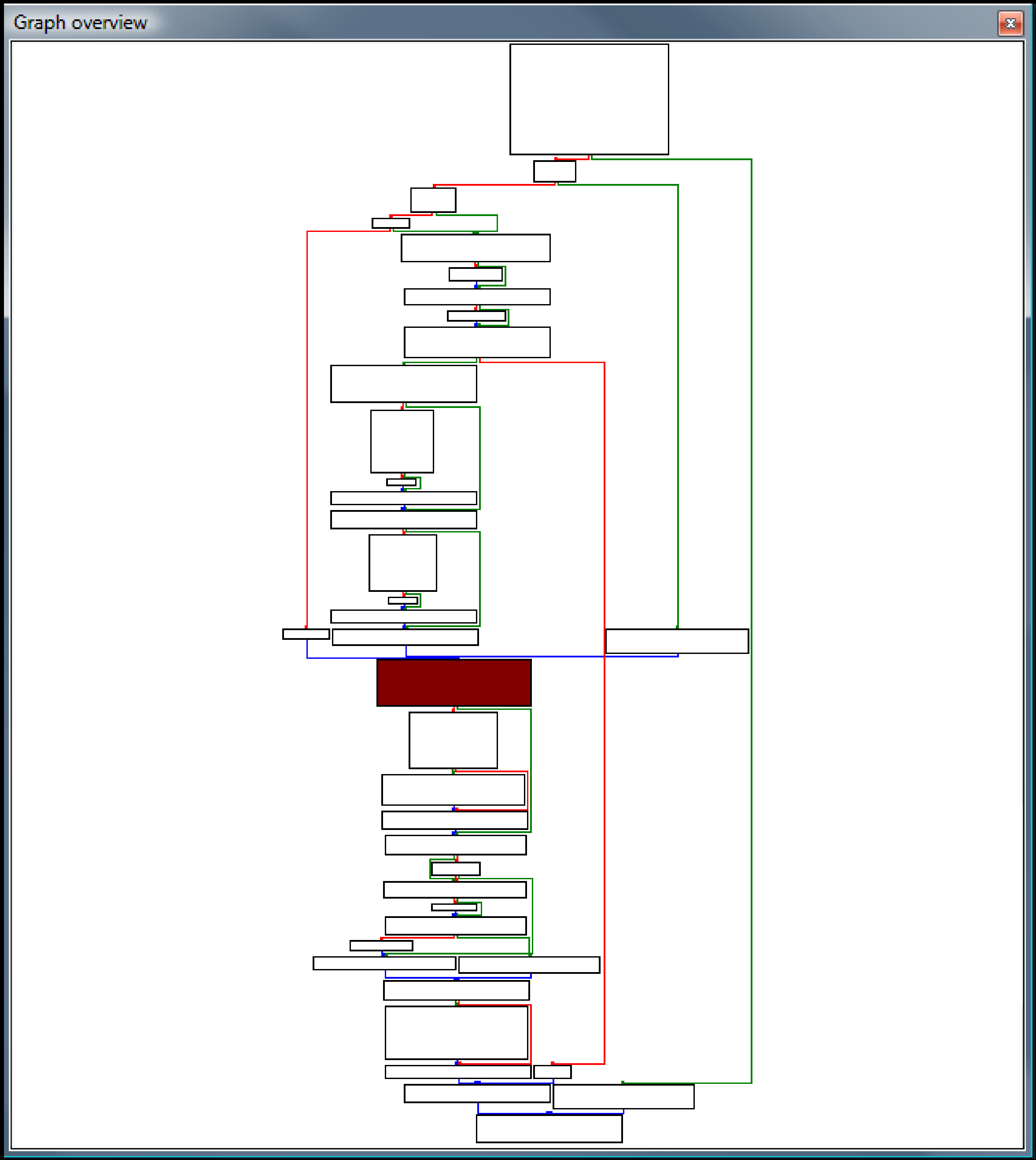
- Graph traversal code is applicable here
  - Assuming no dynamic transfers of execution, like:

```
call [edx+0x20]
```

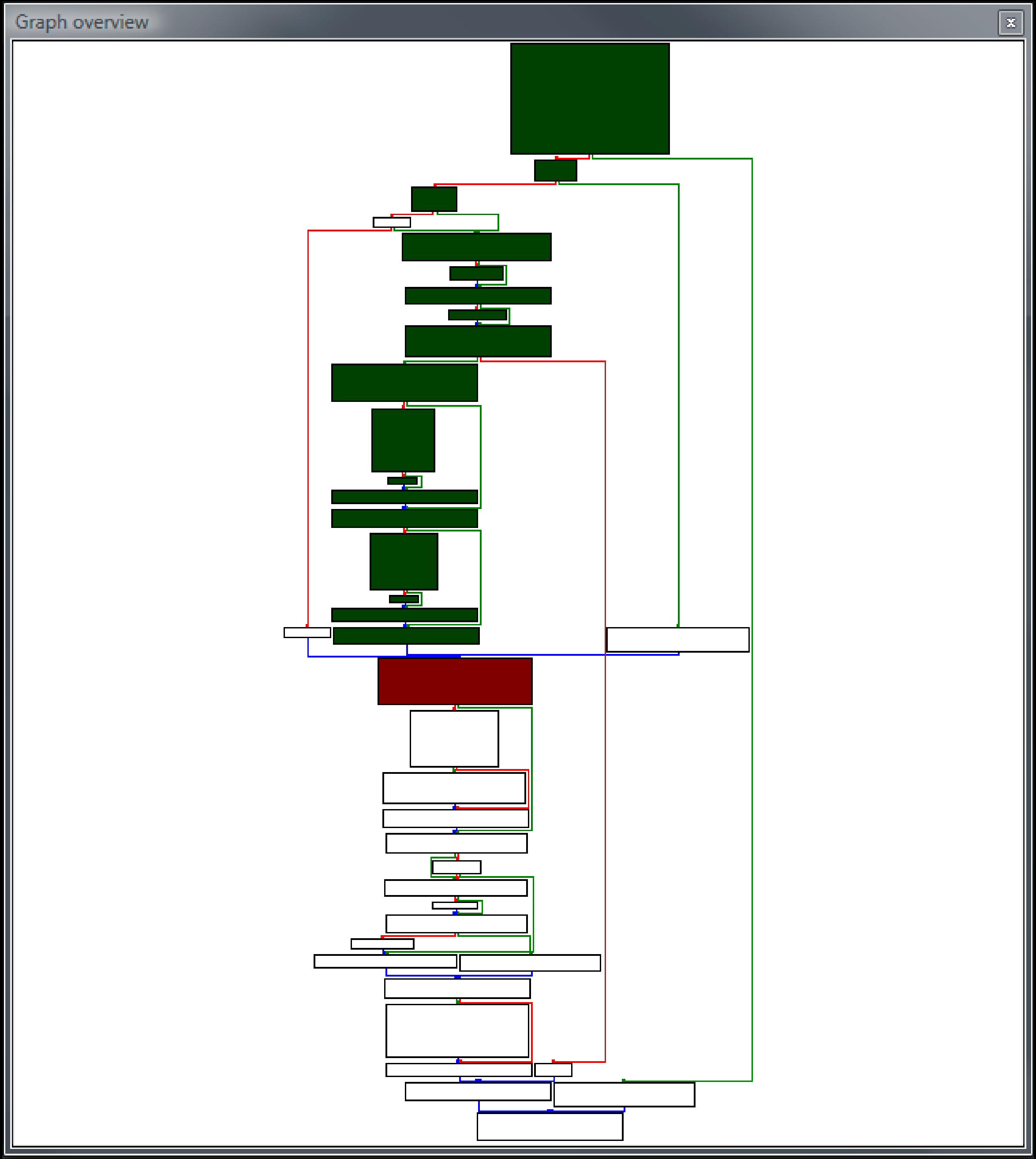
Graphing tricks

- Reachability (Function & Basic Block)
  - Upgraph/Downgraph/Intersection
  - Discover new vectors for attacks
  - Discover paths to interesting code
- Locate recursive functions programmatically
  - Loop detection
- Binary diffing (BinDiff from Zynamics)

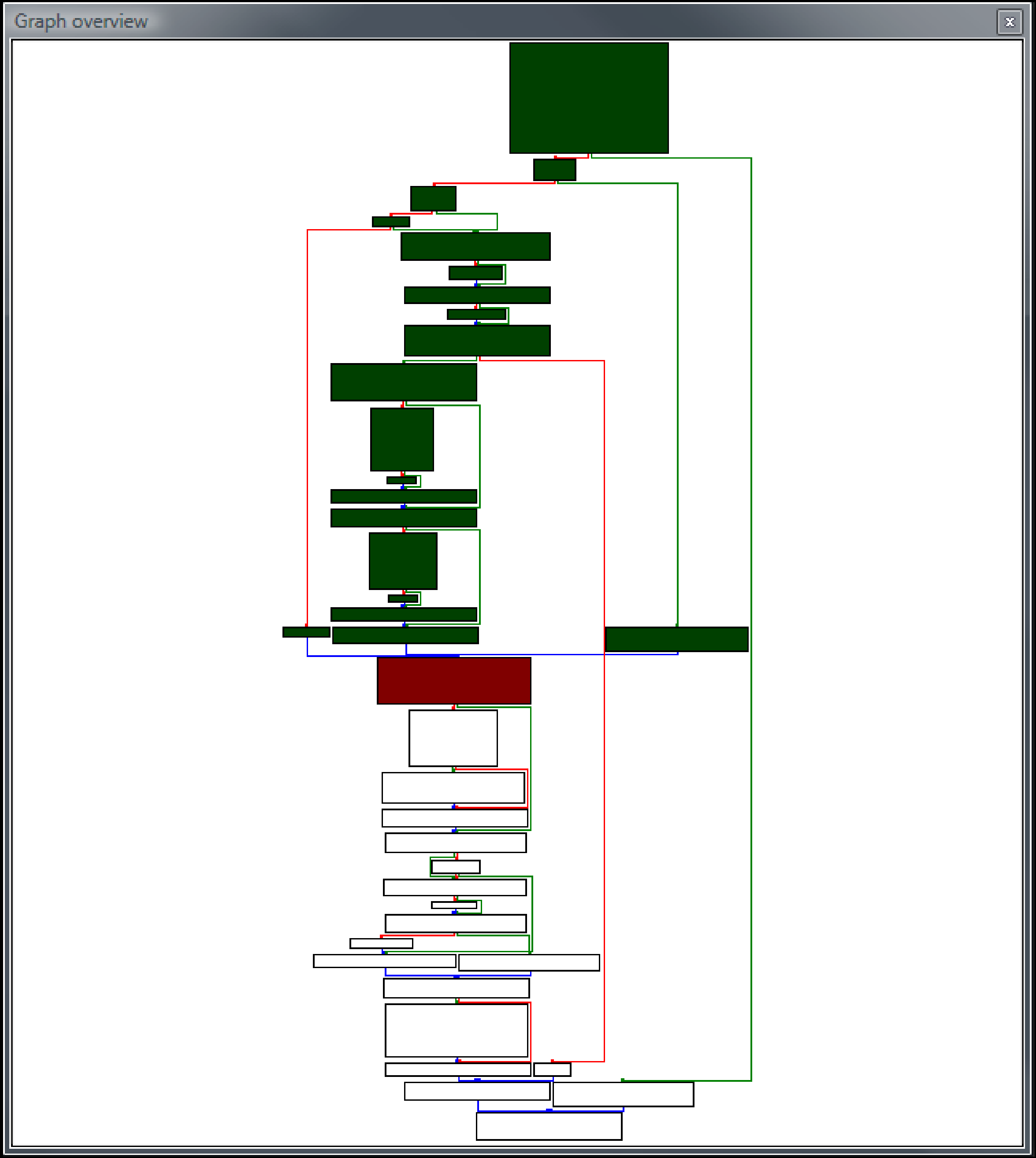
Graphing



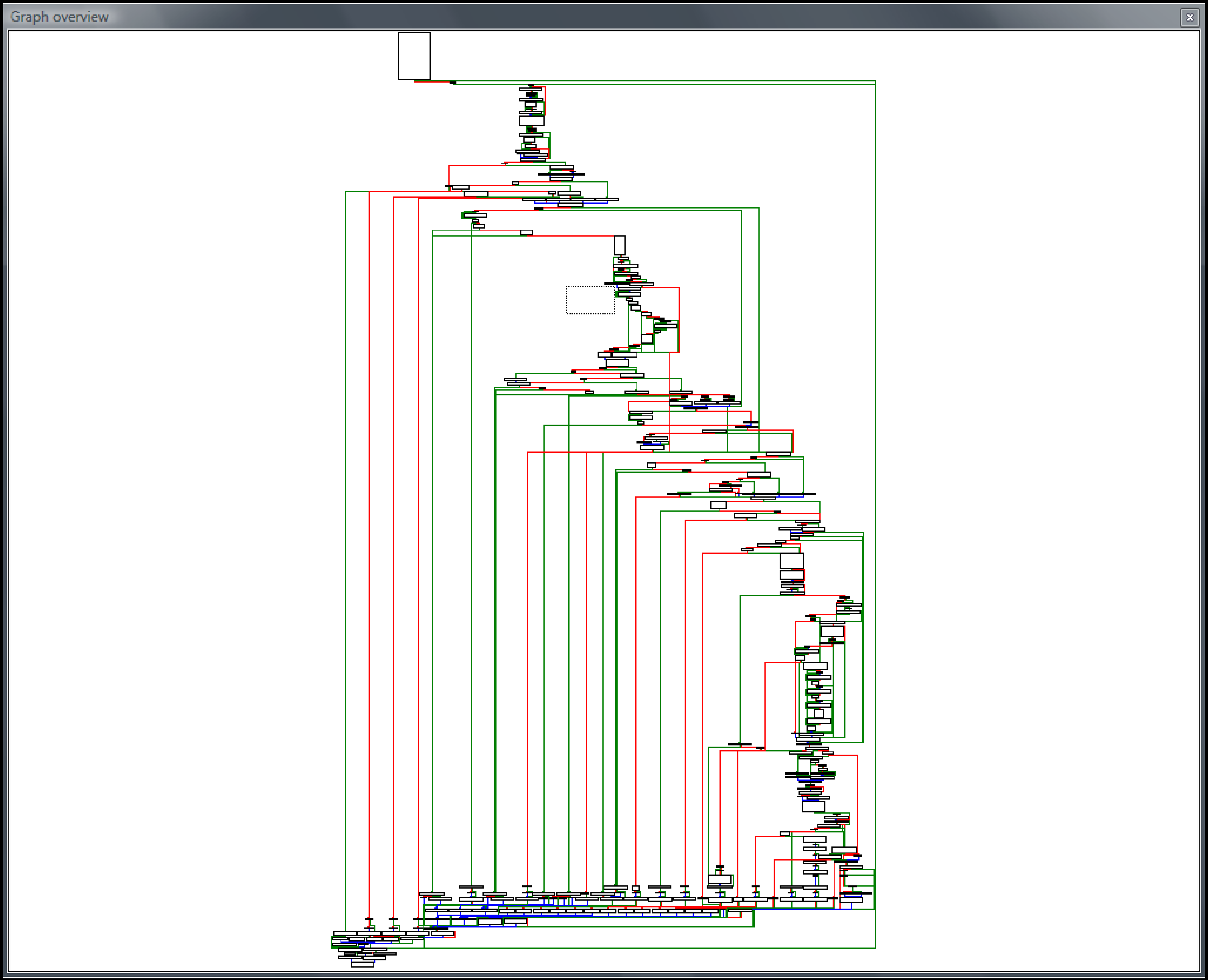
Graphing



Graphing



Graphing



Questions?

Intro to binary data structures

Objects (think object-oriented, C++, …)

- @ecx
- Constructors
- Destructors
- Function tables
    - Methods
- Inheritance

Variables

- Local
- Global
- Structures
- Defined on Stack vs. Heap
    - Important for exploitation

Introduction to IDA Pro

How many here have used a disassembler? IDA?

Important facilities to a reverser provided by IDA

- FLIRT
- Strings
  - assert() calls
  - debug functions
- Cross referencing
- Imports/Exports
- Segments

IDA SDK, IDC, IDAPython, IDA Debugger

- Plugins
- Automated analysis (we'll get to this later)

RE – Static Analysis

Important to locate sources of user input

- No runtime info available (besides sometimes RTTI)

Cross referencing and graphing is key

- C++ can make this aggravating

Pattern matching is helpful

- IDC/IDAPython
  - Find me all “movsx” from this function down
  - Find me all “add reg32, x” followed by malloc()
  - Loop detection
  - Unsafe library calls
    - *cpy
    - *alloc

RE – Dynamic Analysis

Breakpoints allow for jump start on analysis

- e.g. Memory breakpoint on recv() buffer

Ability to resolve…

- Object structure and relationships
    - Type information
- Input from other processes/systems/configs/…
    - Global variables

Ability to populate .idb with runtime information

<u>**Crucial to exploit development**</u>

- e.g. Analyze heap layout dynamically

Questions?

RE – Debuggers

	Pros	**Cons**
WinDBG	Mature piece of software. Great symbol support. Allows for neat tricks like heap walking and integrity checks. Kernel!	Steep learning curve. Poor plugin API.
OllyDBG	Intuitive user interface. Large community of users. Nice plugin API.	Flakey symbol support. Only supports 32-bit. **Default install exposes exploitable vulnerabilities!**
PyDBG	Scriptable and easily extensible.	Python is slow. Only supports 32-bit. Designed to be event-based.
IDA debugger	Contains 9 debugging engines. Built-in to IDA.	Multiple module support can be tricky to get the hang of. UI sketchy.

To Recap

Reverse from the top down

Understand the system to understand it’s parts

Use the proper tools to aid you

Saves time and focus

Use every technique you have available

Mixture of static and dynamic analysis

Conclusion of Session One

Questions?

E-mail the mailing list if you have additional questions

I am subscribed as well

Alternatively

My gmail username is aportnoy

Thanks!