Remote Binary Planting
First Overlooked, Then Downplayed, Now Ignored
HITBSECCONF 2011, Amsterdam

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

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
Overlooked
Downplayed

“A user has to go through multiple warnings and dialogs”
“Accessing a remote share and opening a document is unlikely”
Ignored

Many of the publicly known bugs remain unfixed (source: Secunia)
Practically all of the unpublished bugs we have found remain unfixed
New software is being created with these bugs
DLL Search Order

`LoadLibrary("SomeLib.dll")`

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

you

bad guy
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
Attacking From Internet – The WebDAV Magic

1. The attacker sends an email to a user in the internal corporate network.
2. The email contains a link to a malicious file.
3. The user accesses the link and downloads the malicious file.
4. The file is uploaded to the WebDAV server, and the user is then directed to access it through the WebDAV interface.

```
»Hi John! Check out this document.«
```
Attack Vectors

1. Clicking on a link in browser + doubleclick
2. Clicking on a link in e-mail + doubleclick
3. Clicking on a link in IM message + doubleclick
4. Planting a DLL on a file server + file open
5. Document and DLL in a ZIP archive + file open
6. Document and DLL on a USB stick + file open
7. Document and DLL on CD/DVD + file open
8. ...
9. Advanced binary planting attacks
Binary Planting Demo
Binary Planting Goes “EXE”
Searching for Non-Absolute EXEs

CreateProcess(“SomeApp.exe”)

1. The directory from which the application was loaded
2. Current Working Directory (CWD)
3. C:\Windows\System32
4. C:\Windows\System
5. C:\Windows
6. PATH
Searching for Non-Absolute EXEs

ShellExecute("SomeApp.exe")

The directory from which the application was loaded:

1. Current Working Directory (CWD)
2. C:\Windows\System32
3. C:\Windows\System
4. C:\Windows
5. PATH
Searching for Non-Absolute EXEs

_spawn*p* and _exec*p*

The directory from which the application was loaded

1. Current Working Directory (CWD)
2. C:\Windows\System32
3. C:\Windows\System
4. PATH
DLL vs. EXE Planting

120+ EXE

400+ DLL
How Many Bugs?!?

100.000.000.000

Hundreds of BP bugs on every Windows computer
Tens of thousands of ways to break into any bank
... or competitor’s network
... or government agency
... or nuclear facility in Iran
What Can You Do?
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 CWDIllegalInDIIISearch 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, transfer the data file (alone) to local drive and open it
- Alert your administrators about binary planting
Advanced Binary Planting

[ Luka’s white magic ]
Special Folders
In-Process COM Server

[Image of Registry Editor with highlighted entries]

- `My Computer\HKEY_CLASSES_ROOT\CLSID\{21EC2020-3AEA-1069-A2DD-08002B30309D}\InProcServer32`
- `shell32.dll`
Pwning Innocent Applications
Wordpad on Windows XP PoC

CoCreateInstance (CLSID)
- C:\Windows\System32\deskpan.dll
- C:\Windows\System\deskpan.dll
- C:\Windows\deskpan.dll

CWD set
- WORDPAD.EXE

double click
- [Image of Wordpad window with file: 42071714-76d4-11d1-8b24-00a0c9068ff3]
Word 2010 on Windows 7 PoC

LoadLibrary("ehtrace.dll")

- C:\Windows\System32\ehtrace.dll
- C:\Windows\System\ehtrace.dll
- C:\Windows\ehtrace.dll

CWD set

WINWORD.EXE

PSISDECD.DLL

Binary planting: {2E095DD0-AF56-47E4-A099-EAC038DECC24}
Pwning Your Website Visitor
XP + IE8
(Front View)
Finding Your Digital Vulnerabilities Before Others Do.

Your Security Problems

- Executives, Supervisors, Auditors
  You are the legal owner of your corporate data and information protection. More...

- IT managers, Security Officers
  You're responsible for the security of your company's information system. More...

Our Security Solutions

- Application Security Analysis
  We find security problems in software that you develop or use. More...

- Penetration Testing
  We become your friendly attacker and try to penetrate into... More...

ACROS Security

- is specialized in providing advanced security analyses of products and systems. Our innovative security research pushes the boundaries of global knowledge, keeps our customers ahead of competitors and users safe from attackers.

FOLLOW US ON twitter

...for updates on our security research.

ACROS in the Media

- ComputerWorld, "Unpatched DLL bugs let hackers exploit Windows 7 and IE9, says researcher" (May 2011)

News and Announcements

- ACROS will demonstrate binary planting attacks against IE9 at
Windows XP & Internet Explorer 8 PoC

CoCreateInstance (CLSID)

C:\Windows\System32\deskpan.dll
C:\Windows\System\deskpan.dll
C:\Windows\deskpan.dll

IEXPLORE.EXE

CWD set

WORDPAD.EXE

1st click

2nd click
XP + IE8
(Backstage)
Finding Your Digital Vulnerabilities Before Others Do.

Your Security Problems
- Executives, Supervisors, Auditors
  You are the legal owner of your corporate data and information protection. More...
- IT managers, Security Officers
  You’re responsible for the security of your company’s information system. More...

Our Security Solutions
- Application Security Analysis
  We find security problems in software that you develop or use. More...
- Penetration Testing
  We become your friendly attacker and try to penetrate into... More...

ACROS Security
is specialized in providing advanced security analyses of products and systems. Our innovative security research pushes the boundaries of global knowledge, keeps our customers ahead of competitors and users safe from attackers.

FOLLOW US ON twitter
...for updates on our security research.

ACROS in the Media
ComputerWorld, "Unpatched DLL bugs let hackers exploit Windows 7 and IE9, says researcher" (May 2011)

News and Announcements
ACROS will demonstrate binary planting attacks against IE9 at...
Win7 + IE9 + Protected mode (Front View)
Finding Your Digital Vulnerabilities Before Others Do.

ACROS Security
is specialized in providing advanced security analyses of products and systems. Our innovative security research pushes the boundaries of global knowledge, keeps our customers ahead of competitors and users safe from attackers.

FOLLOW US ON twitter
...for updates on our security research.

ACROS in the Media
ComputerWorld, "Unpatched DLL bugs let hackers exploit Windows 7 and IE9, says researcher" (May 2011)

News and Announcements
ACROS will demonstrate binary planting attacks against IE9 at Hack In The Box 2011 Amsterdam in May. (May 2011)

If you liked this video you can save it to your computer using right-click and Send To -> Compressed (zipped) folder
Windows 7 & Internet Explorer 9 PoC

**VERCLSID.EXE**

support.microsoft.com: “The **VERCLSID.EXE** program validates shell extensions before they are instantiated by the Windows shell or by Windows Explorer.”
Windows 7 & Internet Explorer 9 PoC

LoadLibrary("ehtrace.dll")

C:\Windows\System32\ehtrace.dll
C:\Windows\System\ehtrace.dll
C:\Windows\ehtrace.dll
Win7 + IE9 + Protected mode (Backstage)
Finding Your Digital Vulnerabilities Before Others Do.

If you liked this video you can save it to your computer using right-click and Send To - > Compressed (zipped) folder

ACROS Security

is specialized in providing advanced security analyses of products and systems. Our innovative security research pushes the boundaries of global knowledge, keeps our customers ahead of competitors and users safe from attackers.

FOLLOW US ON twitter

for updates on our security research.

ACROS in the Media

ComputerWorld, "Unpatched DLL bugs let hackers exploit Windows 7 and IE9, says researcher" (May 2011)

News and Announcements

ACROS will demonstrate binary planting attacks against IE9 at Hack In The Box 2011 Amsterdam in May. (May 2011)
What to do right now?

Developers

• Don’t register In-Process COM Servers with relative path to DLL
• Find and fix all unsafe library/executable loads

Users

• XP: remove the deskpan.dll reference in registry
• Win7: copy/create ehTrace.dll to System32 folder
• Don’t browse the Web until further notice ;-)

There’s much more to come!
Resources

www.binaryplanting.com
blog.acrossecurity.com

http://support.microsoft.com/kb/2264107
http://securityxploded.com/dllhijackauditor.php

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

Google “binary planting”, “dll hijacking”, “dll preloading”
Public Binary Planting Tools

### DLLHijackAuditKit

<table>
<thead>
<tr>
<th>Seq...</th>
<th>Time...</th>
<th>Process Name</th>
<th>PID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>123</td>
<td>9:08:4.</td>
<td>Explorer.EXE</td>
<td>184</td>
<td>QueryOpen</td>
</tr>
<tr>
<td>124</td>
<td>9:08:4.</td>
<td>Explorer.EXE</td>
<td>184</td>
<td>CreateFile</td>
</tr>
<tr>
<td>125</td>
<td>9:08:4.</td>
<td>Explorer.EXE</td>
<td>184</td>
<td>QueryStandardInformationFile</td>
</tr>
<tr>
<td>130</td>
<td>9:08:4.</td>
<td>Explorer.EXE</td>
<td>184</td>
<td>CloseFile</td>
</tr>
<tr>
<td>134</td>
<td>9:08:4.</td>
<td>lsass.exe</td>
<td>1036</td>
<td>RegOpenKey</td>
</tr>
<tr>
<td>135</td>
<td>9:08:4.</td>
<td>lsass.exe</td>
<td>1036</td>
<td>RegOpenKey</td>
</tr>
<tr>
<td>136</td>
<td>9:08:4.</td>
<td>lsass.exe</td>
<td>1036</td>
<td>RegQueryValue</td>
</tr>
<tr>
<td>137</td>
<td>9:08:4.</td>
<td>lsass.exe</td>
<td>1036</td>
<td>RegCloseKey</td>
</tr>
<tr>
<td>138</td>
<td>9:08:4.</td>
<td>lsass.exe</td>
<td>1036</td>
<td>RegOpenKey</td>
</tr>
<tr>
<td>139</td>
<td>9:08:4.</td>
<td>lsass.exe</td>
<td>1036</td>
<td>RegQueryValue</td>
</tr>
<tr>
<td>140</td>
<td>9:08:4.</td>
<td>lsass.exe</td>
<td>1036</td>
<td>RegCloseKey</td>
</tr>
<tr>
<td>141</td>
<td>9:08:4.</td>
<td>lsass.exe</td>
<td>1036</td>
<td>RegCloseKey</td>
</tr>
<tr>
<td>142</td>
<td>9:08:4.</td>
<td>lsass.exe</td>
<td>1036</td>
<td>RegQueryValue</td>
</tr>
<tr>
<td>143</td>
<td>9:08:4.</td>
<td>lsass.exe</td>
<td>1036</td>
<td>RegOpenKey</td>
</tr>
<tr>
<td>144</td>
<td>9:08:4.</td>
<td>lsass.exe</td>
<td>1036</td>
<td>RegQueryValue</td>
</tr>
<tr>
<td>145</td>
<td>9:08:4.</td>
<td>lsass.exe</td>
<td>1036</td>
<td>RegCloseKey</td>
</tr>
<tr>
<td>146</td>
<td>9:08:4.</td>
<td>lsass.exe</td>
<td>1036</td>
<td>RegCloseKey</td>
</tr>
<tr>
<td>147</td>
<td>9:08:4.</td>
<td>lsass.exe</td>
<td>1036</td>
<td>RegQueryValue</td>
</tr>
<tr>
<td>148</td>
<td>9:08:4.</td>
<td>lsass.exe</td>
<td>1036</td>
<td>RegCloseKey</td>
</tr>
</tbody>
</table>

Showing 3,999 of 22,372 events (17%)
Are you Binary Planting positive?

www.binaryplanting.com/test.htm