

On non-existent 0-days, stable binary exploits and user interaction

Alisa Esage

Esage Lab // 000 C0P

GOAL

**NEED SOME 0-DAY REMOTE EXPLOITS*
FOR TOP SOFTWARE/OS, FAST**

How they do it

- Target memory corruption
- X% fuzzing + Y% static analysis
 - Only combination is viable
 - Other approaches are immature
- Fuzzing: massive overhead
 - Set up a framework
 - Develop patterns/heuristics !!
 - Take machine time
 - Analyze crash dumps !
 - Exploit, bypass DEP/ASLR/Sandbox !!!
- Perspective
 - protections harden
 - need more and more time to succeed
 - and resources to begin with

Perspective vectors

- By-design vulnerabilities
 - E.g. DLL Hijacking, UI redressing, LD_LIBRARY_PATH...
- Sandbox bypass for complex systems
 - E.g. JAVA: bypass SecurityManager -> full privileges for unsigned applet -> win
- Certificates
 - E.g. Adobe PDF: signed document -> trusted document -> full-privileged JavaScript -> win

Why DLL Hijacking?

- Test hacking skills!
 - Succeed with a blind alley before hitting the highway
- Looks easy
 - Plenty of previous research, e.g. binaryplanting.com
 - Interns must do research, too
- Real world targetted attacks: CVE-2011-1980, CVE-2011-1991, CVE-2011-2100
 - They work
- MS12-046 vbe6.dll
 - They still exist!
- OS behaviour undocumented
 - There is place for research

Research focus

- Top, clean platforms
 - Windows 7
 - Windows XP
 - Office 2010
 - Office 2007
 - Adobe Acrobat/Reader
- Find a new remote delivery vector
 - Not a “.dll” in e-mail attachment
 - Not a “.dll” in a network share
- Find something yet unfound

Tech recap

- Exe -> dll by relative path
- DLL Search Order
- Current Directory (CD) – MS DOS rudiment
- Default: app path
- File open: file path
- Some other changes
- Exploitation profit: Bypass restrictions, LPE, RCE
- Vectors: local, local network, client-side

Advantages

- 100% stable exploit
- 100% silent execution on non-supported targets
- Very little overhead
- No mess with protections
- ! Not fixable globally with simple measures like DEP/ASLR
 - Only developers education can help
 - Will reappear in new software forever

Challenges

- Search
 - “Trivial => already found” myth
- Exploitation
 - Nobody ever tried to manipulate CD
- User interaction
 - Triggered by clicking menus... now what?
- Masking / delivery
 - Document + DLL binding looks suspicious

Arguing myths

NONEXISTENT?

7500+ missing Windows DLLs

	A	B
1	Название DLL	ОС, в которых отсутствует
449	avmenu.dll	Windows 8, Server 2012, WindowsXP, Server 2003
450	avmeter.dll	Server 2008, Win Vista, Server 2012, Windows 7, Windows 8, Server 2003
451	avolprop.dll	WindowsXP, Windows 8, Win Vista, Windows 7, Server 2003
452	avrt.dll	WindowsXP, Server 2003
453	avtapi.dll	Server 2008, Windows 7, Server 2012, Win Vista, Windows 8, Server 2003
454	awwav.dll	Win Vista, Server 2008, Windows 7, Windows 8, Server 2003, Server 2012
455	axaltocm.dll	Windows 7, Windows 8, WindowsXP, Server 2003, Server 2012
456	AxInstSv.dll	Server 2003, WindowsXP, Server 2008
457	AzRLPia.dll	Windows 8, Win Vista, WindowsXP, Server 2012, Windows 7, Server 2008
458	azrlpia2.dll	Windows 8, Windows 7, Server 2012, Win Vista, Server 2008, WindowsXP
459	azroleui.dll	WindowsXP
460	AzSqlExt.dll	WindowsXP, Server 2003
461	backsnap.dll	Win Vista, Windows 8, WindowsXP, Server 2012, Windows 7, Server 2008
462	basebrd.dll	Server 2003, WindowsXP
463	basecsp.dll	Server 2003, WindowsXP
464	BatchParser.dll	Win Vista, Server 2003, Windows 7, Server 2008, Windows 8, WindowsXP
465	batt.dll	Windows 8, Server 2012
466	bcdeditai.dll	Win Vista, Server 2008, Windows 7, Server 2003, WindowsXP
467	bcdprov.dll	WindowsXP, Server 2003

20+ Mb filtered log per app

Time of Day	Process Name	PID	Operation	Path	Result
14:57:11,2682566	EXCEL.EXE	3836	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\PDFMaker...	NAME NOT FOUND
14:57:11,2751617	EXCEL.EXE	3836	CreateFile	C:\Program Files\Microsoft Office\Office12\MPS.dll	NAME NOT FOUND
14:57:11,2753342	EXCEL.EXE	3836	CreateFile	C:\Windows\System32\MPS.dll	NAME NOT FOUND
14:57:11,2756400	EXCEL.EXE	3836	CreateFile	C:\Windows\system\MPS.dll	NAME NOT FOUND
14:57:11,2757756	EXCEL.EXE	3836	CreateFile	C:\Windows\MPS.dll	NAME NOT FOUND
14:57:11,2759052	EXCEL.EXE	3836	CreateFile	C:\Users\daemon\Desktop\MPS.dll	NAME NOT FOUND
14:57:11,2760329	EXCEL.EXE	3836	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\PDFMaker...	NAME NOT FOUND
14:57:11,3007070	acrotray.exe	244	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\Acrobat\nt...	NAME NOT FOUND
14:57:13,4089440	EXCEL.EXE	3836	CreateFile	C:\Program Files\Microsoft Office\Office12\ATMLI...	NAME NOT FOUND
14:57:15,4962153	acrotray.exe	244	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\Acrobat\pr...	NAME NOT FOUND
14:57:15,6574357	acrotray.exe	244	CreateFile	C:\Windows\System32\wbem\wbemcomn.dll	NAME NOT FOUND
14:57:15,6670424	acrotray.exe	244	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\Acrobat\C...	NAME NOT FOUND
14:57:15,6769404	acrotray.exe	244	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\Acrobat\R...	NAME NOT FOUND
14:57:15,6990090	acrotray.exe	244	CreateFile	C:\Windows\System32\wbem\NTDSAPI.dll	NAME NOT FOUND
14:57:15,8030169	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\wbemcomn.dll	NAME NOT FOUND
14:57:15,8198506	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\NTDSAPI.dll	NAME NOT FOUND
14:57:15,8267253	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\NCObjAPI.DLL	NAME NOT FOUND
14:57:15,8913089	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\CRYPTBASE.dll	NAME NOT FOUND
14:57:15,8922964	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\ntmarta.dll	NAME NOT FOUND
14:57:15,9067852	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\CRYPTSP.dll	NAME NOT FOUND
14:57:15,9154699	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\RpcRtRemote.dll	NAME NOT FOUND
14:57:15,9626356	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\framedynos.dll	NAME NOT FOUND
14:57:16,0462638	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\SspiCli.dll	NAME NOT FOUND
14:57:16,0470821	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\WTSAPI32.dll	NAME NOT FOUND
14:57:16,3674810	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\WMI.DLL	NAME NOT FOUND
14:57:17,0191646	csrss.exe	348	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\Acrobat\Ad...	NAME NOT FOUND
14:57:17,0246286	Acrobat.exe	2568	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\Acrobat\W...	NAME NOT FOUND
14:57:17,0562178	Acrobat.exe	2568	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\Acrobat\C...	NAME NOT FOUND

Arguing myths

NOT EXPLOITABLE?

Good!

Time of Day	Process Name	PID	Operation	Path	Result
1:54:23,2735941	OUTLOOK.EXE	3288	QueryOpen	D:_TEST_\imageres.dll	NAME NOT FOUND
1:54:35,0773821	OUTLOOK.EXE	3288	QueryOpen	D:_TEST_\cryptui.dll	NAME NOT FOUND
1:54:45,8151853	mpc-hc.exe	3044	QueryOpen	D:_TEST_\xvidcore.dll	NAME NOT FOUND
1:54:45,8161857	mpc-hc.exe	3044	QueryOpen	D:_TEST_\xvidcore.dll	NAME NOT FOUND
1:54:45,8182477	mpc-hc.exe	3044	QueryOpen	D:_TEST_\avisynth.dll	NAME NOT FOUND
1:54:45,8188166	mpc-hc.exe	3044	QueryOpen	D:_TEST_\avisynth.dll	NAME NOT FOUND
1:54:45,8217443	mpc-hc.exe	3044	QueryOpen	D:_TEST_\ff_liba52.dll	NAME NOT FOUND
1:54:45,8224413	mpc-hc.exe	3044	QueryOpen	D:_TEST_\ff_liba52.dll	NAME NOT FOUND
1:54:45,8251856	mpc-hc.exe	3044	QueryOpen	D:_TEST_\IntelQuickSyn...	NAME NOT FOUND
1:54:45,8259004	mpc-hc.exe	3044	QueryOpen	D:_TEST_\IntelQuickSyn...	NAME NOT FOUND
1:54:45,9473821	mpc-hc.exe	3044	QueryOpen	D:_TEST_\xvidcore.dll	NAME NOT FOUND
1:54:45,9481133	mpc-hc.exe	3044	QueryOpen	D:_TEST_\xvidcore.dll	NAME NOT FOUND
1:54:45,9510509	mpc-hc.exe	3044	QueryOpen	D:_TEST_\avisynth.dll	NAME NOT FOUND
1:54:45,9517870	mpc-hc.exe	3044	QueryOpen	D:_TEST_\avisynth.dll	NAME NOT FOUND
1:54:45,9550430	mpc-hc.exe	3044	QueryOpen	D:_TEST_\ff_liba52.dll	NAME NOT FOUND
1:54:45,9558464	mpc-hc.exe	3044	QueryOpen	D:_TEST_\ff_liba52.dll	NAME NOT FOUND

Not so good

Time of Day	Process Name	PID	Operation	Path	Result
14:57:11,2682566	EXCEL.EXE	3836	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\PDFMaker...	NAME NOT FOUND
14:57:11,2751617	EXCEL.EXE	3836	CreateFile	C:\Program Files\Microsoft Office\Office12\MPS.dll	NAME NOT FOUND
14:57:11,2753342	EXCEL.EXE	3836	CreateFile	C:\Windows\System32\MPS.dll	NAME NOT FOUND
14:57:11,2756400	EXCEL.EXE	3836	CreateFile	C:\Windows\system\MPS.dll	NAME NOT FOUND
14:57:11,2757756	EXCEL.EXE	3836	CreateFile	C:\Windows\MPS.dll	NAME NOT FOUND
14:57:11,2759052	EXCEL.EXE	3836	CreateFile	C:\Users\daemon\Desktop\MPS.dll	NAME NOT FOUND
14:57:11,2760329	EXCEL.EXE	3836	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\PDFMaker...	NAME NOT FOUND
14:57:11,3007070	acrotray.exe	244	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\Acrobat\nt...	NAME NOT FOUND
14:57:13,4089440	EXCEL.EXE	3836	CreateFile	C:\Program Files\Microsoft Office\Office12\ATMLI...	NAME NOT FOUND
14:57:15,4962153	acrotray.exe	244	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\Acrobat\pr...	NAME NOT FOUND
14:57:15,6574357	acrotray.exe	244	CreateFile	C:\Windows\System32\wbem\wbemcomn.dll	NAME NOT FOUND
14:57:15,6670424	acrotray.exe	244	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\Acrobat\C...	NAME NOT FOUND
14:57:15,6769404	acrotray.exe	244	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\Acrobat\R...	NAME NOT FOUND
14:57:15,6990090	acrotray.exe	244	CreateFile	C:\Windows\System32\wbem\NTDSAPI.dll	NAME NOT FOUND
14:57:15,8030169	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\wbemcomn.dll	NAME NOT FOUND
14:57:15,8198506	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\NTDSAPI.dll	NAME NOT FOUND
14:57:15,8267253	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\NCObjAPI.DLL	NAME NOT FOUND
14:57:15,8913089	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\CRYPTBASE.dll	NAME NOT FOUND
14:57:15,8922964	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\ntmarta.dll	NAME NOT FOUND
14:57:15,9067852	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\CRYPTSP.dll	NAME NOT FOUND
14:57:15,9154699	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\RpcRtRemote.dll	NAME NOT FOUND
14:57:15,9626356	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\framedynos.dll	NAME NOT FOUND
14:57:16,0462638	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\SspiCli.dll	NAME NOT FOUND
14:57:16,0470821	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\WTSAPI32.dll	NAME NOT FOUND
14:57:16,3674810	wmiprvse.exe	768	CreateFile	C:\Windows\System32\wbem\WMI.DLL	NAME NOT FOUND
14:57:17,0191646	csrss.exe	348	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\Acrobat\Ad...	NAME NOT FOUND
14:57:17,0246286	Acrobat.exe	2568	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\Acrobat\W...	NAME NOT FOUND
14:57:17,0562178	Acrobat.exe	2568	CreateFile	C:\Program Files\Adobe\Acrobat 10.0\Acrobat\C...	NAME NOT FOUND

Goal: manipulate CD

If **SafeDllSearchMode** is enabled, the search order is as follows:

1. The directory from which the application loaded.
2. The system directory. Use the **GetSystemDirectory** function to get the path.
3. The 16-bit system directory. There is no function that obtains the path of this directory.
4. The Windows directory. Use the **GetWindowsDirectory** function to get the path.
5. The current directory.
6. The directories that are listed in the PATH environment variable. Note that the **Path** registry key is used. The **App Paths** key is not used when computing the DLL search order.

If **SafeDllSearchMode** is disabled, the search order is as follows:

1. The directory from which the application loaded.
2. The current directory.
3. The system directory. Use the **GetSystemDirectory** function to get the path.
4. The 16-bit system directory. There is no function that obtains the path of this directory.
5. The Windows directory. Use the **GetWindowsDirectory** function to get the path.
6. The directories that are listed in the PATH environment variable. Note that the **Path** registry key is used. The **App Paths** key is not used when computing the DLL search order.

CD internals

- 0:005> dt _PEB @\$peb -r

- ntdll!_PEB

- ...

- +0x010 ProcessParameters : 0x00020000 _RTL_USER_PROCESS_PARAMETERS

- ...

- +0x024 CurrentDirectory : _CURDIR

- +0x000 DosPath : _UNICODE_STRING "C:\Documents and Settings\h\My Documents\"

- +0x008 Handle : 0x00000b50 Void

- // получение адреса CurrentDirectory (первый dword - размеры, второй – указатель на строку)

- 0:005> dd poi(@\$peb+0x010)+0x024

- 00020024 02080052 00020290 00000b50 01840182

- 00020034 00020498 006e006c 0002061c 00740072

- // проверка адреса CD

- 0:005> du 0x20290

- 00020290 "C:\Documents and Settings\h\My D"

- 000202d0 "ocuments\"













- // точка останова

- 0:005> ba w 4 0x20290

CD internals - 2

- MSDN: “it is the directory in which the active application started, unless it has been explicitly changed“ – **actually no**
- Way of starting an app affects CD
 - App exec default: app dir
 - App exec: Software\Microsoft\Windows\CurrentVersion\App Paths
 - Exec by Ink: Ink dir
 - **Document open: document dir**
 - **CreateProcess(): lpCurrentDirectory**
- CD set internally by some API
 - **GetOpenFileName() / GetSaveFileName()**
 - FindFirstFile() / FindNextFile() (presumably)
- Many file system APIs depend on CD
 - So developers call SetCurrentDirectory() every now and then

So...?

1984	 CreateFile	C:\Program Files\Windows Media Player\rapi.dll	NAME NOT FOUND
1984	 CreateFile	C:\Windows\System32\rapi.dll	NAME NOT FOUND
1984	 CreateFile	C:\Windows\system\rapi.dll	NAME NOT FOUND
1984	 CreateFile	C:\Windows\rapi.dll	NAME NOT FOUND
1984	 CreateFile	C:\Program Files\Windows Media Player\rapi.dll	NAME NOT FOUND
1984	 CreateFile	C:\Program Files\Adobe\Acrobat 10.0\PDFMaker\Office\rapi.dll	NAME NOT FOUND
1984	 CreateFile	C:\Program Files\Adobe\Acrobat 10.0\Acrobat\rapi.dll	NAME NOT FOUND
1984	 CreateFile	C:\Program Files\Microsoft Office\Office14\rapi.dll	NAME NOT FOUND
1984	 CreateFile	C:\Windows\System32\rapi.dll	NAME NOT FOUND
1984	 CreateFile	C:\Windows\rapi.dll	NAME NOT FOUND
1984	 CreateFile	C:\Windows\System32\wbem\rapi.dll	NAME NOT FOUND
1984	 CreateFile	C:\Windows\System32\WindowsPowerShell\v1.0\rapi.dll	NAME NOT FOUND

Local exploitation

- Bypass restrictions/LPE: place exploit DLL into unrestricted location
- Consider %PATH%

PATH FTW



I experience a very strange problem. I have the following path variable.

1



1

```
%SystemRoot%\system32\WindowsPowerShell\v1.0\;C:\Python27\;C:\Python27\Scripts;C:\Program Files\Common Files\Microsoft Shared\Windows Live;C:\Program Files (x86)\Common Files\Microsoft Shared\Windows Live;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program Files (x86)\Lenovo\Access Connections\;C:\Program Files\ThinkPad\Bluetooth Software\;C:\Program Files\ThinkPad\Bluetooth Software\syswow64;C:\SWTOOLS\ReadyApps;C:\Program Files (x86)\Windows Live\Shared;C:\Program Files (x86)\GTK2-Runtime\bin;C:\Program Files\Intel\WiFi\bin\;C:\Program Files\Common Files\Intel\WirelessCommon\;C:\Users\Robert\AppData\Roaming\Python\Scripts;C:\Windows\system32\WindowsPowerShell\v1.0\;C:\Program Files\Common Files\Microsoft Shared\Windows Live;C:\Program Files (x86)\Common Files\Microsoft Shared\Windows Live;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program Files (x86)\Lenovo\Access Connections\;C:\Program Files\ThinkPad\Bluetooth Software\;C:\Program Files\ThinkPad\Bluetooth Software\syswow64;C:\SWTOOLS\ReadyApps;C:\Program Files (x86)\Windows Live\Shared;C:\Program Files (x86)\GTK2-Runtime\bin;C:\Program Files\Intel\WiFi\bin\;C:\Program Files\Common
```

Remote exploitation

- Just open a document (the lucky case)
- Make user Open/Save/Import/Export files, then trigger
- Or automate file operations with a script
- Induce an app state with CD changed by developer
- Set CD explicitly
- Find an app that CreateProcess()-es vulnerable app with good CD






Arguing myths

EXPLOIT DLL TOO OBVIOUS?

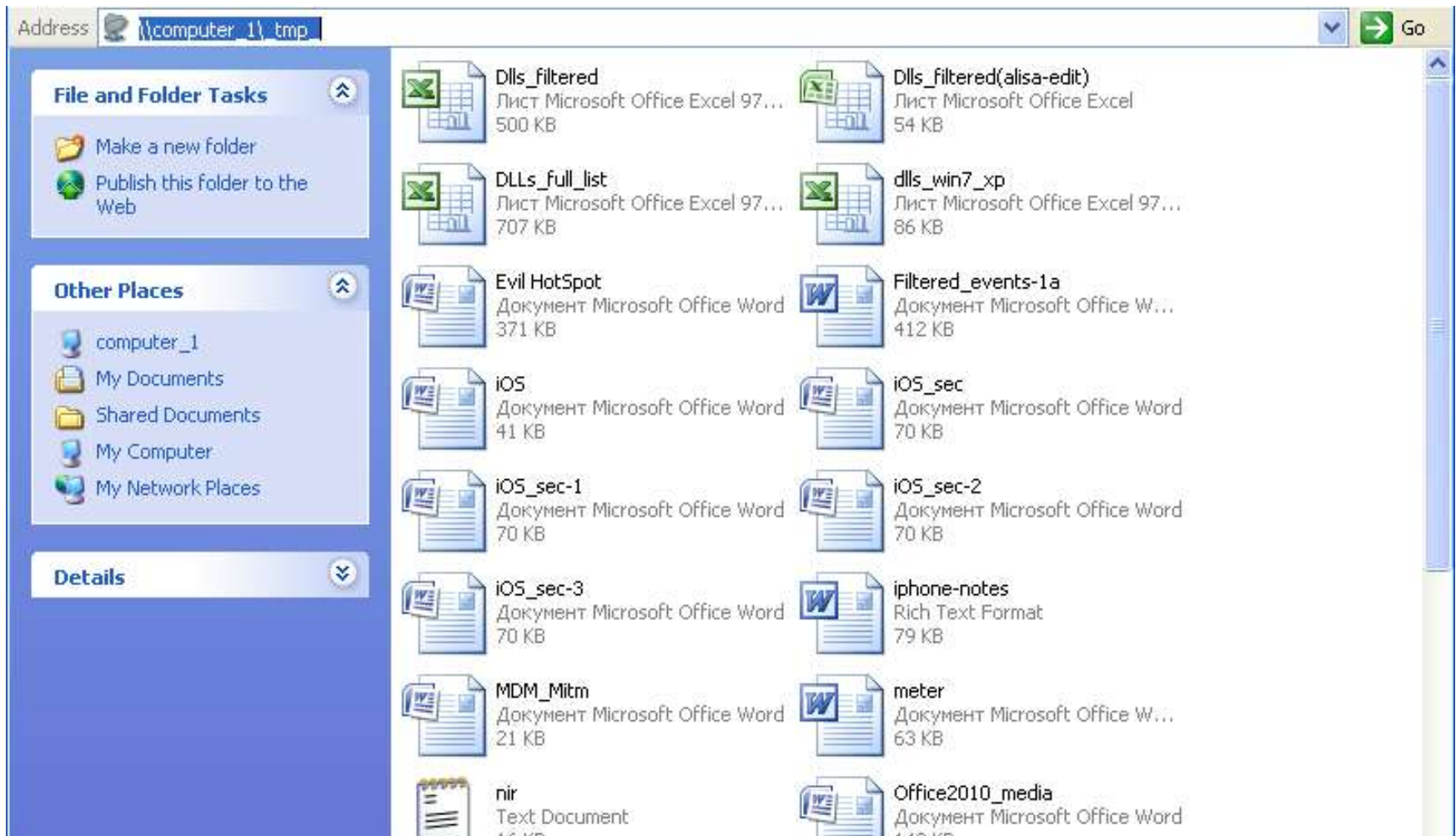
No hiding

The PDF was detected on April 13 in a 7z archive, which included

- 1) 2 clean pdfs (have some info about the victim and not included for the
- 2) oleacc.dll Size: 32768 MD5: BADD488212891EBC1D76BE901E70D4A1
- 3) Speaker information1.pdf Size: 12253 MD5: 7EA84B62DA84DCD8B6F577D6
- 4) Thumbs.db 34816 bytes 2898107be3c4ac71cd16898b6a08fe87

Name	Size	Type
 Agenda.pdf	45 KB	Adobe Acrobat Doc...
 oleacc.dll	32 KB	Application Extension
 Speaker Information1.pdf	12 KB	Adobe Acrobat Doc...
 Speaker Information2.pdf	174 KB	Adobe Acrobat Doc...
 Thumbs.db	16 KB	Data Base File

A needle in the haystack



Torrents

Torrent Contents

Name: HQ Wallpapers Cats









Comment: <http://rutracker.org/forum/viewtopic.php?t=251554>

Size: 446 MB (disk space: 27.7 GB)

Date: 29.06.2010 13:55:48

Select All

Select None

Name	Size
+ <input checked="" type="checkbox"/>  1024x768	66.4 MB
+ <input checked="" type="checkbox"/>  1280x1024	13.5 MB
+ <input checked="" type="checkbox"/>  1280x960	3.77 MB
+ <input checked="" type="checkbox"/>  1280x800	1.50 MB
+ <input checked="" type="checkbox"/>  1440x900	5.38 MB
+ <input checked="" type="checkbox"/>  1600x1200	137 MB
+ <input checked="" type="checkbox"/>  1680x1050	9.27 MB
+ <input checked="" type="checkbox"/>  1920x1200	94.0 MB

Browser UI redressing

- IE9 on Windows 7
- Context: Local directory, network shared directory, WebDAV
- Explorer dir underneath a website
- **Demo**
- Also works in Chrome on Windows 7, but restricted to file download operations

Browser UI redressing (2)

- Chrome on Windows 7
- Context: remote
- Web server directory underneath a website
- Click-jacking game to silently download necessary files one-by-one
- Until all files are saved in %Downloads%
- Open exploit document

Set CD macro (MS Office)

- Context: local dir, network shared dir
- You can just execute arbitrary DLL from a macro
- But better to execute a `kernel32!SetCurrentDirectory()` API to fool forensic analysts
- **Demo**

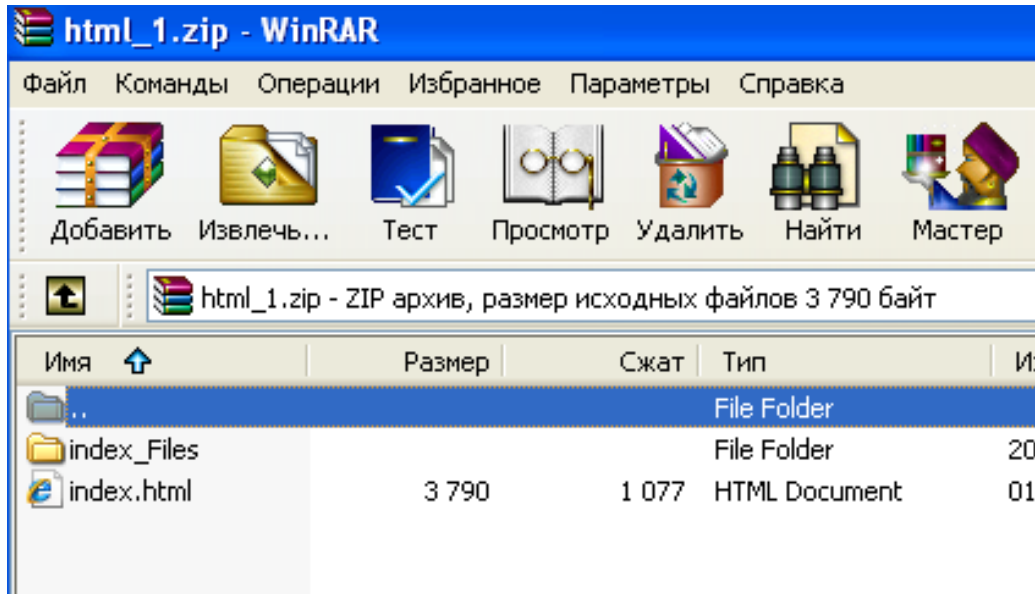
MHT

- Single file in e-mail attachment
- Can contain any types of files, incl. binary
- Browser extracts files to %INET_TMP%
- Open exploit document by clicking <a href=“.\files\document.txt”
- Exploit DLL will be executed from the same directory
- IE9 on Windows 7

Archives

- Any archives for Windows that extract all files by default? Not SFX of course
- WinRAR (latest): browse archive, double-click a HTML document only
 - Will extract ALL files into %TMP%
 - Including exploit DLL
 - Local browser context already

WinRAR FTW



WinRAR.exe	2116	QueryDirec...	C:\Documents and Settings\h\Local Settings\Temp\Rar\$EXa0.019\index_Files\calc.exe	NO SUCH FIL
WinRAR.exe	2116	CloseFile	C:\Documents and Settings\h\Local Settings\Temp\Rar\$EXa0.019\index_Files	SUCCESS
WinRAR.exe	2116	CreateFile	C:\Documents and Settings\h\Local Settings\Temp\Rar\$EXa0.019\index_Files\c...	SUCCESS
WinRAR.exe	2116	CreateFile	C:\Documents and Settings\h\Local Settings\Temp\Rar\$EXa0.019\index_Files	SUCCESS
WinRAR.exe	2116	CloseFile	C:\Documents and Settings\h\Local Settings\Temp\Rar\$EXa0.019\index_Files	SUCCESS
WinRAR.exe	2116	SetEndOfFi...	C:\Documents and Settings\h\Local Settings\Temp\Rar\$EXa0.019\index_Files\calc.exe	SUCCESS
WinRAR.exe	2116	SetAllocati...	C:\Documents and Settings\h\Local Settings\Temp\Rar\$EXa0.019\index_Files\calc.exe	SUCCESS
WinRAR.exe	2116	ReadFile	C:_tmp\html_1\html_1.zip	SUCCESS
WinRAR.exe	2116	ReadFile	C:_tmp\html_1\html_1.zip	SUCCESS
WinRAR.exe	2116	ReadFile	C:_tmp\html_1\html_1.zip	SUCCESS
WinRAR.exe	2116	WriteFile	C:\Documents and Settings\h\Local Settings\Temp\Rar\$EXa0.019\index_Files\calc.exe	SUCCESS

Multistage

- Case: DLL triggered by manual file import, no registered extension handler – unexploitable?
- Stage 1: User gets an e-mail from admin (fake) instructing to install the attached reg-file (looks innocent)
- In two weeks, stage 2: user gets an e-mail from a friend with a RAR-ed html game
- Click-jacked open file -> exploit
- Or open file via network share
- As simple as the user is

So, what do we have?

- **Some** 0-day vulnerabilities in up-to-date top platforms
 - Think of non-top software
- Ways to manipulate CD
- Ways to hide DLL
- Remote DLL Hijacking exploitation looks like normal client-side exploitation
- What else?

Conclusions

- Is this a good vector for mass attacks?
 - Authors of CVE-2011-1991, 1980, 2100 could tell us for sure
 - I say no
 - 0-day exploits are not necessary for mass attacks anyway
- Excellent vector for rapid targeted/onsite attacks
 - Plenty of vulnerabilities everywhere
 - Easy 'n fast to find **in arbitrary environment**
 - Ease 'n fast to exploit (after this presentation 😊)
- **Even the most trivial bug can be worked down to a good exploit**

Questions?

Thanks to my team and interns

Thank you for attention

@alisaesage