Advanced (Persistent) Binary Planting

Mitja Kolsek
ACROS

Today's Menu

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

acros

RSACONFERENCE2012

Binary Planting Quick Summary

DLL hijacking, DLL preloading, Insecure library loading, …
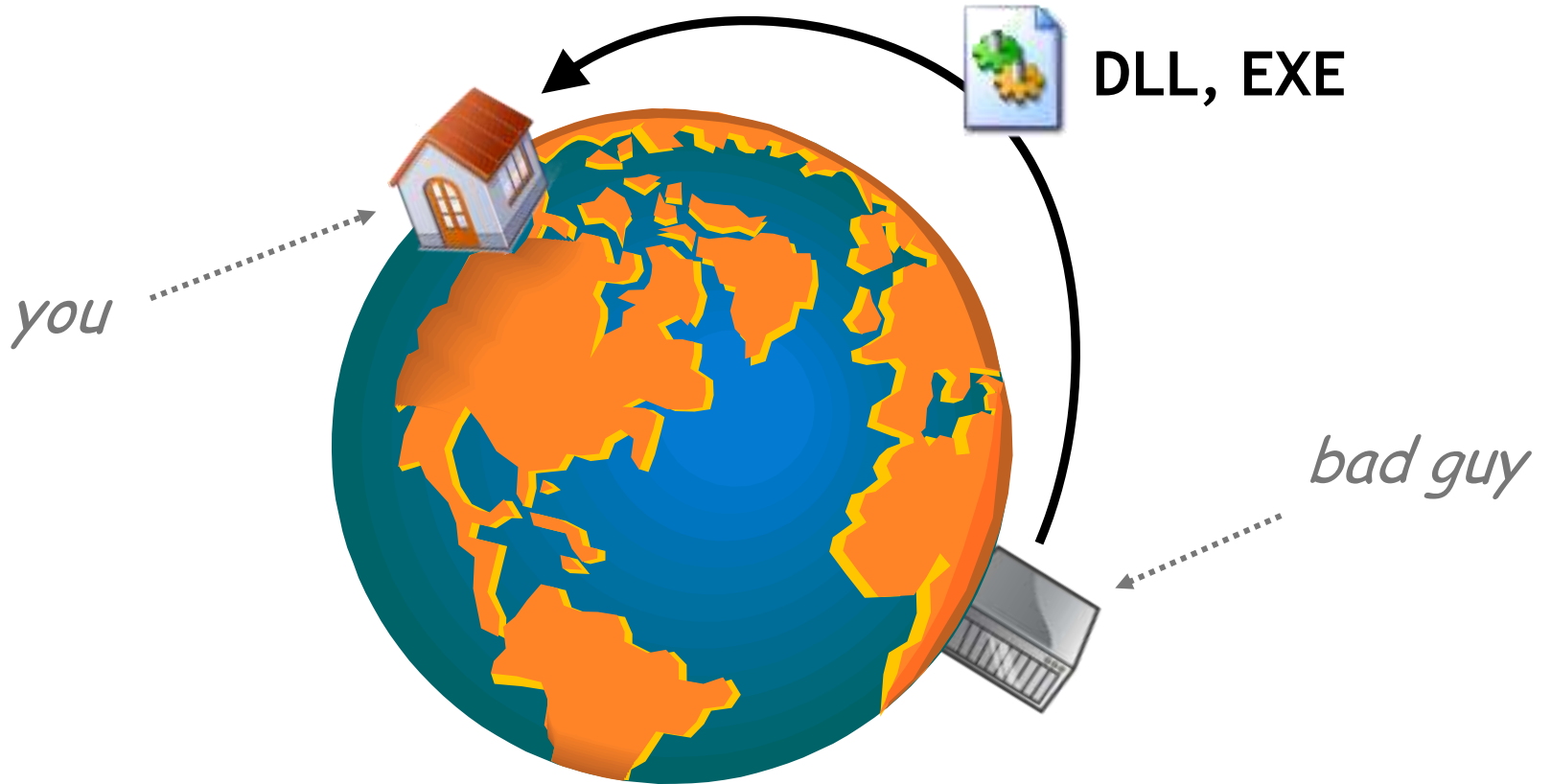
DLL, EXE

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

RSΛCONFERENCE2012

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

acros

RSACONFERENCE2012

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"

RSACONFERENCE**2012**

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
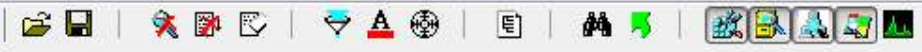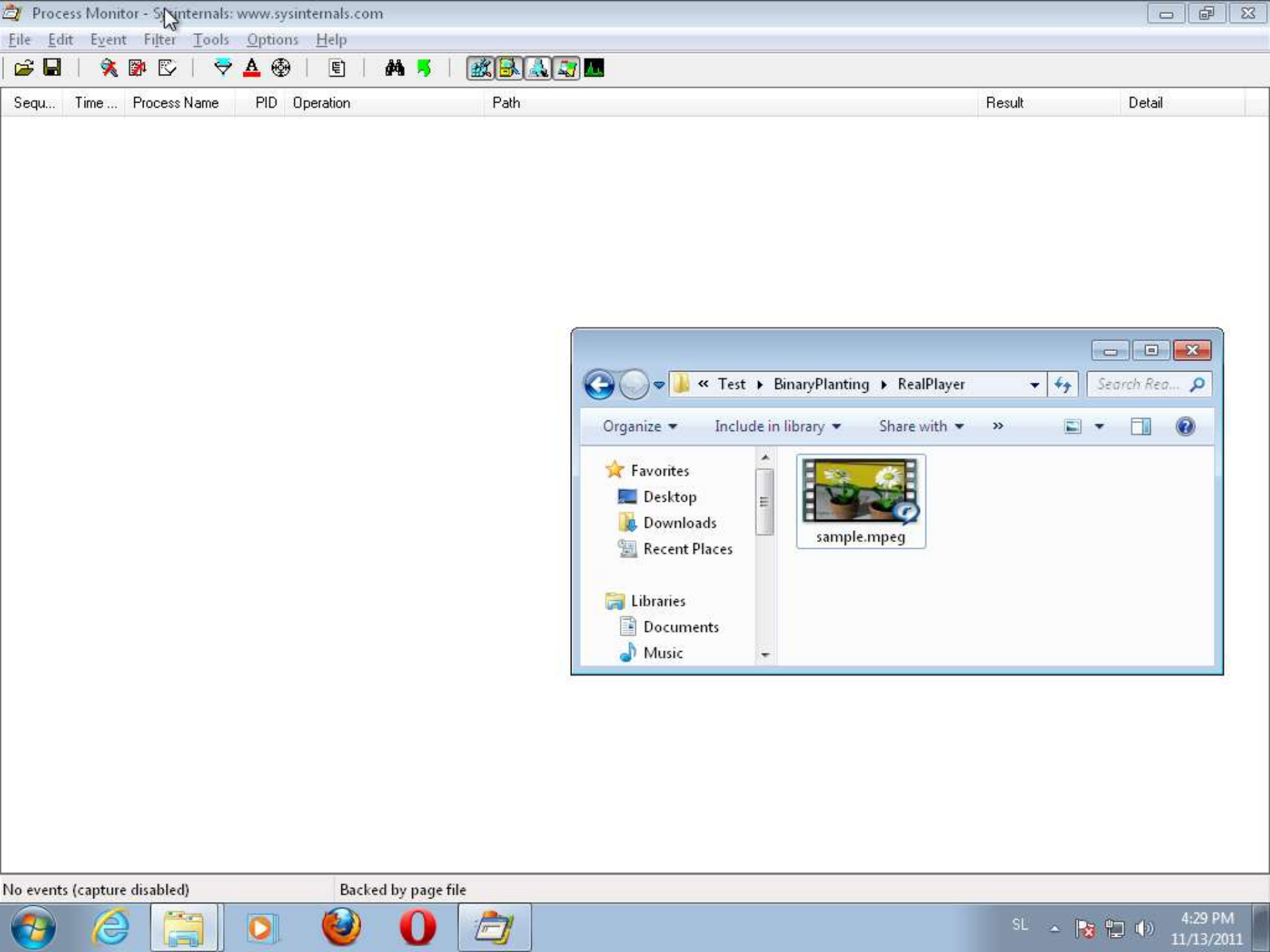6. Re-launch Application
7. If successful, see call stack

RSACONFERENCE2012

Case Study #1: Real Player
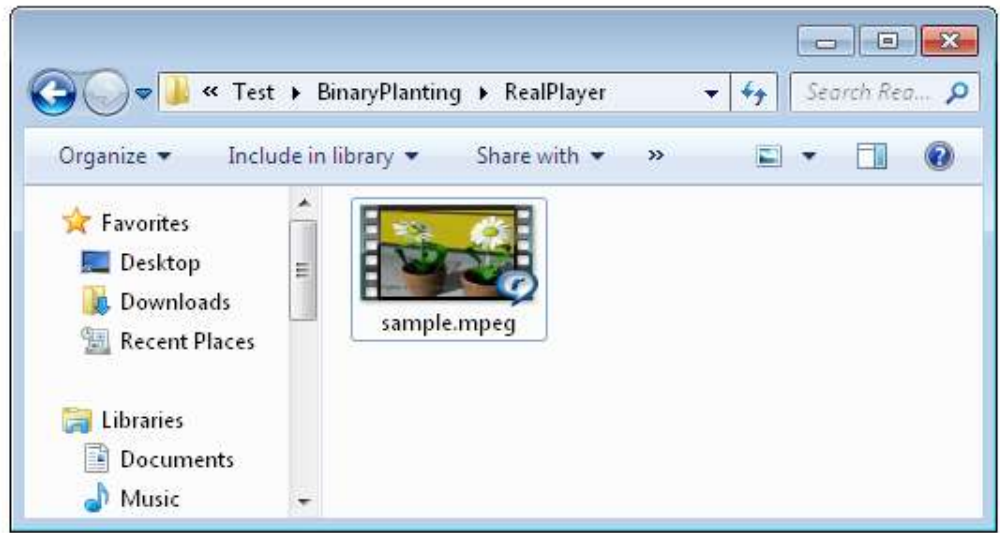
I used to load rio500.dll from CWD. Wait... I still do.

Publicly reported in February 2010 by Taeho Kwon and Zhendong Su

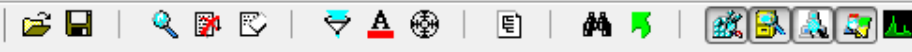http://www.cs.ucdavis.edu/research/tech-reports/2010/CSE-2010-2.pdf

acros

RSACONFERENCE2012

File   Edit   Event   Filter   Tools   Options   Help

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

No events (capture disabled)   Backed by page file

« Test ▸ BinaryPlanting ▸ RealPlayer

Organize ▾   Include in library ▾   Share with ▾   »

Search Rea...

★ Favorites
  🖥 Desktop
  ⬇ Downloads
  📍 Recent Places

📚 Libraries
  📄 Documents
  🎵 Music

sample.mpeg

SL   4:29 PM
          11/13/2011

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...		
12	4:33:3...	RealShare.exe	1520	CreateFile	C:\Test\Binary...		
13	4:33:3...	RealPlay.exe	3024	CreateFile	C:\Test\Binary...		
14	4:33:3...	RealPlay.exe	3024	CreateFile	C:\Test\Binary...		

‹‹ Test ▸ BinaryPlanting ▸ RealPlayer

Search Rea...

Organize ▾   Open with...   Share with ▾   »

Favorites
  Desktop
  Downloads
  Recent Places

Libraries
  Documents
  Music

sample.mpeg   shdoclc.dll

Showing 15 of 95 events (15%)   Backed by page file

SL   4:34 PM   11/13/2011

Real Player on Windows XP (mpeg)

Real Player on Windows XP (avi)

Case Study #2: Adobe Reader
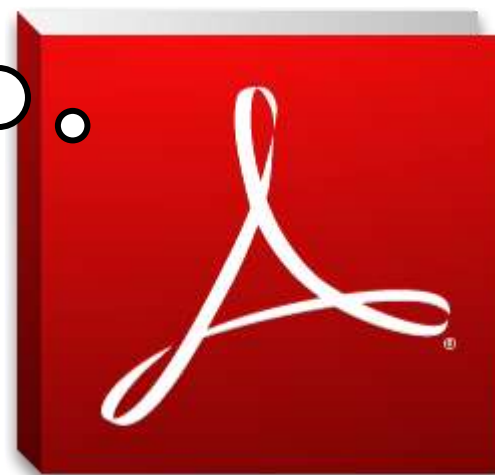
File Edit Event Filter Tools Options Help

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

Test ▸ BinaryPlanting ▸ AdobeReader

Search Ado...

Organize ▾   Include in library ▾   Share with ▾   Burn   New folder

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

- Desktop
- Recent Places

- Libraries
  - Documents
  - Music
  - Pictures
  - Videos

- Computer
  - Local Disk (C:)

- Network

1 item State: 👥 Shared

No events   Backed by page file

5:18 PM
2/9/2012

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

acros

RSACONFERENCE2012

Persistence On Computer

Plant Once, Exploit Many Times

RSACONFERENCE2012

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.

acros ▸ Downloads

Organize ▾   Include in library ▾   Share with ▾   New folder

Favorites
  Desktop
  Downloads
  Recent Places

Libraries
  Documents
  Music
  Pictures
  Videos

Computer
  Local Disk (C:)
  Test (\\WIN-72JB4C

Network
  .host
  WIN-72JB4COMGLH

Search Do...

0 items

SL   12:55 PM
      11/14/2011

Turning the Downloads Folder into a DLL Mine Field

(Original Clickjacking Remix)

Turning the Downloads Folder into an EXE Mine Field

("Ask no questions")

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

acros

"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")

acros

RSACONFERENCE2012

192.168.0.88/binaryplanting/malicious.html

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).

+You **Search** Images Videos Maps News Shopping Gmail More ▾

dzimejlgugl@gmail.com ▾

Google

Google Search   I'm Feeling Lucky

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

acros

RSACONFERENCE2012

Apply *This*

Save The Planet, Plant a Binary

RSACONFERENCE2012

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

acros

RSACONFERENCE2012

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

acros

RSACONFERENCE2012

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

acros

RSACONFERENCE2012

Pentesters

Pentesters

Just-in-time binary planting
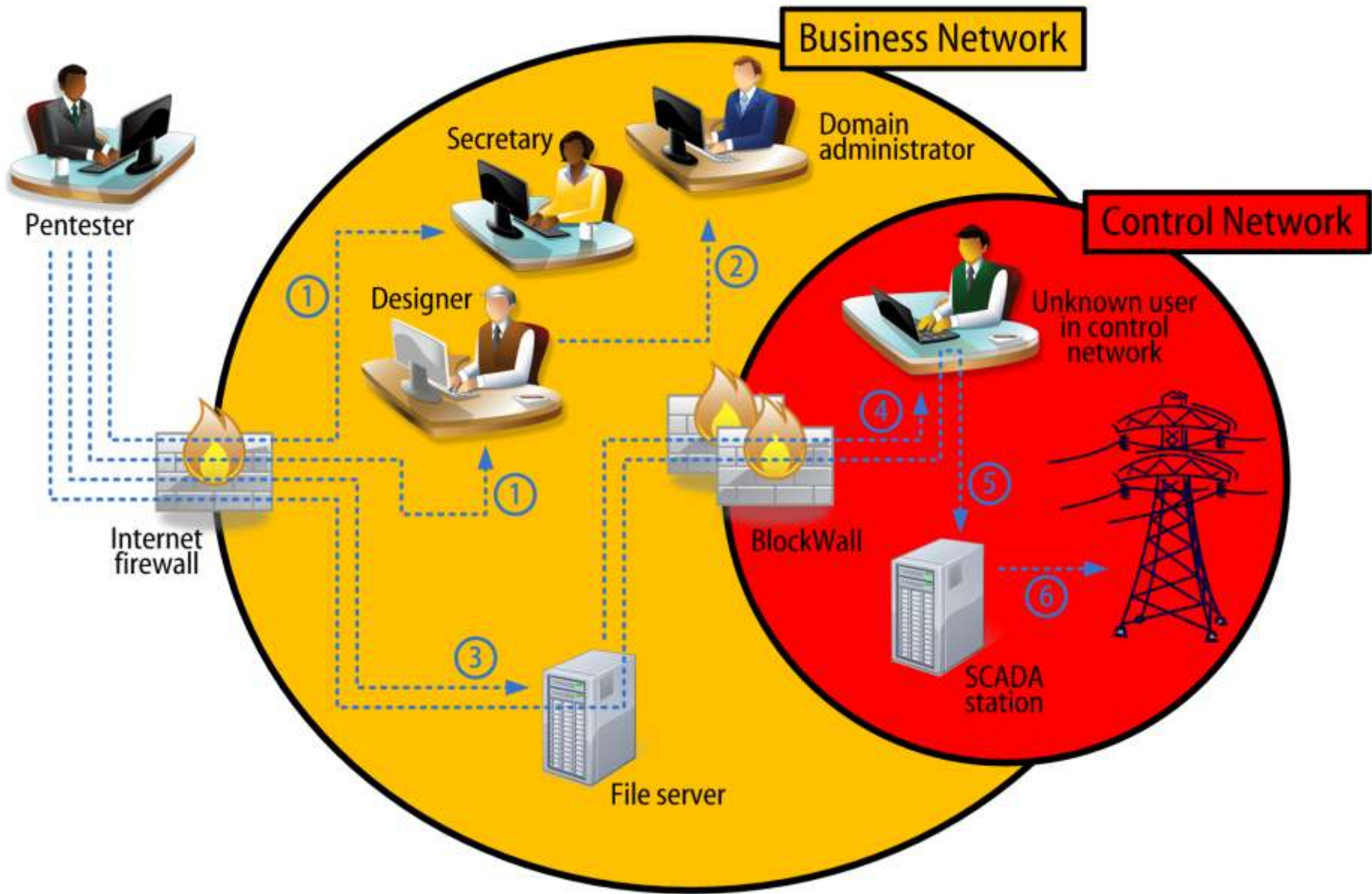
- Find vulns where and when you need them

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

RSACONFERENCE2012

acros

Business Network

Control Network

Pentester

Secretary

Domain administrator

Designer

Unknown user in control network

Internet firewall

BlockWall

SCADA station

File server

43

RSACONFERENCE2012

acros

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/)

acros

RSACONFERENCE2012

Plant Your Questions

Mitja Kolsek

ACROS

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