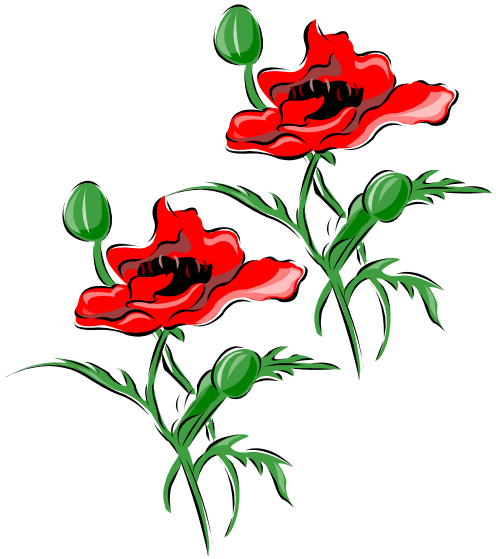


# Remote Binary Planting

## The Forgotten Vulnerability Affair

*HITBSECCONF 2010 Malaysia*




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

# Objectives

1. Can we find 512+ bugs?
2. Can balloons be used as progress bar?

# 200 Bugs Milestone

# 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

- M
- Or

Apr 20

Meanw

8:22 PM Aug 18th via TweetDeck
Retweeted by 52 people Reply Retweet

hdmoore
HD Moore

Aug 18, 2010 Apple fixes iTunes, Acros publishes ASPR

Later that day The cat gets "out of the bug"


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

# DLL Search Order – The "Troublemaker"

```
LoadLibrary("SomeLib.dll")
```

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

# Causes For Not Finding Binaries in Primary Locations

1. Programmer checks for local capabilities by trying to load a library
2. Language-dependent DLLs
3. A custom/partial install
4. Application is prepared for future enhancements
5. Backward compatibility
6. O/S Porting (loading “linuxlib.so.1” on Windows)
7. Missing delay-load DLLs
8. Wrong assumptions about “side by side” DLLs
9. Some DLLs are present on OS1 but not on OS2 (dwmapi.dll)
10. Application written so that it finds its binaries in PATH
11. Different paths to system DLLs in registry between OS1 and OS2
12. Assumptions about installed components
13. DLL loaded by 3rd party process in another location
14. Incomplete uninstalls
15. ...

Closed-Source
3rd Party Components

# Binary Planting Attacks

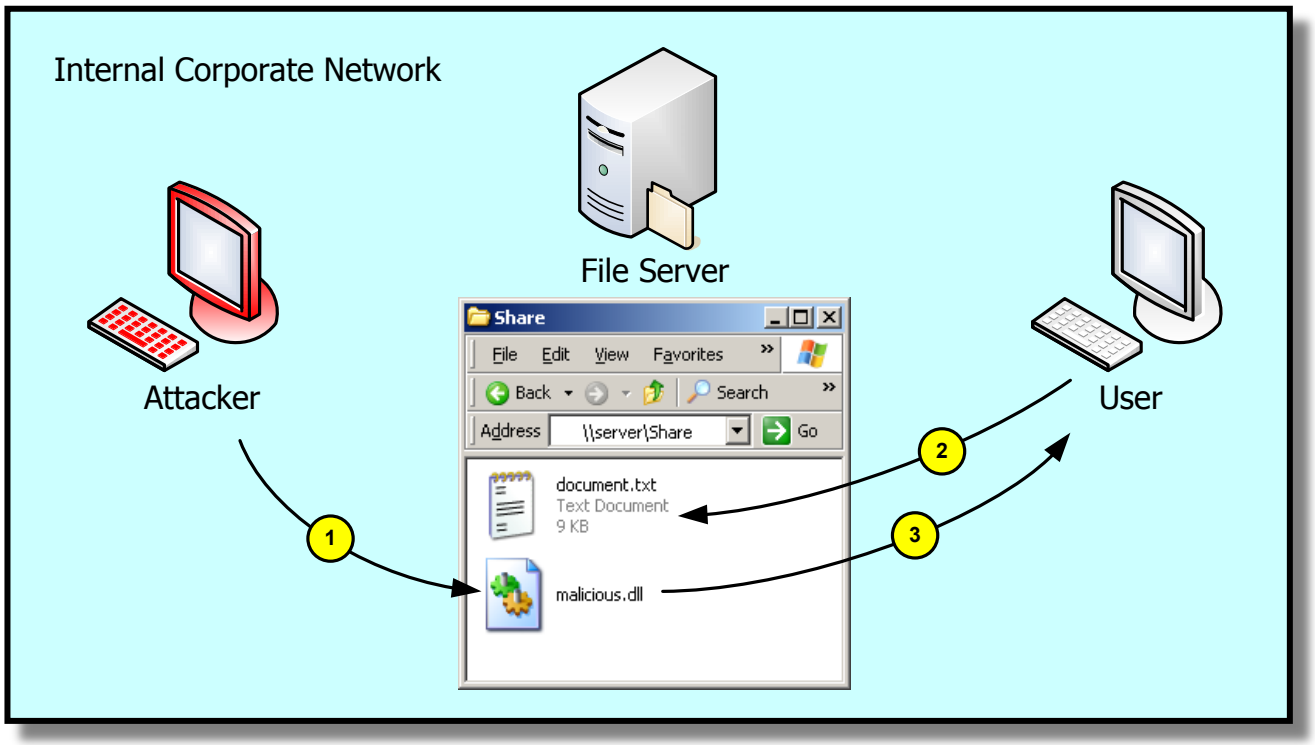
# 3-Step Attack Scenario

1. Planting a malicious binary
2. Getting CWD to the location of binary
3. Waiting for the app to load and execute it

# Setting The Current Working Directory

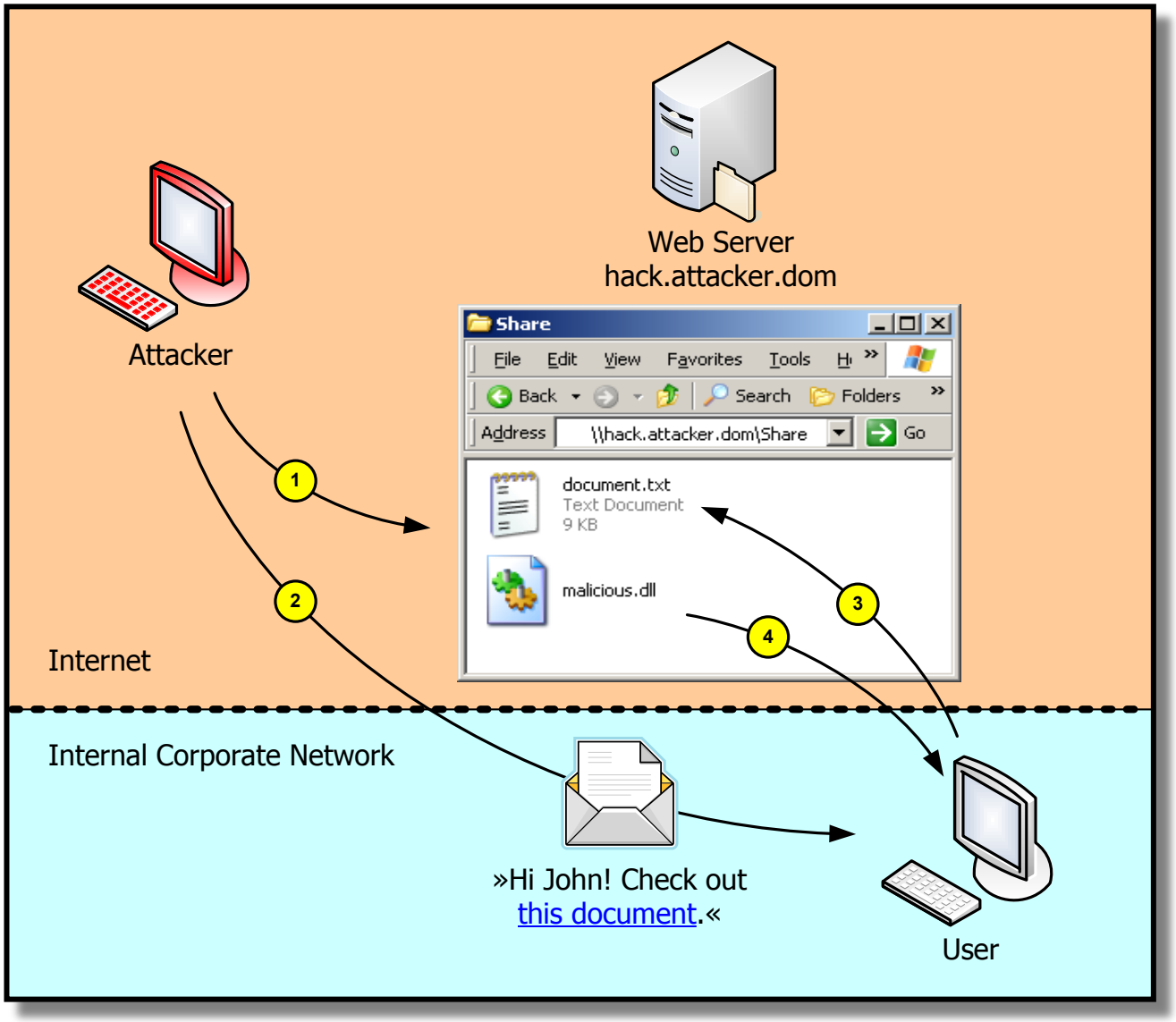
1. Double-clicking a file in Explorer
2. File Open, File Save dialogs
3. Last open/save location
4. Fixed location
5. cmd.exe: cd command
6. File explorers
7. CreateProcess, ShellExecute
8. New process gets parent's CWD

# Internal Network Attack




# Local Goes Remote

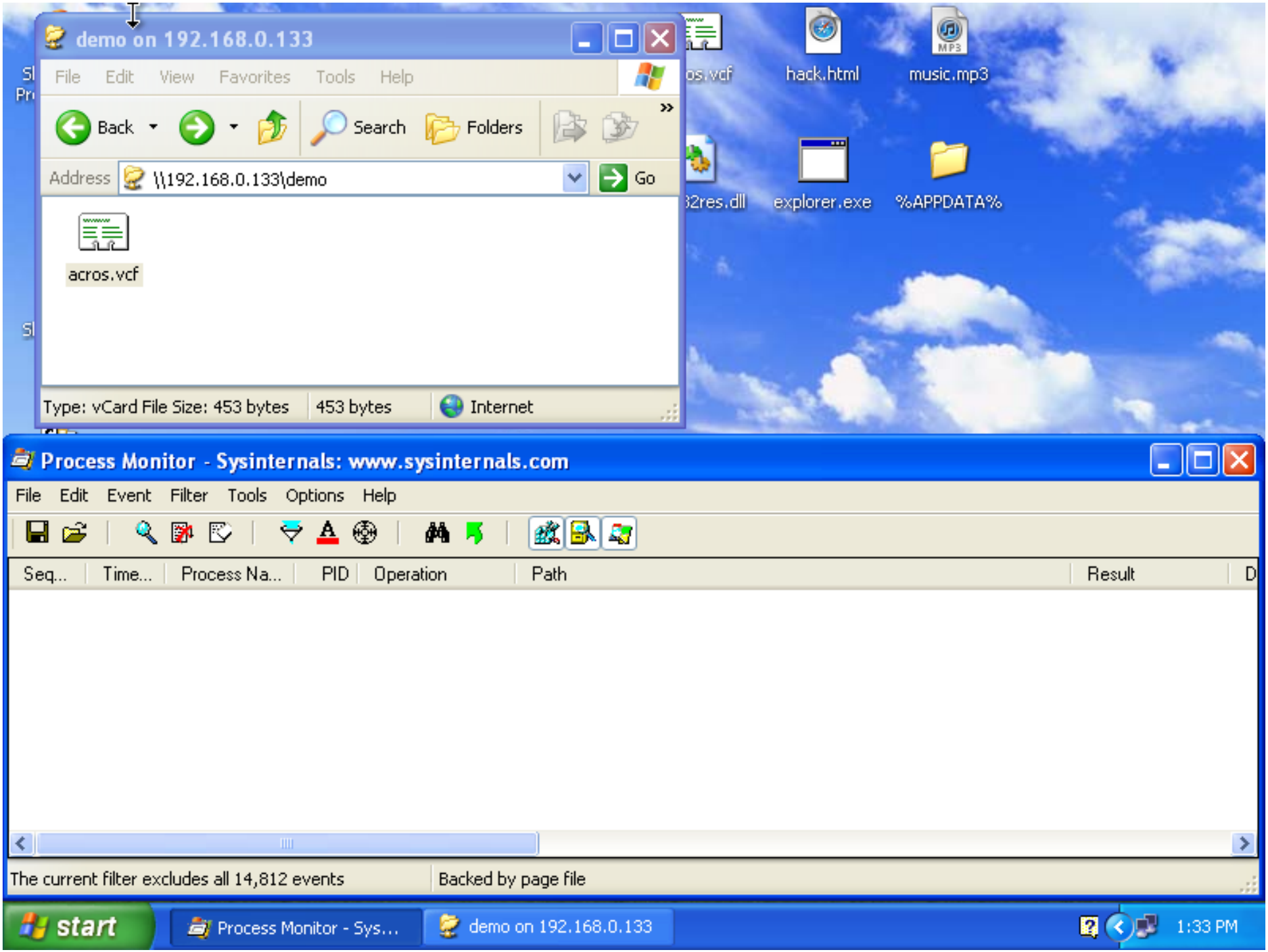
# Attacking From Internet – The WebDAV Magic



# 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 binary on a file server
5. Document and binary in a ZIP archive
6. Document and binary on a USB stick
7. Document and binary on CD/DVD
8. Local privilege escalation
9. Advanced binary planting attacks

# DLL Planting Demo



demo on 192.168.0.133
File Edit View Favorites Tools Help
Back Search Folders
Address \\192.168.0.133\demo
Go
acros.vcf
Type: vCard File Size: 453 bytes
453 bytes
Internet
os.vcf
hack.html
music.mp3
2res.dll
explorer.exe
%APPDATA%
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Seq... Time... Process Na... PID Operation Path Result D
The current filter excludes all 14,812 events
Backed by page file
start
Process Monitor - Sys...
demo on 192.168.0.133
1:33 PM

# 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

# Score

DLL Planting: 400+

EXE Planting: 120+

# Our Research

# Research Summary

## Inspected 200+ Windows applications

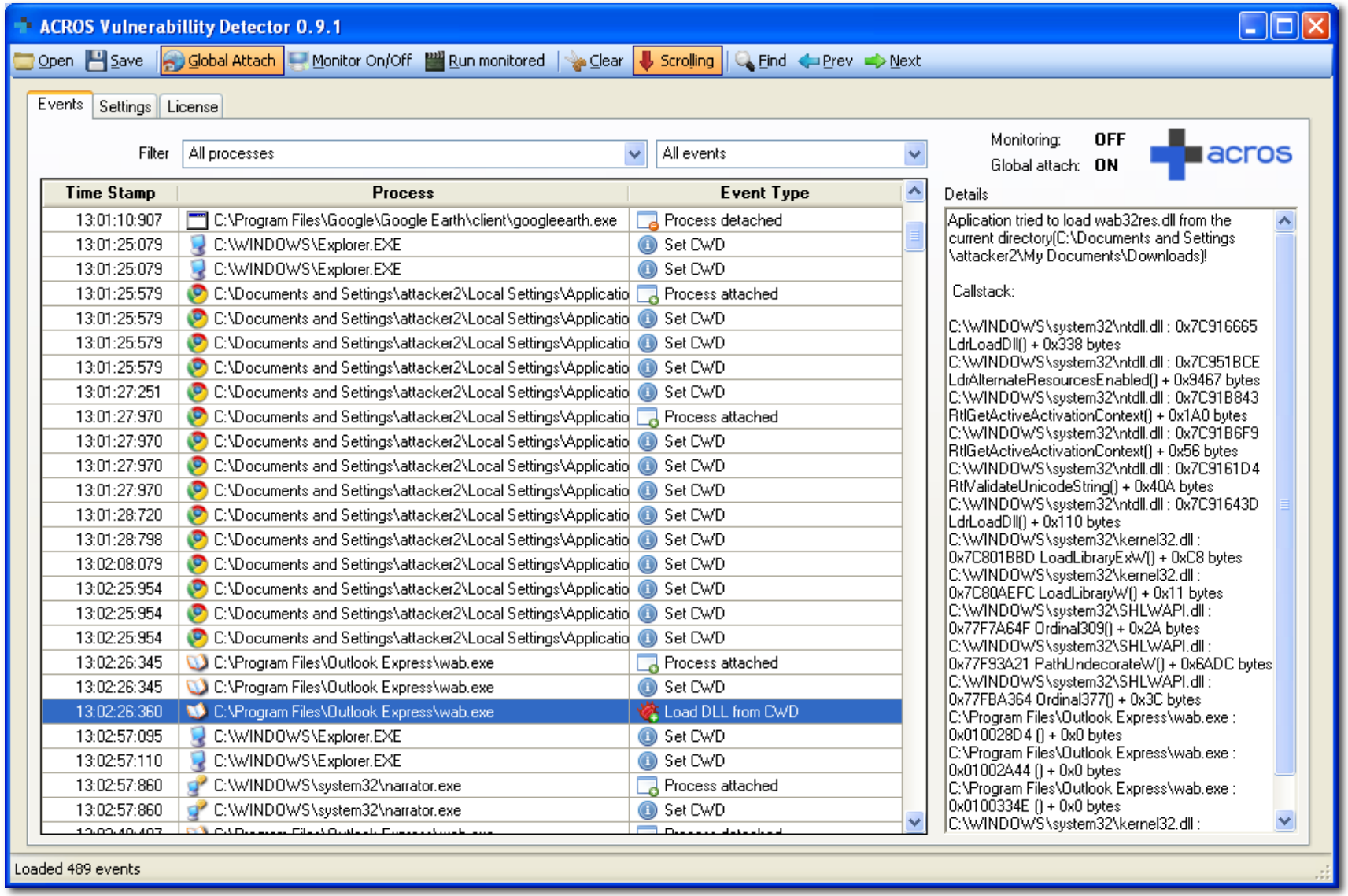
- At least one exploitable Binary Planting issue
  - in almost every one!
- (And we barely scratched the surface)

## 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



# How Many Bugs?!?

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

~100.000.000.000 bugs

Approx. 11.000 times the number of bicycles in Beijing

Hundreds of BP bugs every Windows computer

Tens of thousands of ways to break to any bank

... or competitor's n

... or government a

... or nuclear facility

# Affected Vendors

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

**... 70+ at Secunia**

**...100+ from our research**

# Recommendations

# 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

# 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

# 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, download the data file (alone) to local drive and open it
- Alert your administrators about binary planting

# What Microsoft Could Do

## Short Term

Extend the hotfix to EXE

Introduce SetExeDirectory()

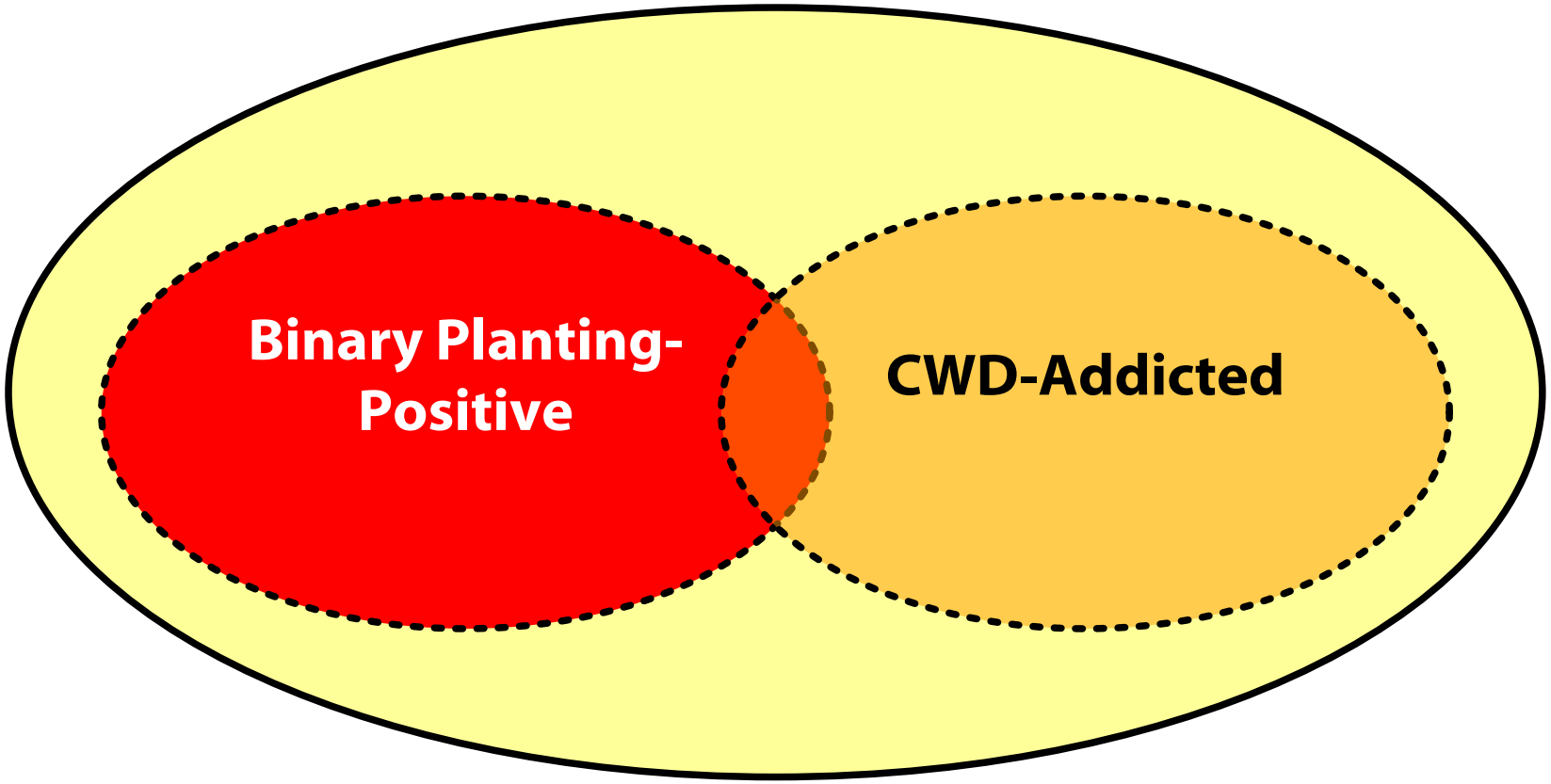
Safe search path for EXE loading

Set the default for file browse dialogs to not change CWD

## Long Term

Remove CWD from search paths

# The Ultimate Solution: Eliminating CWD From The Game




# Apple Re-Hacking Demo

# DLL Search Order after SetDllDirectory Call

```
SetDllDirectory(safepath)
LoadLibrary("SomeLib.dll")
```

1. The directory from which the application loaded
2. C:\Windows\System32
3. C:\Windows\System
4. C:\Windows
5. The **SetDllDirectory** location
6. System PATH; User PATH

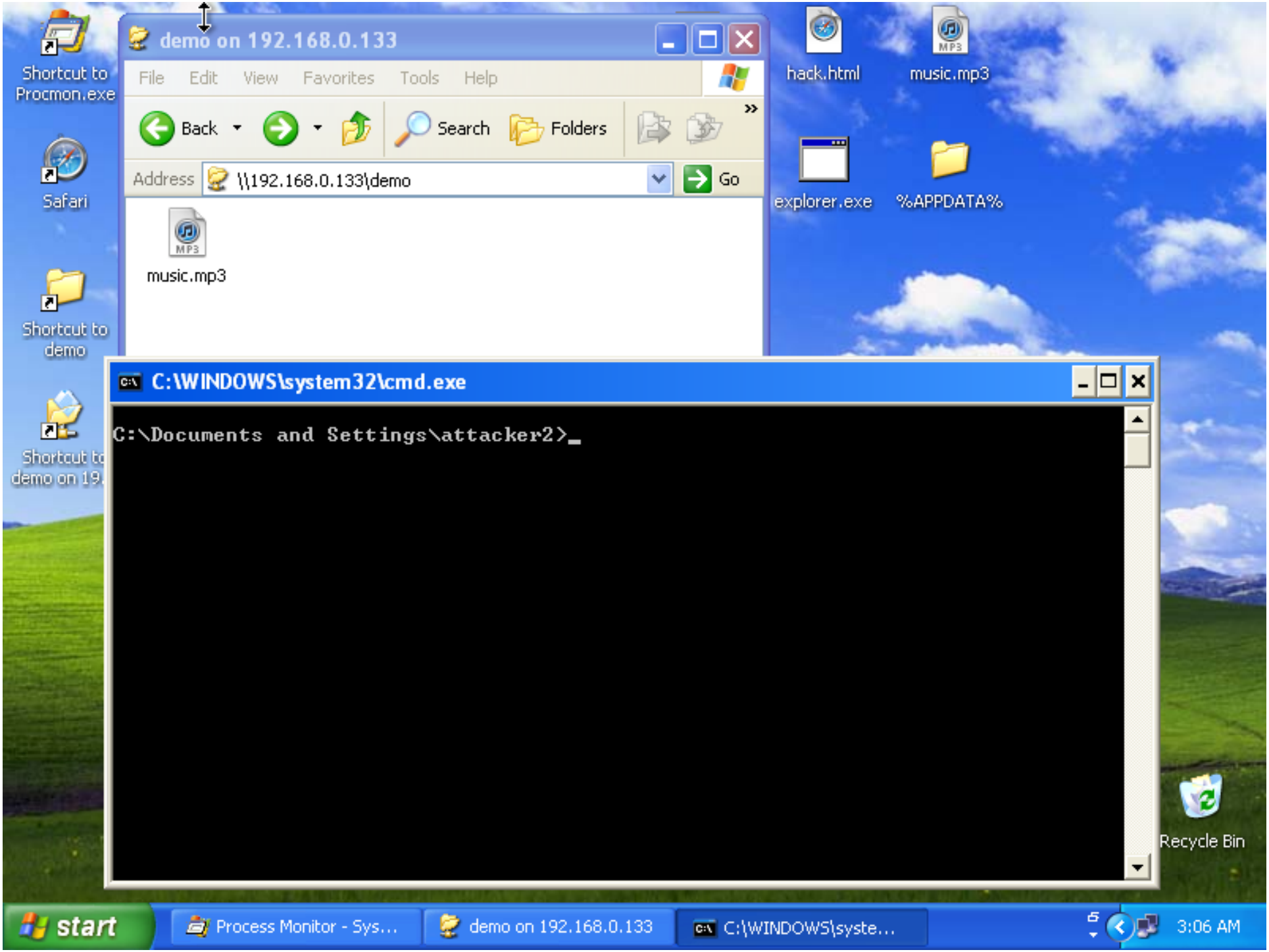
# Unresolved Environment Variables

- *"Win32 Oddities – **Unable to Expand** System Variables"*
- *"Vista - REG_EXPAND_SZ **only seems to expand some** variables"*
- *"Path Environment Variable **Incorrect** After Logon"*
- *"Windows installer **screws up** the PATH environment variable"*
- *"Environment variables **not being expanded** in Path registry entry"*
- *"ExpandEnvironmentStringsForUser() API does **NOT expand** the environment variable %USERNAME% on Windows 7"*

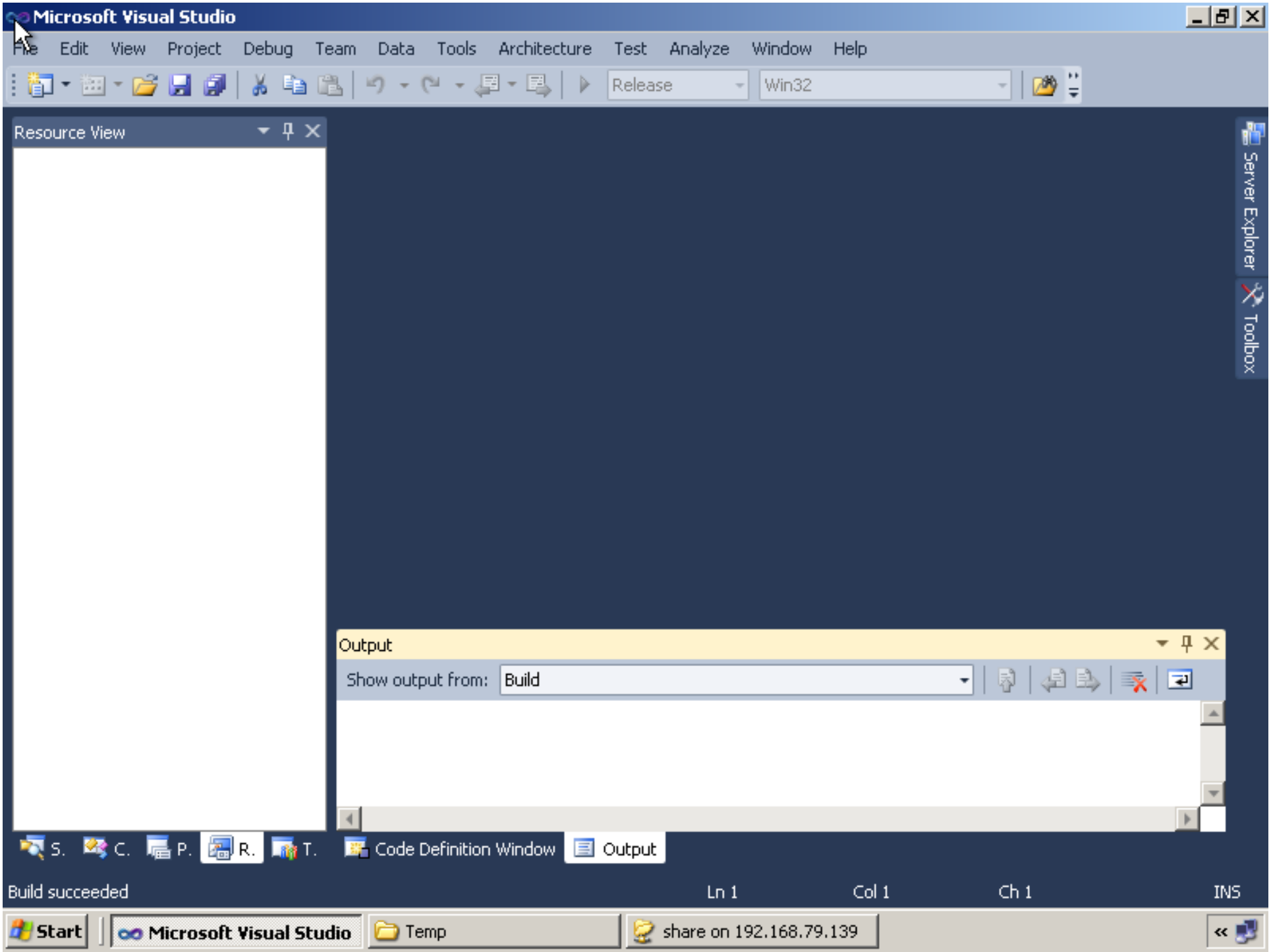
- *Microsoft Support, 2007: "Environment variable may not expand %APPDATA% to the Application folder"*
  http://support.microsoft.com/kb/329308

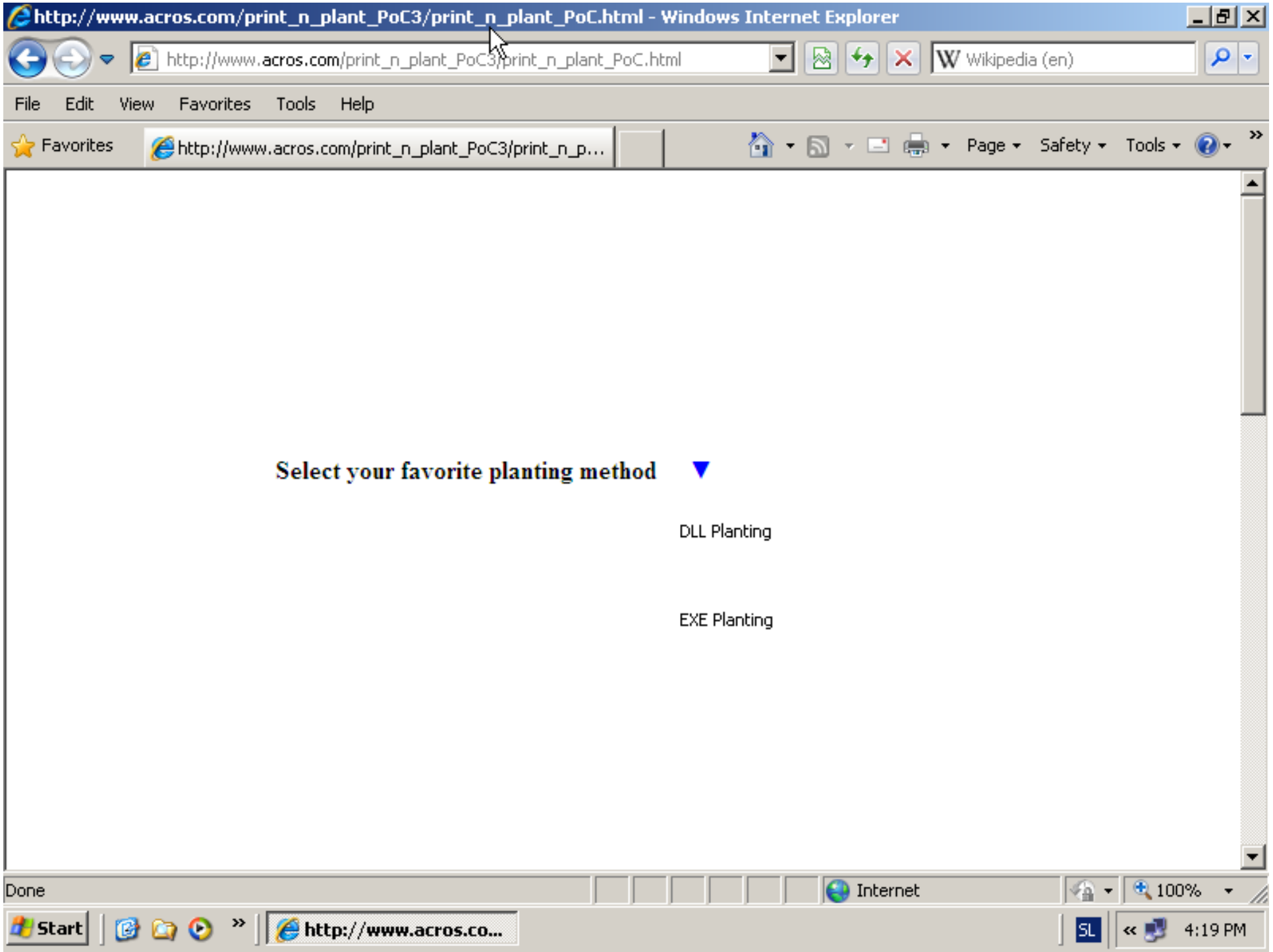
# Unresolved Environment Variables – Real World Examples

- %APPDATA%/Python/Scripts
- %ProgramFiles(x86)%
- %CommonProgramFiles%/Microsoft Shared/Windows Live
- %PROGRAMFILES(x86)%/Common Files/Microsoft Shared/Ink
- %USERPROFILE%/Local Settings/Temp
- %systemroot%/system32/DATA/Config
- %NpmLib%


Shortcut to Procmon.exe
Safari
Shortcut to demo
Shortcut to demo on 19...
demo on 192.168.0.133
File Edit View Favorites Tools Help
Back Search Folders
Address \\192.168.0.133\demo
Go
music.mp3
hack.html
music.mp3
explorer.exe
%APPDATA%
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\attacker2>_
Recycle Bin
start
Process Monitor - Sys...
demo on 192.168.0.133
C:\WINDOWS\syste...
3:06 AM

# 0-Code
# Vulnerable Application Demo


Microsoft Visual Studio
File Edit View Project Debug Team Data Tools Architecture Test Analyze Window Help
Release
Win32
Resource View
Server Explorer
Toolbox
Output
Show output from: Build
S. C. P. R. T. Code Definition Window Output
Build succeeded
Ln 1 Col 1 Ch 1 INS
Start
Microsoft Visual Studio
Temp
share on 192.168.79.139


http://www.acros.com/print_n_plant_PoC3/print_n_plant_PoC.html - Windows Internet Explorer
http://www.acros.com/print_n_plant_PoC3/print_n_plant_PoC.html
Wikipedia (en)
File Edit View Favorites Tools Help
Favorites
http://www.acros.com/print_n_plant_PoC3/print_n_p...
Page Safety Tools
Select your favorite planting method
DLL Planting
EXE Planting
Done
Internet
100%
Start
http://www.acros.co...
SL
4:19 PM

# Resources

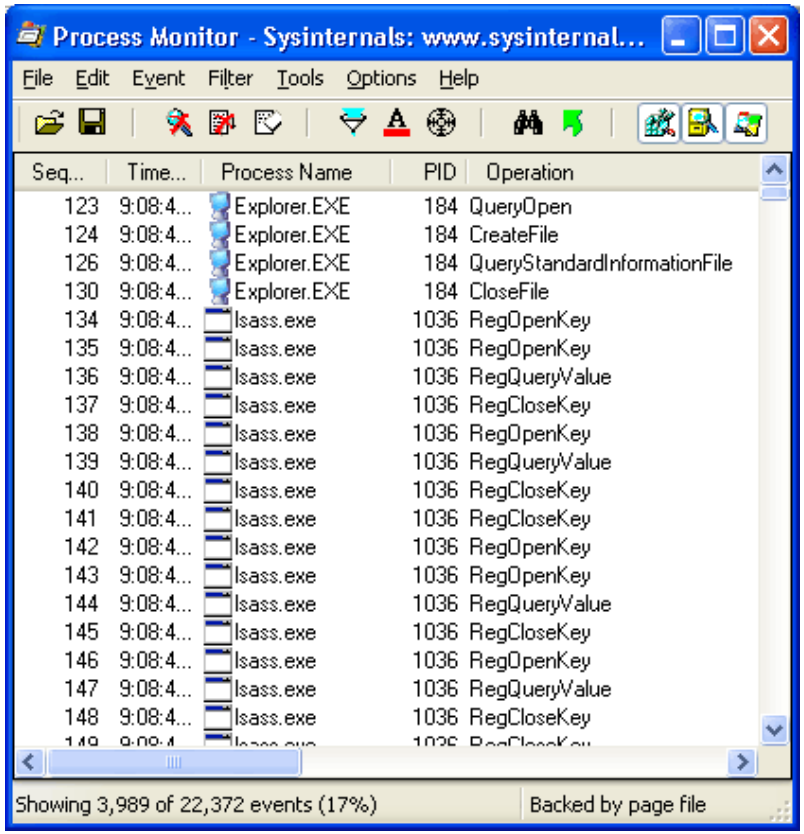
**www.binaryplanting.com**
**blog.acrossecurity.com**

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

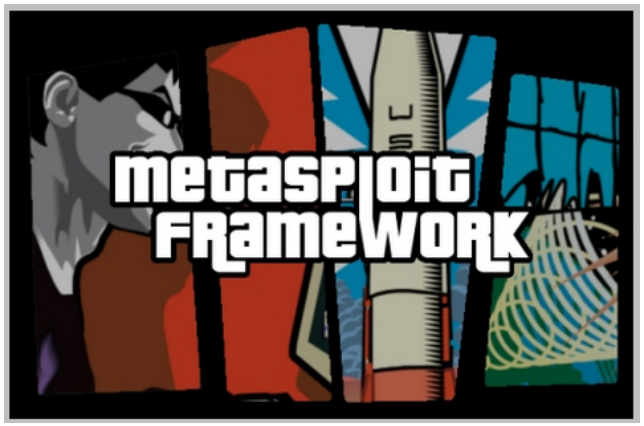
http://secunia.com/advisories/windows_insecure_library_loading/

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

# Public Binary Planting Tools




DLLHijackAuditKit





www.binaryplanting.com/test.htm

*(tell your friends, colleagues about it)*