Advanced (Persistent) Binary Planting

Mitja Kolsek

ACROS

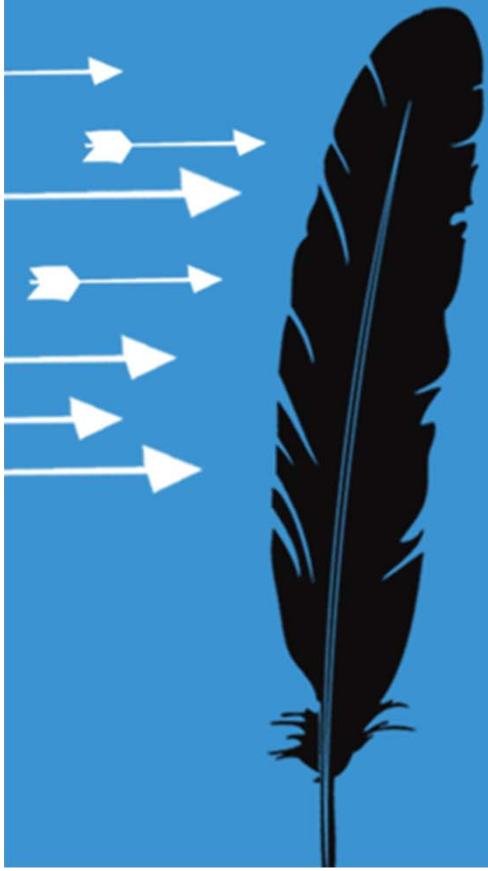
Session ID: HT2-302

Session Classification: Advanced

RSACONFERENCE2012

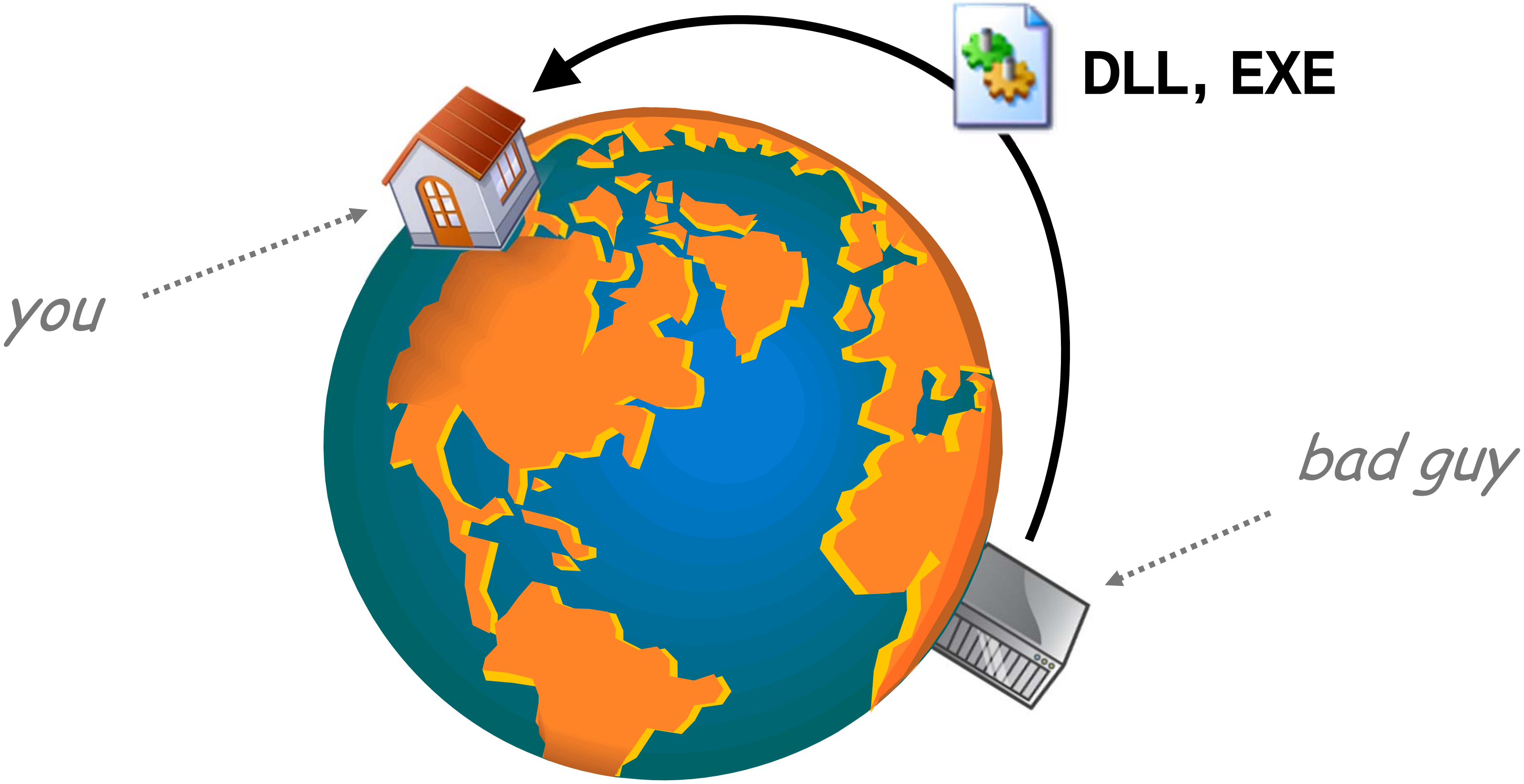
Today’s Menu

Appetizer	Quick Recap Of Binary Planting
Entrée	Persistence In Software
Main course	Persistence On Computer
Desert	Guidelines



Binary Planting Quick Summary

DLL hijacking, DLL preloading, Insecure library loading, …


DLL, EXE
you
bad guy

DLL Search Order

```
LoadLibrary(“SomeLib.dll”)
```

1. The directory from which the application loaded
2. C:\Windows\System32
3. C:\Windows\System
4. C:\Windows
5. Current Working Directory (CWD)
6. PATH

EXE Search Order

```
CreateProcess(“SomeApp.exe”)
```

1. The directory from which the application loaded
2. Current Working Directory (CWD)
3. C:\Windows\System32
4. C:\Windows\System
5. C:\Windows
6. PATH

EXE Search Order

```
ShellExecute("SomeApp.exe")
```

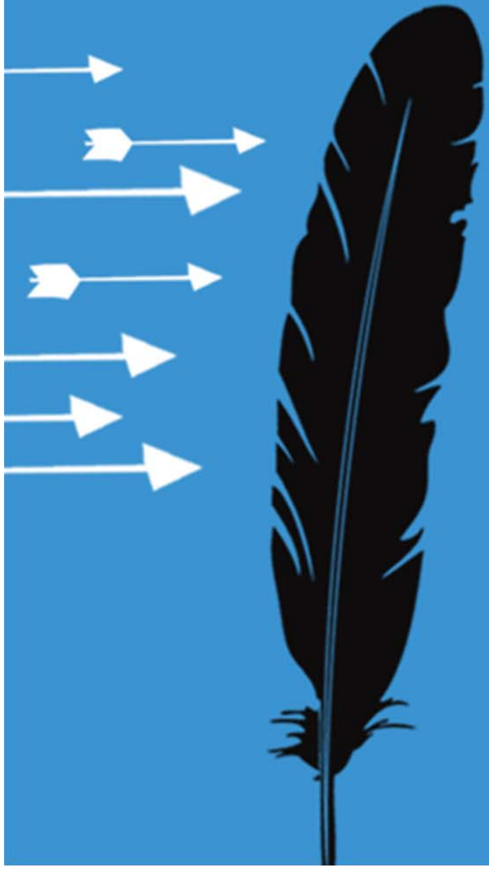
1. **Current Working Directory (CWD)**
2. **C:\Windows\System32**
3. **C:\Windows\System**
4. **C:\Windows**
5. **PATH**

Initial Research

- Extended scope: Launching EXEs
- Improved attack vector: WebDAV
- 200+ Windows apps = 500+ binary planting bugs
- Guidelines for developers, administrators
  - www.binaryplanting.com/guidelinesDevelopers.htm
  - www.binaryplanting.com/guidelinesAdministrators.htm
- Free Online Binary Planting Exposure Test
  - www.binaryplanting.com/test.htm

Advanced Research

- COM-Servers, “special folders”
- Setting CWD through IE
- Exploits
  - IE8 on Windows XP – two clicks on a web site
  - IE9 on Windows 7 – right click, add to archive
- File planting
  - Java - **`.hotspotrc`** planting
  - Chrome - **`pkcs11.txt`** planting



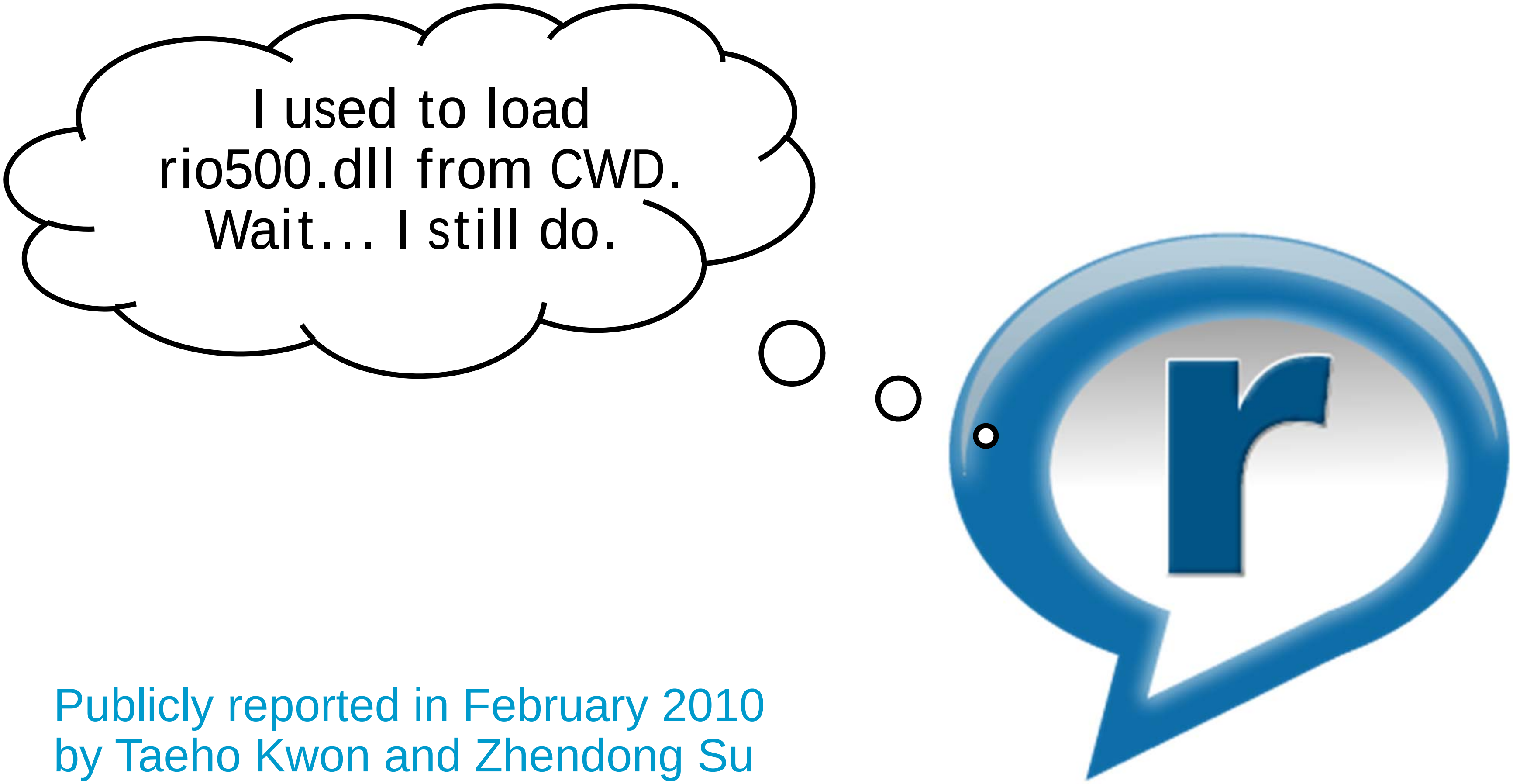
Persistence In Software

"The bug that just won't go away"

Microsoft (Sysinternals) Process Monitor

1. Filter = “Path Contains <our-path>”
2. Launch Application
3. Exclude irrelevant activities
4. Look for DLL and EXE accesses
5. Plant DLL/EXE
6. Re-launch Application
7. If successful, see call stack

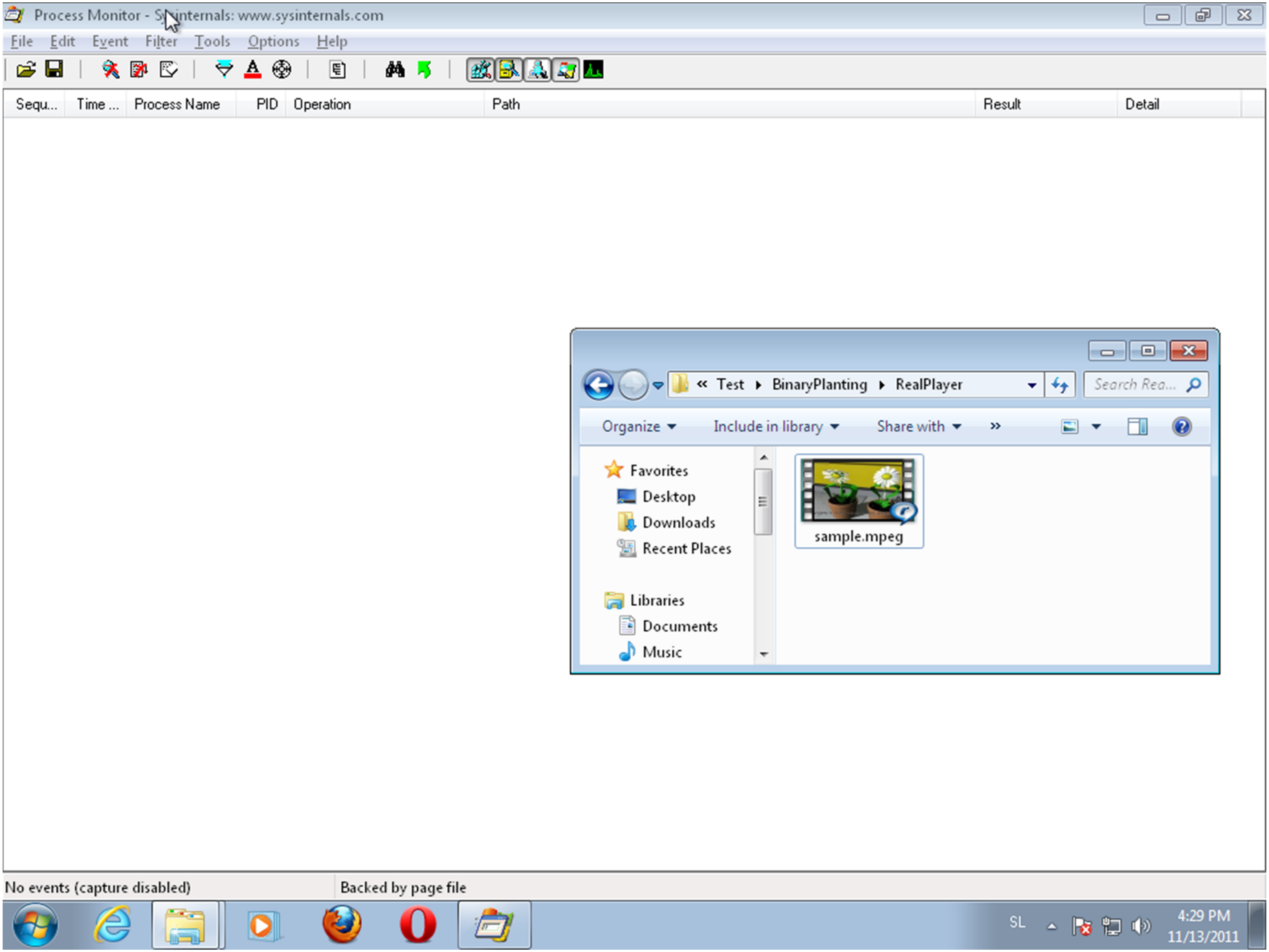
Case Study #1: Real Player



I used to load rio500.dll from CWD. Wait… I still do.

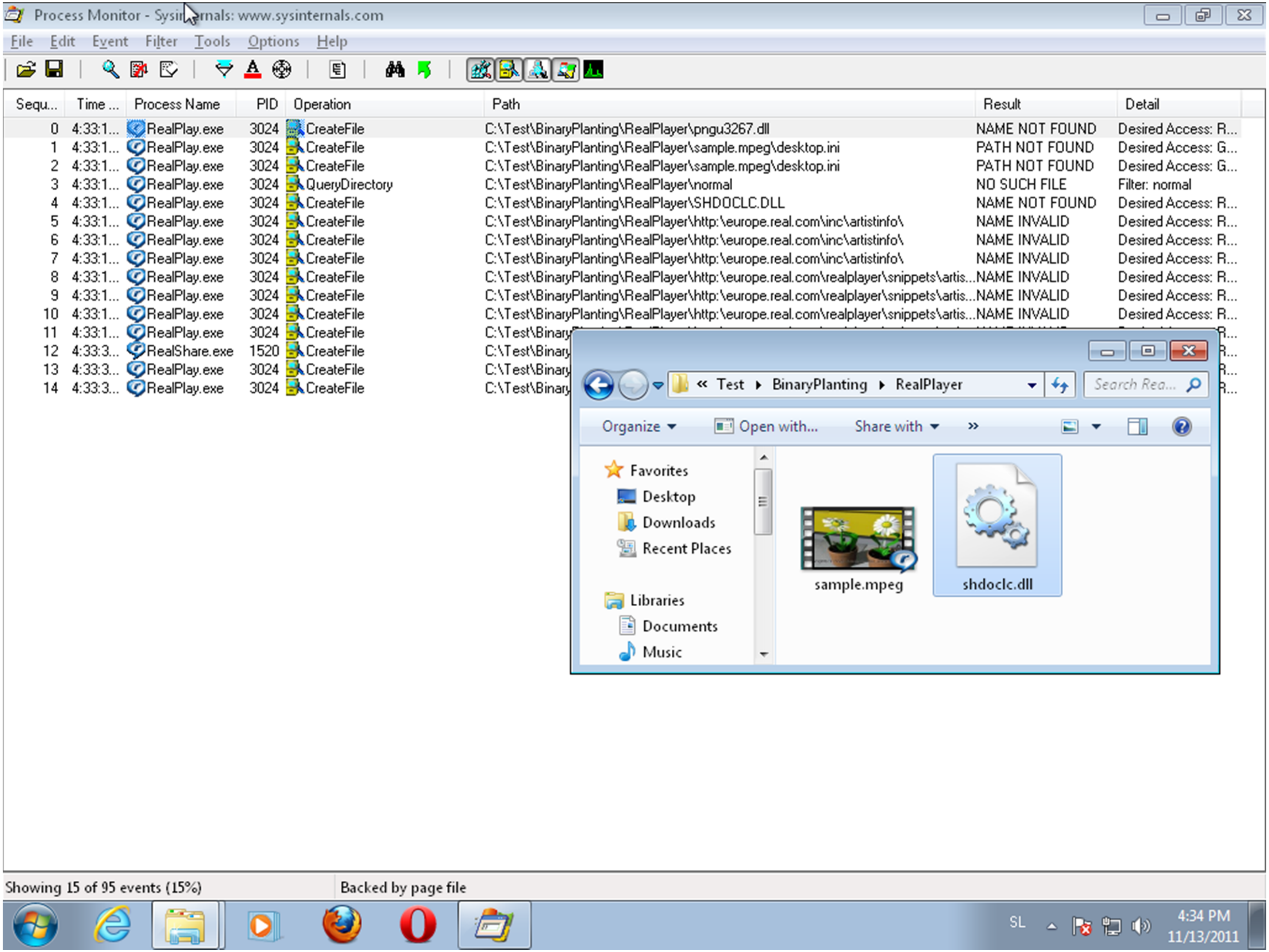
Publicly reported in February 2010
by Taeho Kwon and Zhendong Su

http://www.cs.ucdavis.edu/research/tech-reports/2010/CSE-2010-2.pdf


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Sequ... Time ... Process Name PID Operation Path Result Detail
« Test ▸ BinaryPlanting ▸ RealPlayer
Search Rea...
Organize ▾ Include in library ▾ Share with ▾ »
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
sample.mpeg
SL
4:29 PM
11/13/2011

No events (capture disabled) Backed by page file

False Positives



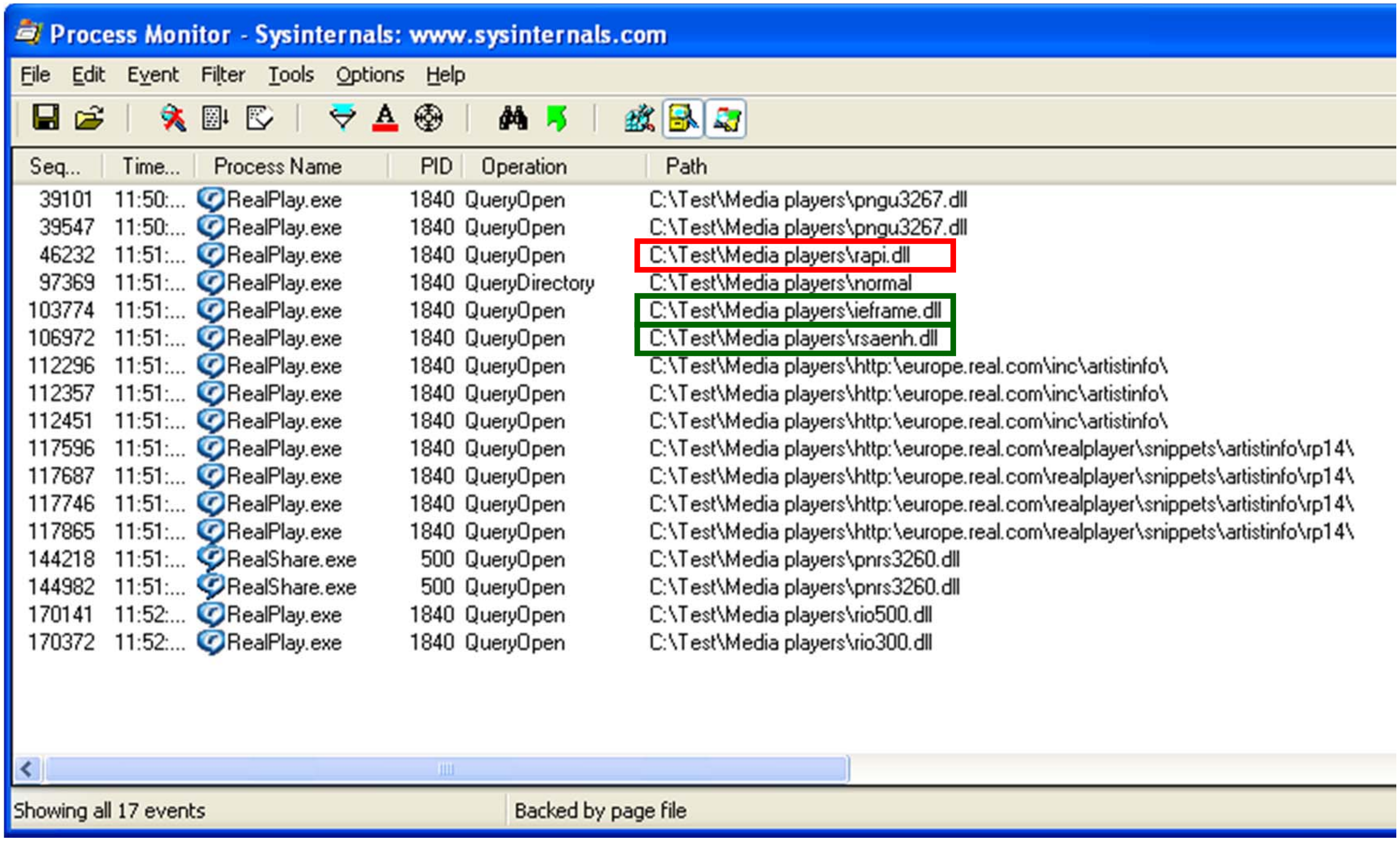
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Sequ...	Time ...	Process Name	PID	Operation	Path	Result	Detail
0	4:33:1...	RealPlay.exe	3024	CreateFile	C:\Test\BinaryPlanting\RealPlayer\pngu3267.dll	NAME NOT FOUND	Desired Access: R...
1	4:33:1...	RealPlay.exe	3024	CreateFile	C:\Test\BinaryPlanting\RealPlayer\sample.mpeg\desktop.ini	PATH NOT FOUND	Desired Access: G...
2	4:33:1...	RealPlay.exe	3024	CreateFile	C:\Test\BinaryPlanting\RealPlayer\sample.mpeg\desktop.ini	PATH NOT FOUND	Desired Access: G...
3	4:33:1...	RealPlay.exe	3024	QueryDirectory	C:\Test\BinaryPlanting\RealPlayer\normal	NO SUCH FILE	Filter: normal
4	4:33:1...	RealPlay.exe	3024	CreateFile	C:\Test\BinaryPlanting\RealPlayer\SHDOCLC.DLL	NAME NOT FOUND	Desired Access: R...
5	4:33:1...	RealPlay.exe	3024	CreateFile	C:\Test\BinaryPlanting\RealPlayer\http:\europe.real.com\inc\artistinfo\	NAME INVALID	Desired Access: R...
6	4:33:1...	RealPlay.exe	3024	CreateFile	C:\Test\BinaryPlanting\RealPlayer\http:\europe.real.com\inc\artistinfo\	NAME INVALID	Desired Access: R...
7	4:33:1...	RealPlay.exe	3024	CreateFile	C:\Test\BinaryPlanting\RealPlayer\http:\europe.real.com\inc\artistinfo\	NAME INVALID	Desired Access: R...
8	4:33:1...	RealPlay.exe	3024	CreateFile	C:\Test\BinaryPlanting\RealPlayer\http:\europe.real.com\realplayer\snippets\artis...	NAME INVALID	Desired Access: R...
9	4:33:1...	RealPlay.exe	3024	CreateFile	C:\Test\BinaryPlanting\RealPlayer\http:\europe.real.com\realplayer\snippets\artis...	NAME INVALID	Desired Access: R...
10	4:33:1...	RealPlay.exe	3024	CreateFile	C:\Test\BinaryPlanting\RealPlayer\http:\europe.real.com\realplayer\snippets\artis...	NAME INVALID	Desired Access: R...
11	4:33:1...	RealPlay.exe	3024	CreateFile	C:\Test\Binary		R...
12	4:33:3...	RealShare.exe	1520	CreateFile	C:\Test\Binary		R...
13	4:33:3...	RealPlay.exe	3024	CreateFile	C:\Test\Binary		R...
14	4:33:3...	RealPlay.exe	3024	CreateFile	C:\Test\Binary		R...

Showing 15 of 95 events (15%)

Backed by page file

Real Player on Windows XP (mpeg)

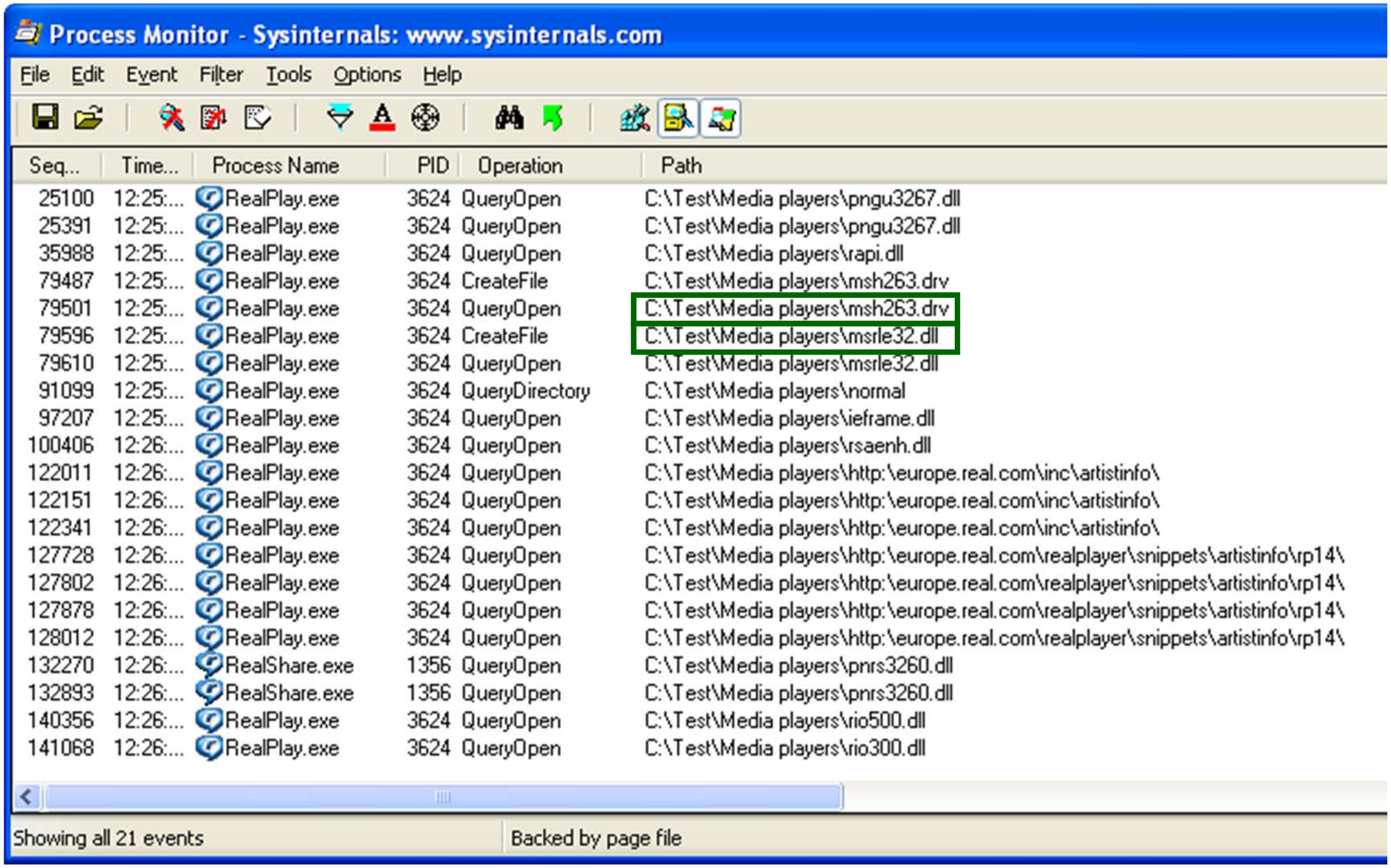

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Seq...	Time...	Process Name	PID	Operation	Path
39101	11:50:...	RealPlay.exe	1840	QueryOpen	C:\Test\Media players\pngu3267.dll
39547	11:50:...	RealPlay.exe	1840	QueryOpen	C:\Test\Media players\pngu3267.dll
46232	11:51:...	RealPlay.exe	1840	QueryOpen	C:\Test\Media players\rapi.dll
97369	11:51:...	RealPlay.exe	1840	QueryDirectory	C:\Test\Media players\normal
103774	11:51:...	RealPlay.exe	1840	QueryOpen	C:\Test\Media players\ieframe.dll
106972	11:51:...	RealPlay.exe	1840	QueryOpen	C:\Test\Media players\rsaenh.dll
112296	11:51:...	RealPlay.exe	1840	QueryOpen	C:\Test\Media players\http:\europe.real.com\inc\artistinfo\
112357	11:51:...	RealPlay.exe	1840	QueryOpen	C:\Test\Media players\http:\europe.real.com\inc\artistinfo\
112451	11:51:...	RealPlay.exe	1840	QueryOpen	C:\Test\Media players\http:\europe.real.com\inc\artistinfo\
117596	11:51:...	RealPlay.exe	1840	QueryOpen	C:\Test\Media players\http:\europe.real.com\realplayer\snippets\artistinfo\rp14\
117687	11:51:...	RealPlay.exe	1840	QueryOpen	C:\Test\Media players\http:\europe.real.com\realplayer\snippets\artistinfo\rp14\
117746	11:51:...	RealPlay.exe	1840	QueryOpen	C:\Test\Media players\http:\europe.real.com\realplayer\snippets\artistinfo\rp14\
117865	11:51:...	RealPlay.exe	1840	QueryOpen	C:\Test\Media players\http:\europe.real.com\realplayer\snippets\artistinfo\rp14\
144218	11:51:...	RealShare.exe	500	QueryOpen	C:\Test\Media players\pnrs3260.dll
144982	11:51:...	RealShare.exe	500	QueryOpen	C:\Test\Media players\pnrs3260.dll
170141	11:52:...	RealPlay.exe	1840	QueryOpen	C:\Test\Media players\rio500.dll
170372	11:52:...	RealPlay.exe	1840	QueryOpen	C:\Test\Media players\rio300.dll

Showing all 17 events

Backed by page file

Real Player on Windows XP (avi)


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

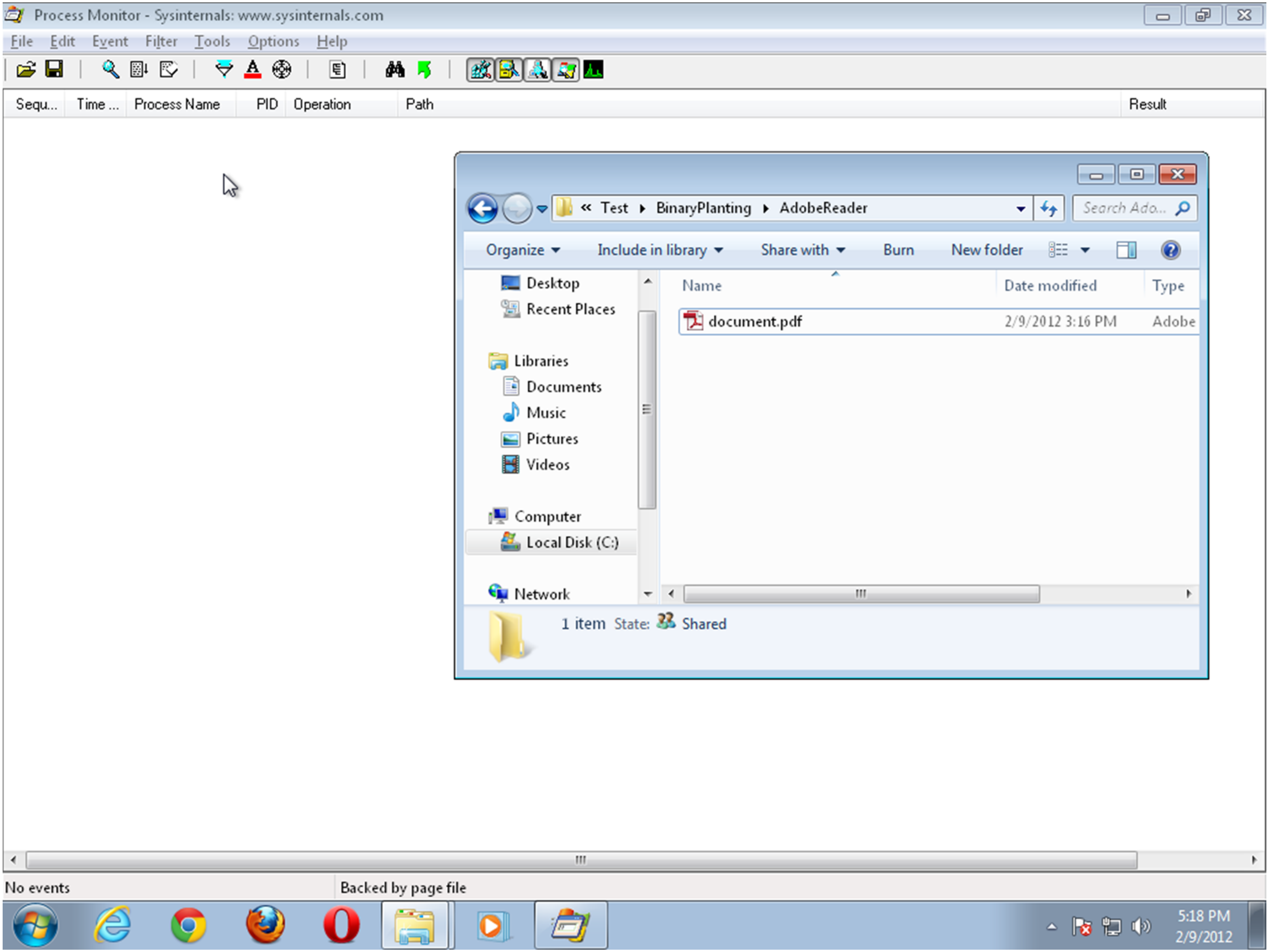
Seq...	Time...	Process Name	PID	Operation	Path
25100	12:25:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\pngu3267.dll
25391	12:25:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\pngu3267.dll
35988	12:25:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\rapi.dll
79487	12:25:...	RealPlay.exe	3624	CreateFile	C:\Test\Media players\msh263.drv
79501	12:25:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\msh263.drv
79596	12:25:...	RealPlay.exe	3624	CreateFile	C:\Test\Media players\msrle32.dll
79610	12:25:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\msrle32.dll
91099	12:25:...	RealPlay.exe	3624	QueryDirectory	C:\Test\Media players\normal
97207	12:25:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\ieframe.dll
100406	12:26:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\rsaenh.dll
122011	12:26:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\http:\europe.real.com\inc\artistinfo\
122151	12:26:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\http:\europe.real.com\inc\artistinfo\
122341	12:26:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\http:\europe.real.com\inc\artistinfo\
127728	12:26:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\http:\europe.real.com\realplayer\snippets\artistinfo\rp14\
127802	12:26:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\http:\europe.real.com\realplayer\snippets\artistinfo\rp14\
127878	12:26:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\http:\europe.real.com\realplayer\snippets\artistinfo\rp14\
128012	12:26:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\http:\europe.real.com\realplayer\snippets\artistinfo\rp14\
132270	12:26:...	RealShare.exe	1356	QueryOpen	C:\Test\Media players\pnrs3260.dll
132893	12:26:...	RealShare.exe	1356	QueryOpen	C:\Test\Media players\pnrs3260.dll
140356	12:26:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\rio500.dll
141068	12:26:...	RealPlay.exe	3624	QueryOpen	C:\Test\Media players\rio300.dll

Showing all 21 events

Backed by page file

Case Study #2: Adobe Reader

I'm doing a very good job with DLLs, but I hear there's an EXE planting there.



Process Monitor - Sysinternals: www.sysinternals.com

Sequ...	Time ...	Process Name	PID	Operation	Path	Result

« Test ▸ BinaryPlanting ▸ AdobeReader

Name	Date modified	Type
document.pdf	2/9/2012 3:16 PM	Adobe

1 item State: Shared

No events

Backed by page file

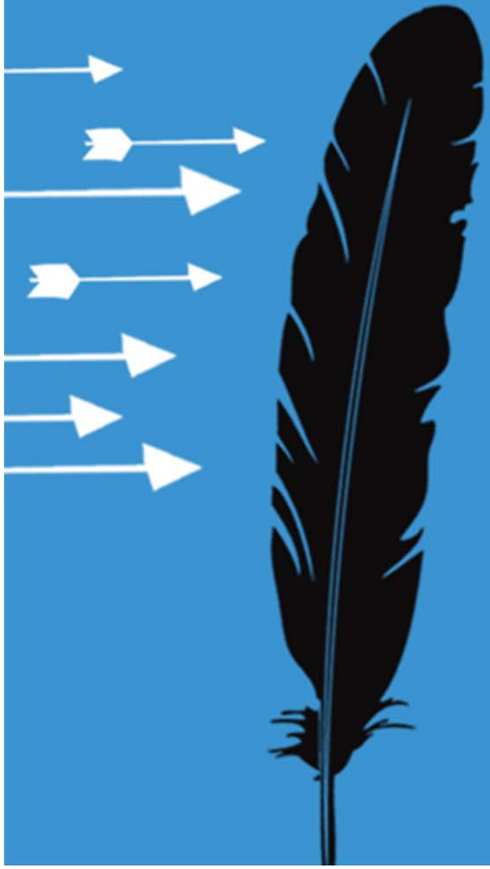
Binary Planting Issues Found

Real Player

1. WinXP: RealPlay.exe loading planted rapi.dll upon startup
2. Win7: RealPlay.exe loading planted SHDOCLC.DLL upon startup
3. RealPlay.exe loading planted rio500.dll upon exit
4. RealPlay.exe loading planted rio300.dll upon exit
5. RealShare.exe loading planted pnrs3260.dll upon startup

Adobe Reader

6. AcroRd32.exe loading planted msiexec.exe (outside sandbox) upon reparing the Reader installation



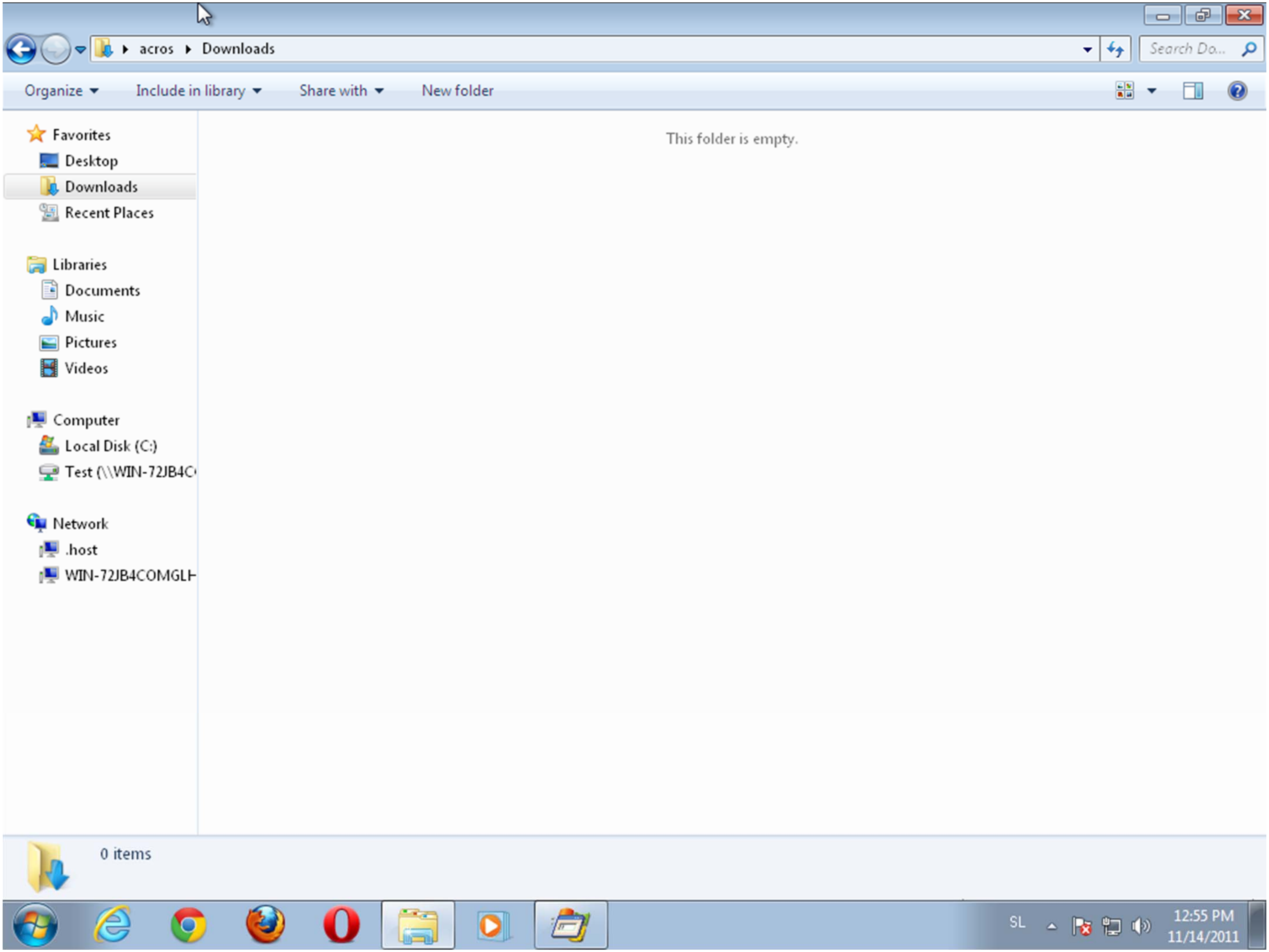
Persistence On Computer

Plant Once, Exploit Many Times

DLL Search Order

```
LoadLibrary(“SomeLib.dll”)
```

1. The directory from which the application loaded
2. C:\Windows\System32
3. C:\Windows\System
4. C:\Windows
5. Current Working Directory (CWD)
6. PATH

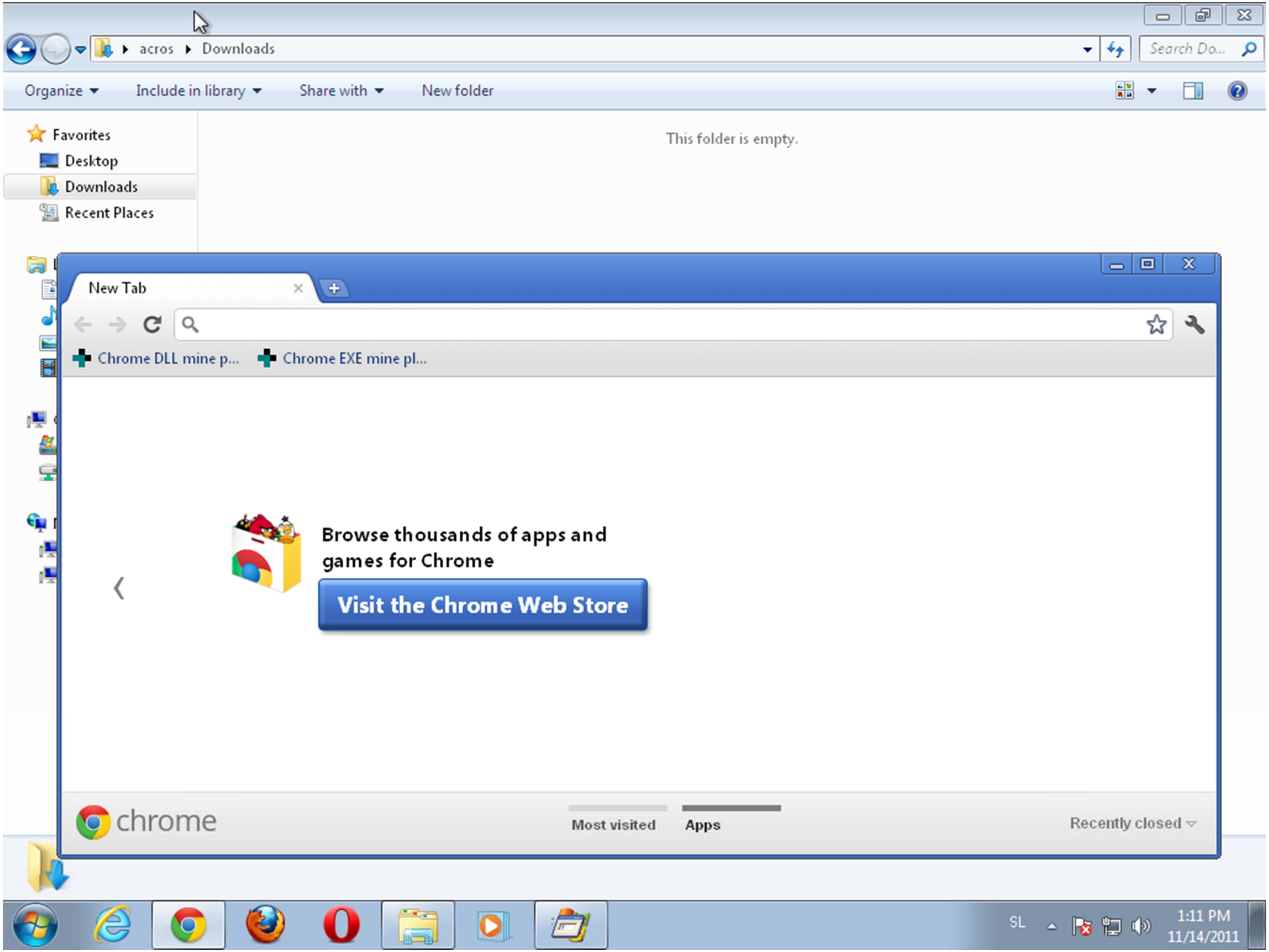


This folder is empty.

0 items

Turning the Downloads Folder into a DLL Mine Field

(Original Clickjacking Remix)

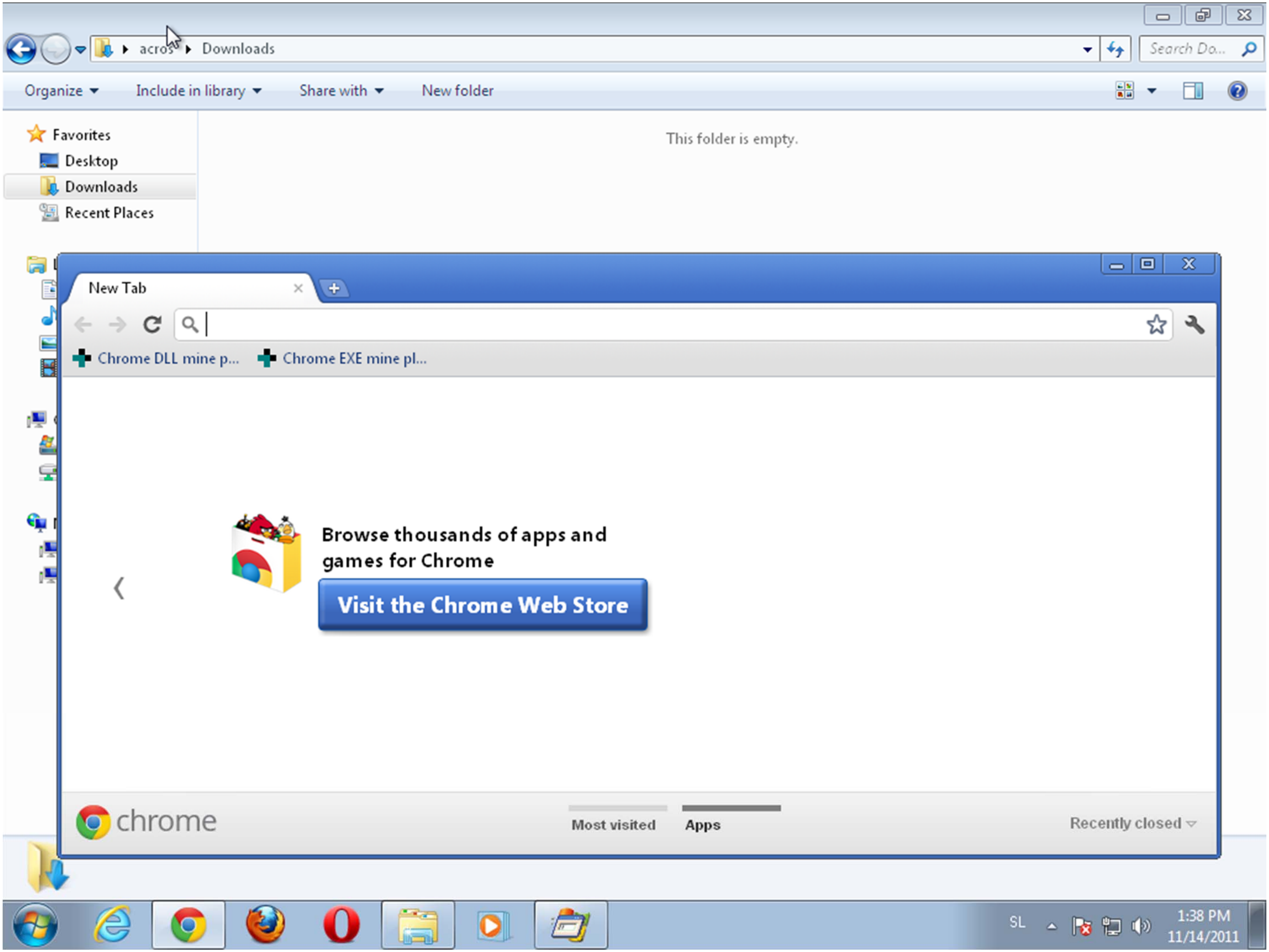


This folder is empty.

Browse thousands of apps and games for Chrome

Turning the Downloads Folder into an EXE Mine Field

("Ask no questions")



This folder is empty.

Browse thousands of apps and games for Chrome

Advanced Persistent Benefits

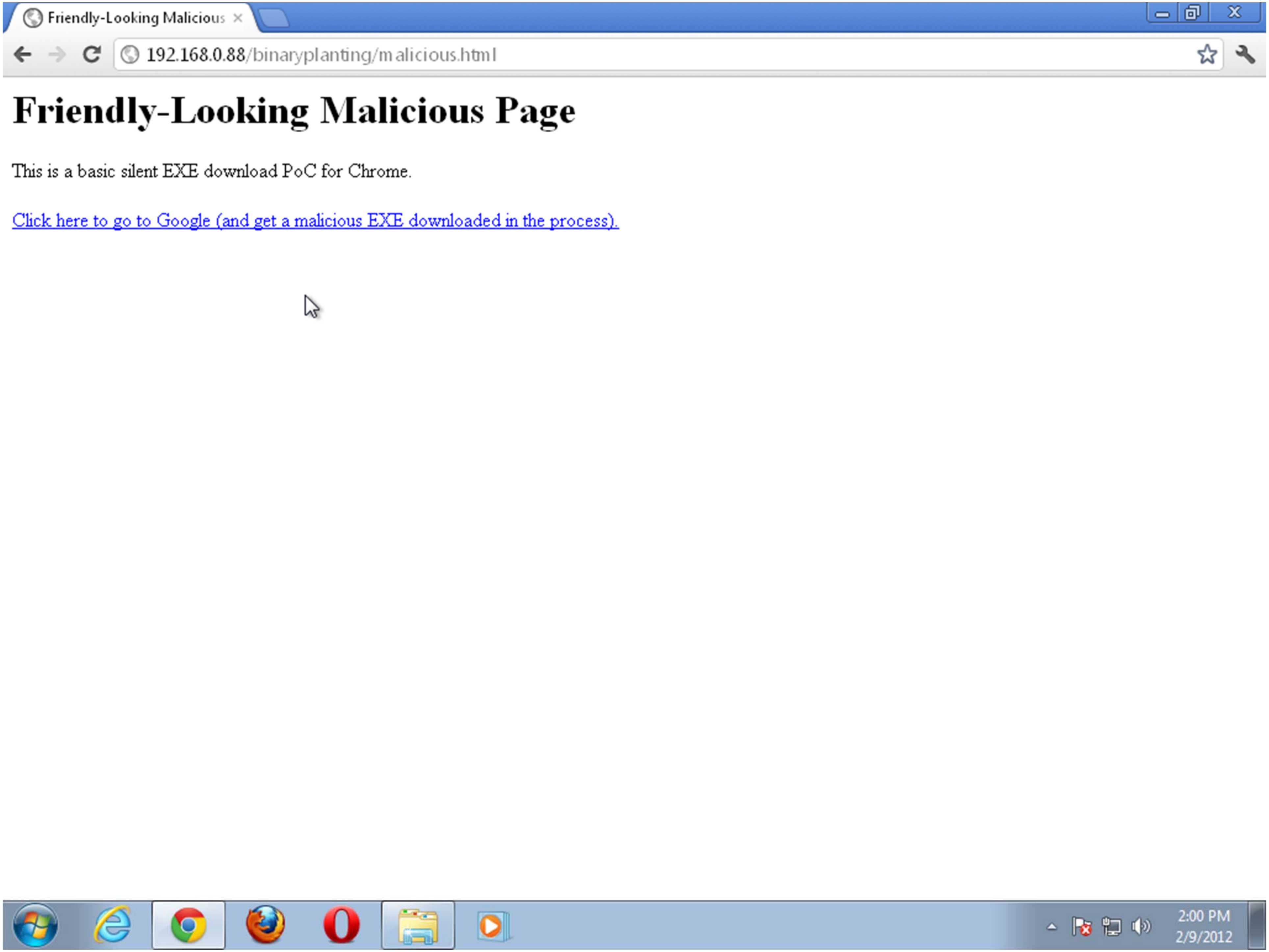
- Persistent – “download today, exploit later”
- Survives browser switching
- Installers get elevated privileges when asked
- No dependence on current working directory
- Fully automated

“Credits”

- Installers loading DLLs from their neighborhood
- InstallShield calls “msiexec.exe” without full path
- Browsers keep downloads until manually deleted
- Browsers share the Downloads folder
- Chrome download clickjackable
- Chrome EXE download fully automated

Two Plus Two Is… An Attack Scenario

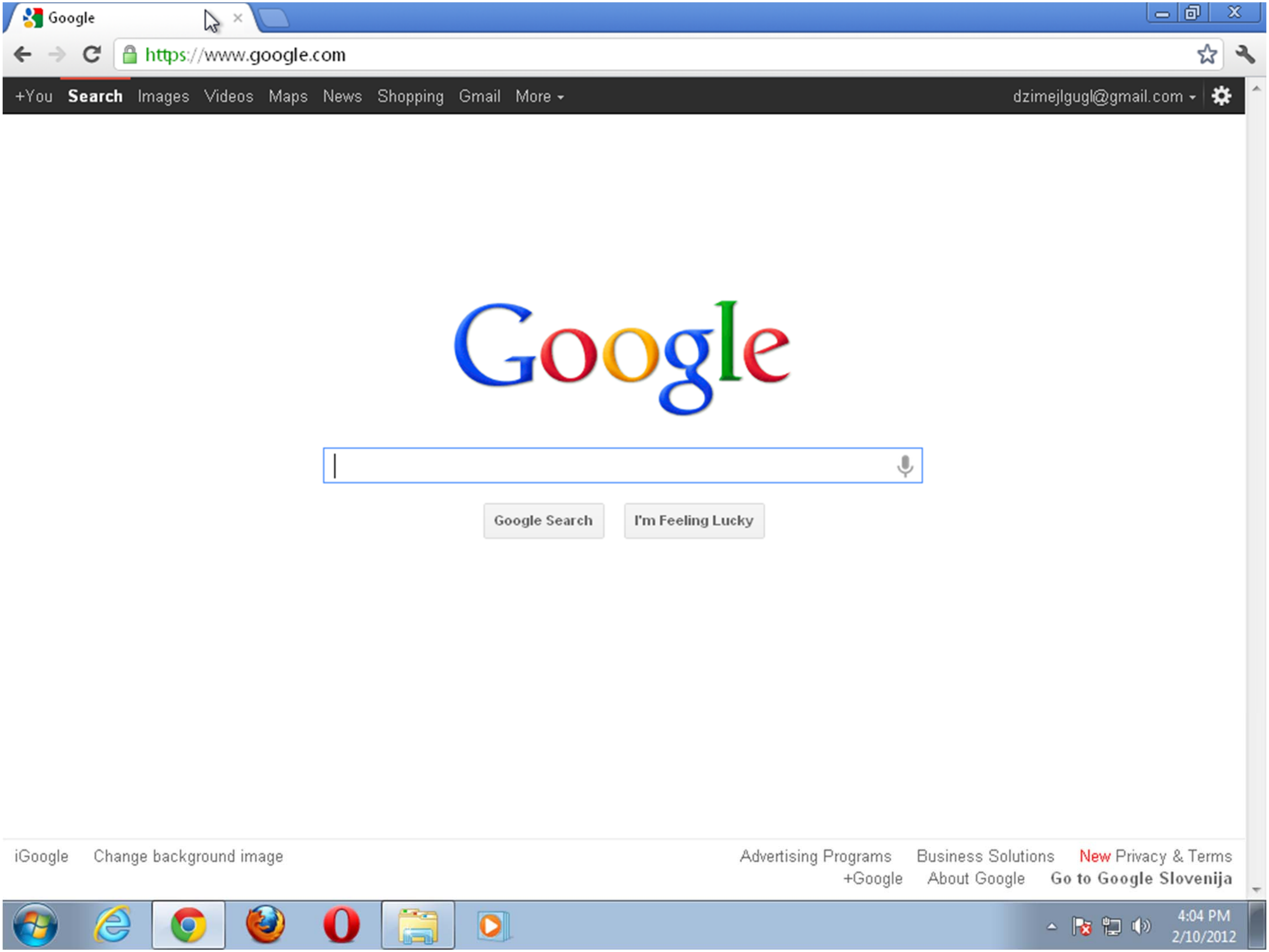
(“Chrome, Reader, GMail and a pinch of curiosity”)


Friendly-Looking Malicious
192.168.0.88/binaryplanting/malicious.html
2:00 PM
2/9/2012

Friendly-Looking Malicious Page

This is a basic silent EXE download PoC for Chrome.

Click here to go to Google (and get a malicious EXE downloaded in the process).


Google
https://www.google.com
+You
Search
Images
Videos
Maps
News
Shopping
Gmail
More
dzimejlgugl@gmail.com
Google
Google Search
I'm Feeling Lucky
iGoogle
Change background image
Advertising Programs
Business Solutions
New Privacy & Terms
+Google
About Google
Go to Google Slovenija
4:04 PM
2/10/2012

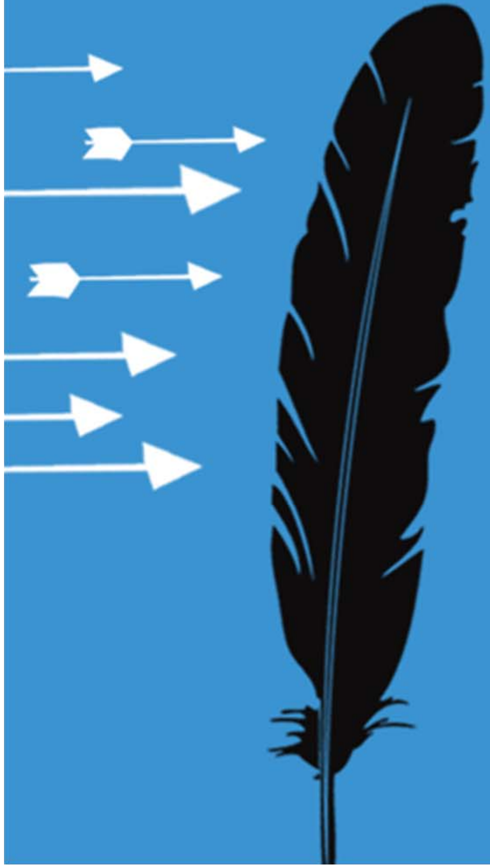
De-mining The Downloads Folder

Browser Vendors

- Use modified names of all downloaded files cryptbase(0).dll, msiexec(0).exe
- Put downloaded files in individual subfolders
- No automatic downloads (doh)
- Make download process non-clickjackable

Users

- Manually clear the Downloads folder
- msiexec.exe, cryptbase.dll, ... can mean you were attacked
- Plant your own benign msiexec.exe and DLLs



Apply *This*

Save The Planet, Plant a Binary

Researchers

Researchers: Efficiency

Staying current

- Make sure you're working with the latest version of the product
- Make sure your O/S is up to date

Environmental variety

- Different O/S, Different DLLs, different drivers, codecs...

Data variety

- Different formats, file extensions, different content

Researchers: Check Your Claims

Make no assumptions

- Not every LoadImage is a hit
- ShellExecute will issue a security warning when launching from a share
- Code signing can be a deal-breaker (but not necessarily)

Don’t blame the butler

- Check call stack to find which module is responsible for the bug, then check the module’s details to find the author

Developers

Developers: Code Safely

Use only absolute paths

- LoadLibrary(“relative.dll”) - FAIL
- CreateProcess(“notepad.exe”) – FAIL
- ShellExecute(“cmd.exe”) - FAIL

CWD usage

- Set CWD to a safe location, quickly
- Call SetDllDirectory(“”)
- SetDefaultDllDirectories, AddDllDirectory and RemoveDllDirectory

Developers: Monitor Your App

Observe file system operations

- On all supported O/S versions
- Different drivers, codecs etc.

Maximize execution coverage

- Different formats, file extensions, different content
- Try all test cases

Pentesters

Pentesters

Just-in-time binary planting

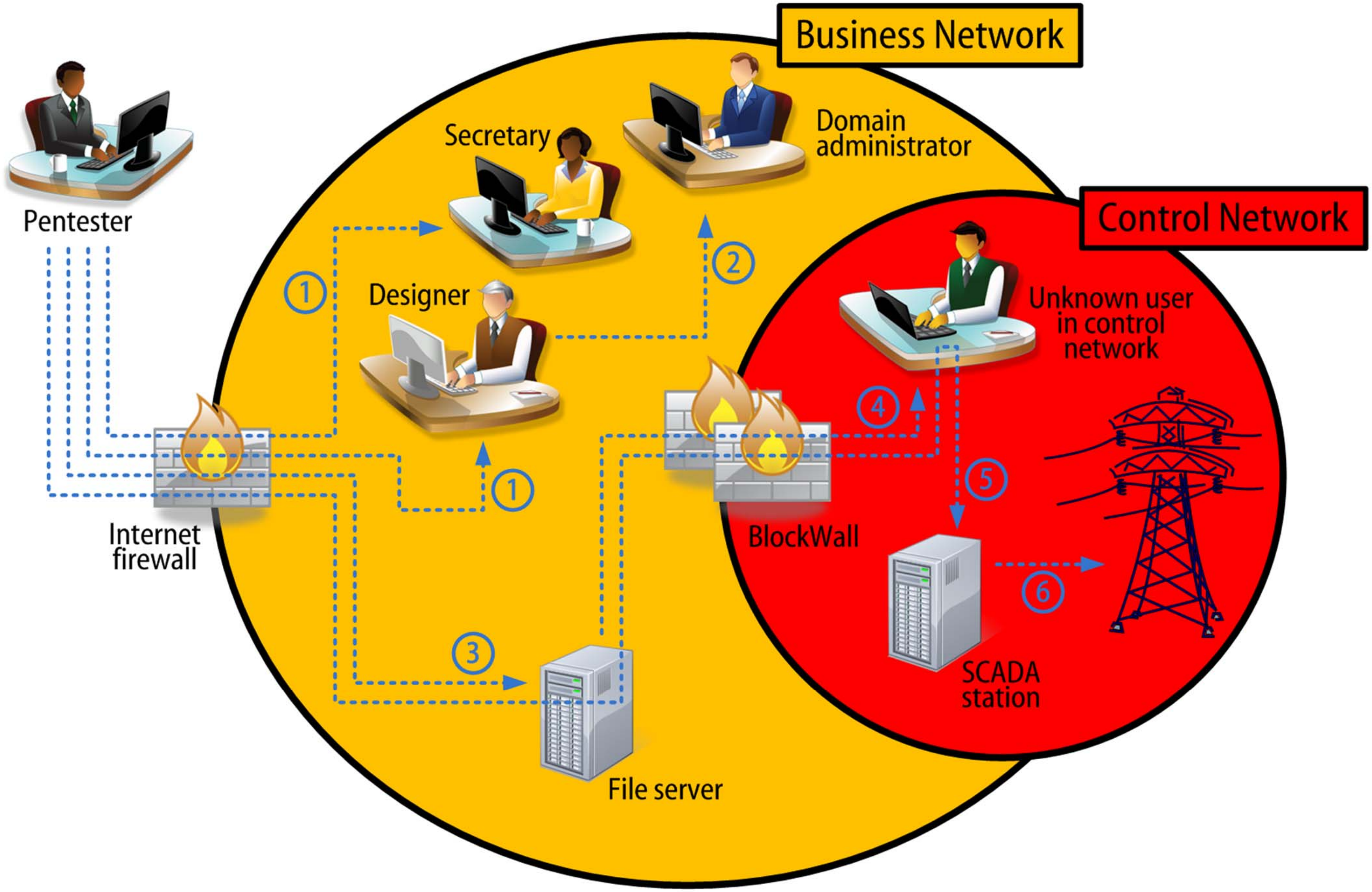
- Find vulns where and when you need them

Usage

- Entering the target network
- Becoming local/domain administrator
- Propagating inside the target network
- Advanced: “blind binary planting”

Keep it simple

- Forget DLL proxying, users are used to apps crashing


Business Network
Control Network
Pentester
Secretary
Domain administrator
Designer
Unknown user in control network
Internet firewall
BlockWall
File server
SCADA station
1
1
2
3
4
5
6

Resources

Tools

- Microsoft / Sysinternals Process Monitor
- Windows Debugging Symbols

Files

- 32 bit DLL: www.binaryplanting.com/demo/malicious32.dll
- 64 bit DLL: www.binaryplanting.com/demo/malicious64.dll
- EXE: calc.exe (what else?)

Knowledge

- www.binaryplanting.com
- blog.acrossecurity.com
- PenTest Magazine August 2011 (http://pentestmag.com/august-issue-pentesting-in-the-cloud/)

Plant Your Questions

Mitja Kolsek

ACROS

www.acrossecurity.com
mitja.kolsek@acrossecurity.com
@acrossecurity
@mkolsek