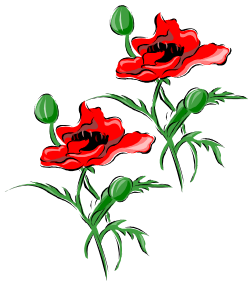


Remote Binary Planting

An Overlooked Vulnerability Affair

OWASP Maribor, 8.12.2010

Mitja Kolsek
ACROS d.o.o.
mitja.kolsek@acrossecurity.com
www.acrossecurity.com

Vulnerability Super-Star

1. Arbitrary Code Execution
2. Easy to Find
3. Easy to Exploit
4. Reliable
5. No Privileges
6. Remote
7. Works Through Firewalls

100.000.000.000

Misunderstood

Underestimated

Downplayed

Ignored

Forgotten

Quasi-Addressed

Still Ignored

Unfixed

The Life of Binary Planting

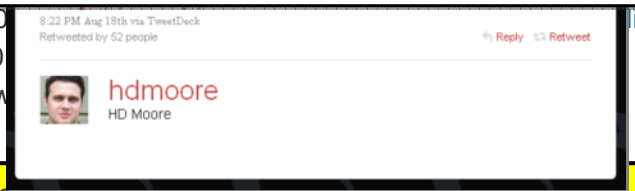
1998 NSA: Windows NT Security Guidelines

DLL Spoofing

"Double clicking on MS Office documents from Windows Explorer may execute arbitrary programs in some cases."

NSA Windows NT Security Guidelines 105 18. Spoofing
© 1998 TSS, Inc. UNCLASSIFIED 18 Mar 98

Mar 20 icrosoft
Apr 20
Meanw



- Less than 10 publicized vulnerabilities in over 10 years
- Mostly local attacks
- Only DLLs perceived as problem

SC MAGAZINE
The Register
NETWORKWORLD
PC WORLD
MICROSOFT Certified Professional Magazine ONLINE
COMPUTERWORLD
ZDNet
heise online
eWEEK
THE H SECURITY
PC PCMAG.COM
REUTERS
Dr.Dobb's
InformationWeek
PC-WELT
CHIP ONLINE
DER SPIEGEL
Slashdot News for Nerds. Stuff that matters.
HITB Magazine Keeping Knowledge Free

Local Media

Monitor
Monitor PRO
moj Mikro
Sistem
stotech
EdiStrosar
MLADINA
INFORMACIJSKA VARNOST
Tehnologija in ljudje
si·cert
preberi.si BETA
Novice iz najboljših virov

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. System PATH; User PATH

It Was Even Worse Before 2004

"UNSAFE" Search Order

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. System PATH; User PATH

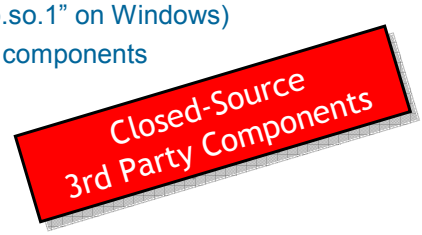
But is it Safe?

"SAFE" Search Order

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. System PATH; User PATH

Causes For Not Finding DLLs in Primary Locations

1. Programmer checks for local capabilities by trying to load a library
2. Some DLLs are present on OS1 but not on OS2 (dwmapi.dll)
3. Custom/partial installs
4. Backward compatibility
5. Forward compatibility
6. Application written so that it finds its binaries in PATH
7. O/S Porting (loading “linuxlib.so.1” on Windows)
8. Assumptions about installed components
9. Incomplete uninstalls
10....



Binary Planting Attacks

3-Step Attack Scenario

1... Plant a malicious DLL

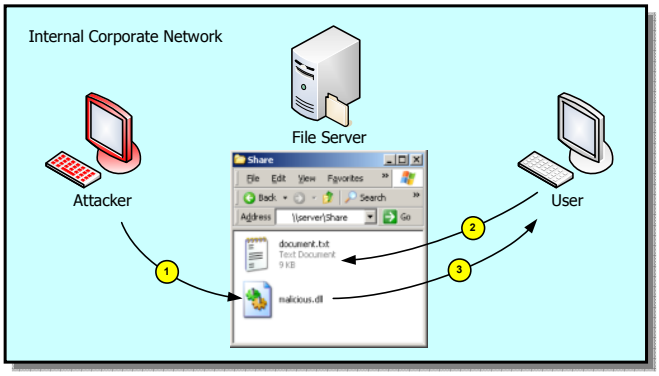
2... Set CWD to location of the DLL

3... Wait

Setting The Current Working Directory

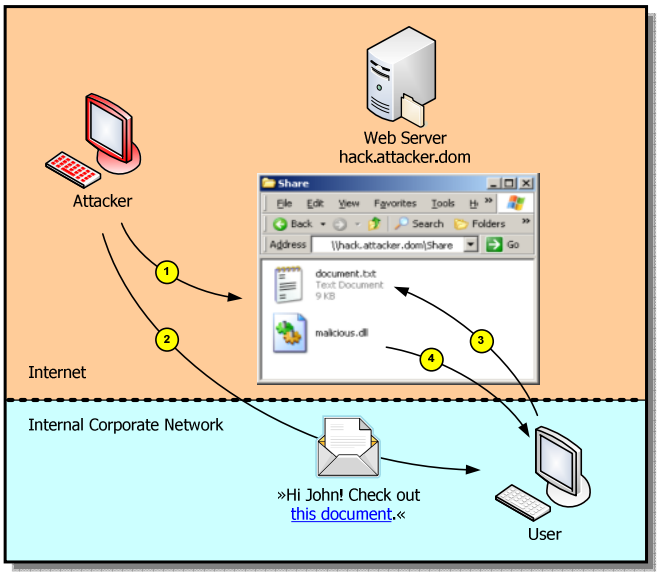
1. Double-clicking a file in Explorer
2. File Open, File Save dialogs
3. Last open/save location
4. cmd.exe: cd command
5. File explorers
6. CreateProcess, ShellExecute
7. New process inherits parent's CWD
8. Shortcuts
9. ...

Internal Network Attack



Local Goes Remote

Attacking From Internet – The WebDAV Magic

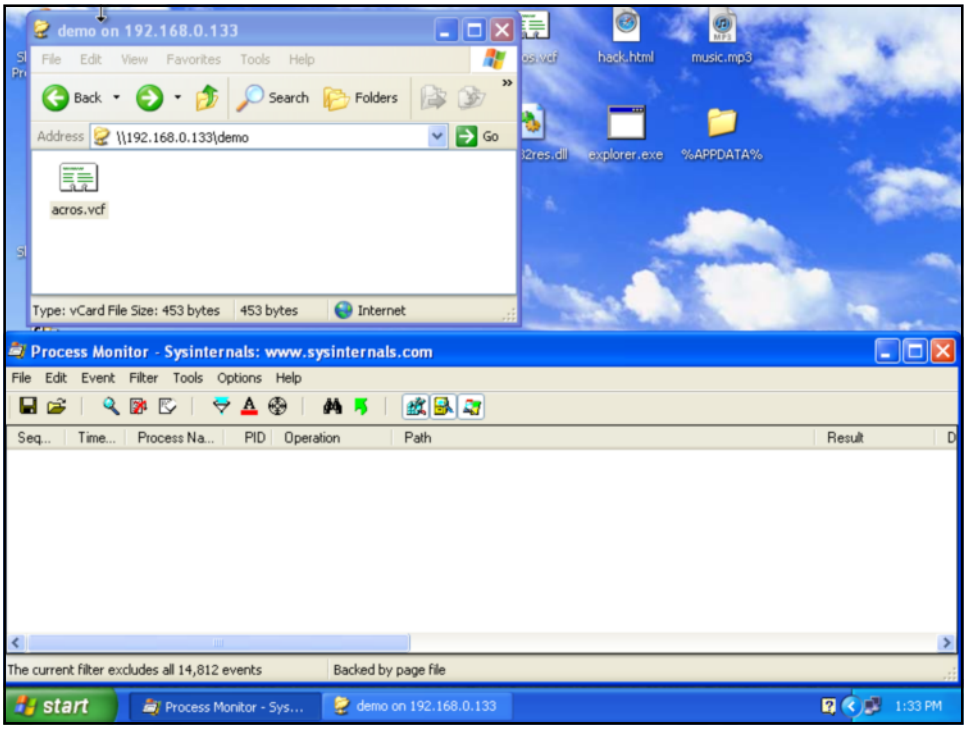


Attack Vectors

1. Clicking on a link in browser
2. Clicking on a link in e-mail
3. Clicking on a link in IM message
4. Planting a DLL on a file server
5. Document and DLL in a ZIP archive
6. Document and DLL on a USB stick
7. Document and DLL on CD/DVD
8. Local privilege escalation
9. Advanced binary planting attacks

Binary Planting Demo

wab.exe
Address Book
Microsoft Corporation



Binary Planting Goes “EXE”

Searching for Non-Absolute EXEs

```
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. System PATH; User PATH

Searching for Non-Absolute EXEs

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

~~The directory from which the application loaded~~

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

Searching for Non-Absolute EXEs

```
_spawn*p* and _exec*p*
```

~~The directory from which the application loaded~~

1. Current Working Directory (CWD)
2. C:\Windows\System32

~~C:\Windows\System~~

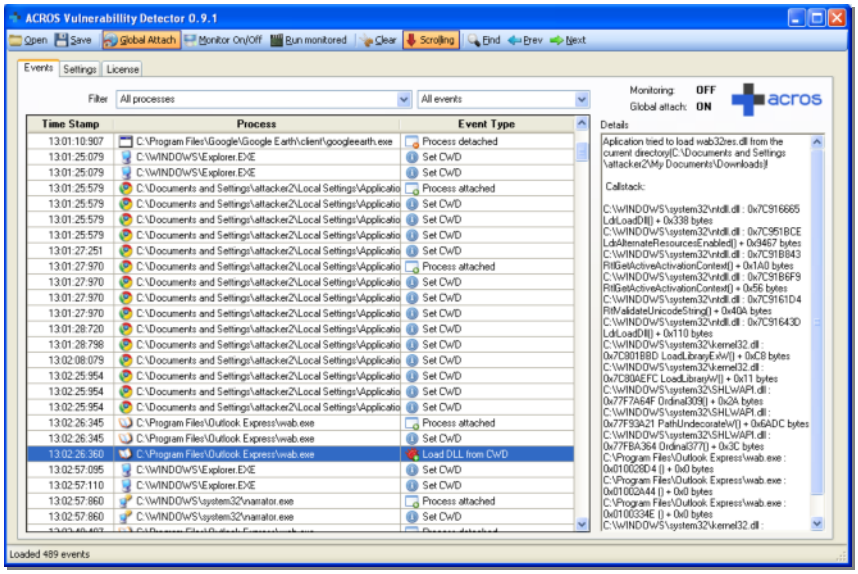
3. C:\Windows
4. System PATH; User PATH

Our Research

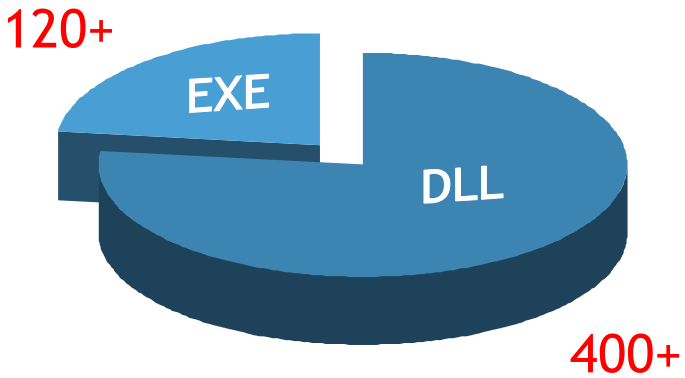
Research Summary

- Inspected 200+ Windows applications
  - At least one exploitable Binary Planting issue in almost every one!
  - (And we barely scratched the surface)
- Recorded 520+ Binary Planting issues
- Tool for detecting Binary Planting vulnerabilities
  - GUI, monitoring processes
  - Automated exploitation
  - Ability to directly debug vulnerable code

ACROS Binary Planting Detector



Score – DLL and EXE Plantings



How Many Bugs?!?

100.000.000.000

XP ~1340m, Vista ~400m, Windows 7 ~150m

Approx. 11.000 times the number of bicycles in Beijing

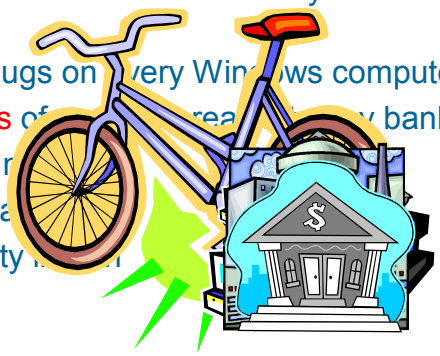
Hundreds of BP bugs on very Windows computer

Tens of thousands of bank

... or competitor's

... or government

... or nuclear facility



Affected Vendors

Microsoft
Apple
Google
VMware
IBM
Siemens
Mozilla
Adobe
Avast
Autodesk
Sophos
PGP ...

... ~100 at Secunia

...100+ from our research

What Can You Do?

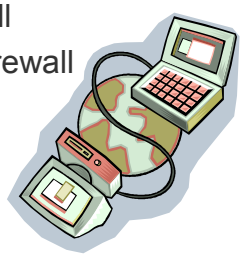
APPLY: Recommendations for Developers

- Use absolute paths to libraries and executables
- Don’t make “let’s see if it’s there” LoadLibrary* calls
- Don’t plan on finding your DLL/EXE in CWD or PATH
- Set CWD to a safe location at startup
- Use SetDllDirectory(“”) at startup
- Don’t use SearchPath function for locating DLLs
- Check your product with Process Monitor or another tool
- Test with CWDIllegalInDllSearch hotfix set to "max".
- Do this for all modules of your product!

http://www.binaryplanting.com/guidelinesDevelopers.htm

APPLY: Recommendations for Administrators

- Install Microsoft's Hotfix, remember to configure it
- Disable "Web Client" service
- Windows Software Restriction Policy, Windows AppLocker (DLL)
- Use a personal firewall with process and connection blocking
- Block outbound SMB on corporate firewall
- Block outbound WebDAV on corporate firewall
- Limit internal SMB, WebDAV traffic
- Restrict write access on file repositories to prevent planting



APPLY: Recommendations for Users

- Be careful when using USB sticks, CDs, DVDs from unknown sources
- Think before double-clicking on anything presented to you
- If in doubt, transfer the data file (alone) to local drive and open it
- Alert your administrators about binary planting

Resources

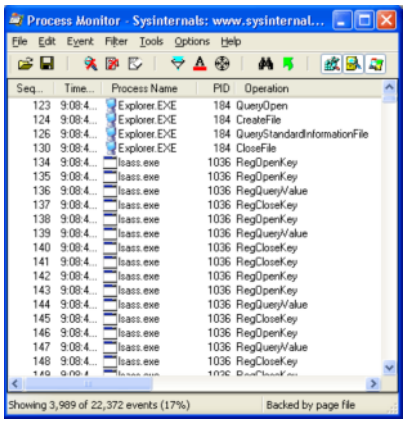
www.binaryplanting.com
blog.acrossecurity.com

http://support.microsoft.com/kb/2264107
http://blog.metasploit.com/2010/08/exploiting-dll-hijacking-flaws.html
http://blog.metasploit.com/2010/08/better-faster-stronger.html
http://securityxploded.com/dllhijackauditor.php
http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx

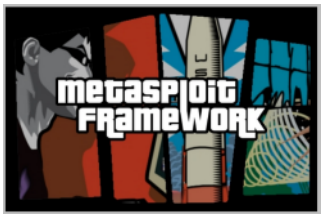
http://secunia.com/advisories/windows_insecure_library_loading/

Google “binary planting”, “dll hijacking”, “dll preloading”

Public Binary Planting Tools



DLLHijackAuditKit



Are you Binary Planting positive?

www.binaryplanting.com/test.htm

The Ultimate Solution: Eliminating CWD From The Game