THE WOW-EFFECT
- or how Microsoft's WOW64 technology unintentionally fools IT Security analysts

Christian Wojner, CERT.at
THIS IS AN AWARENESS TALK!
Wh01am

Person
- Christian Wojner
- Malware Analyst / Reverse Engineer
- CERT.at / GovCERT.gv.at

Publications
- Papers
  - Mass Malware Analysis: A DIY Kit
  - An Analysis of the Skype IMBot Logic and Functionality
  - The WOW-Effect
- Articles
  - HITB Online Mag
  - The Art of DLL Injection
  - Automated Malware Analysis - An Introduction to Minibis
  - HAKIN9 Online Mag
  - Minibis
- Software
  - Minibis
  - Bytehist (REMnux)
  - Densitiescout (REMnux)
  - ProcDOT

Speaker
- FIRST Symposium 2010
- CertVerbund-DE 2010
- Deepsec 2010
- Teliasonera 2011
- Joint FIRST/TF-CSIRT Technical Seminar 2012
- CanSecWest 2012
- CertVerbund-DE 2012
- 0ct0b3rf3st 2012
Sidenotes ...

- Based on a paper I wrote in November 2011
- Topic not entirely new but
  - the implications have been *widely underestimated* or *entirely overseen*
- In contact with Microsoft
  - MSRC (Microsoft Response Center)
  - My impression: Implications were new to them
  - M$ Forensics and Malware analysts got informed
  - Tareq, thx for your support!

07.10.2012
What's the WOW-Effect?

- Not easy to answer in one sentence
- Only one person can do this:
  - It's comparable to an impression of something
  - Try to explain an impression in one sentence
  - This talk will transfer this impression to you
A little tale about "Digital Evolution"

- Boxes got smaller
- Busses got wider
- Memory got bigger
- CPUs got faster
- 16 Bit, 32 Bit, and finally 64 Bit systems became the new main-stream

- But one problem is and was always around ...
  - Backwards compatibility ==> Old things won't die
Once upon a time ... 

Do you like my new haircut? It's 64 Bits long!

WOW!
Manufacturers ...

Dear customers, it's time to switch to 64 Bit systems, NOW!
Customers ...

Cool, but we still want to use our old 32 Bit stuff. What now?
Microsoft ...

No problem, we have an All-In-1 solution for you!
WOW!
WOW - World Of Warcraft?

- NO! It has nothing to do with fantasy ... and monsters ...
  ... so they say.

- WOW stands for ...
  Windows On Windows

- WOW64 stands for ...
  Microsoft Windows-32-on-Windows-64
32 Bit vs. 64 Bit

- Major differences for operating systems ...
  - Registers (32 Bit/64 Bit)
  - Instructionset (x86/x64)
  - Size of pointers (4 Byte/8 Byte)

- Implications ...
  - Structures
  - Objects/Classes
  - Interfaces
  - Calls (API)
WOW64 specifics

- Memory Management
- Registry
- File System
- CPU, Instructionset
A new folder is born

- "SysWOW64"
- Mini-32-Bit-Windows
  - Holds everything that's necessary for 32 Bit processes
- A bitter aftertaste: Confusion, pure ...
  - System32 => 64 Bit files
  - SysWOW64 => 32 Bit files
File System Redirector

- Any 32 Bit application gets redirected:

<table>
<thead>
<tr>
<th>Access to ...</th>
<th>... is redirected to ...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Folders</strong></td>
<td></td>
</tr>
<tr>
<td>%windir%\System32\</td>
<td>%windir%\SysWOW64\</td>
</tr>
<tr>
<td>%windir%\lastgood\system32\</td>
<td>%windir%\lastgood\SysWOW64\</td>
</tr>
<tr>
<td><strong>Files</strong></td>
<td></td>
</tr>
<tr>
<td>%windir%\regedit.exe</td>
<td>%windir%\SysWOW64\regedit.exe</td>
</tr>
</tbody>
</table>
The root of our problem ...

This is done centrally!

What else?

This should be done selectively!
An exemplary impact

- Live forensics / malware analysis
  - A typical approach for a potentially infected system:
    1. Spot suspicious files
    2. Check them against databases
       a. using local tools
       b. using online services
    3. Interpret findings
Preparations

- Example file with MD5 hashes for the upcoming scenarios:

The dynamic link library (DLL) "ieapfltr.dll"

<table>
<thead>
<tr>
<th>32 Bit</th>
<th>64 Bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Windows\SysWOW64\ieapfltr.dll</td>
<td>C:\Windows\system32\ieapfltr.dll</td>
</tr>
<tr>
<td>ee9d715af1b928982f417238b9914484</td>
<td>8eada158d964e3fd1999ad96c9c507ff</td>
</tr>
</tbody>
</table>

Good!  
Malicious!
Impact: MD5 tool

- Yet another MD5 tool (32 Bit)

Malicious!

<table>
<thead>
<tr>
<th>32 Bit</th>
<th>64 Bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Users\chrisu\Documents&gt;md5sum C:\Windows\system32\ieapfltr.dll ee9d715af1b928982f417238b9914484</td>
<td>C:\Windows\system32\ieapfltr.dll 8eada158d964e3fd1999ad96c9c507ff</td>
</tr>
</tbody>
</table>

Good!
That's the WOW-Effect!
Our toolsets

- Approved (maybe old) tools
- Third-party tools (unknown author, no source)
- "Outdated" tools
- Everyone concentrated on 32 Bit in the past

→ Most of our tools are 32 Bit based!

Examples: Hexeditors, Disassemblers, Debuggers, Cygwin, PE Viewers, Resource Editors, ...
Impact: Virus Total / Browsers

- Checking via Virus Total
**Impact: Virus Total / Browsers**

![File already submitted](image)

**32 Bit**
- Path: `C:\Windows\SysWOW64\ieapfltr.dll`
- MD5: `ee9d715af1b928982f417238b9914484`

**64 Bit**
- Path: `C:\Windows\system32\ieapfltr.dll`
- MD5: `8eada158d964e3fd1999ad96c9c507ff`

*Malicious!*

*Good!*
Browsers?!  

- Most of the browsers out there are 32 Bit  
  - 64 Bit versions are becoming available, finally.  
- IE on Windows 7 64 Bit by default 32 Bit  
- Thinking further ...  
  - Any 64 Bit variants of System32 files on Virus Total? I couldn't find ONE. *(November 2011)*  
  - Now: Well, the ones I tried.  
  - Implication: Most of us have been fooled by the WOW-Effect?
Filesystem iteration

- File-system iterations (FindFirstFile) are also affected by the File System Redirector

- Typical tools
  - Filelist differs
  - Recursive copy tools
  - Signature scanning tools
  - ...

07.10.2012
Registry Redirector

- Basically similar to Filesystem Redirector
- 2 coexistent views (32/64)
- 32-bit view is inside the 64-bit view in a special sub-node: Wow6432Node
- Specific Registry keys are ...
  - shared
    ≡ same object
  - reflected (< Windows 7 / Server 2008 R2)
    ≡ same value (automatically synchronized)
  - redirected (← Not so awesome!)
## Redirected Keys

<table>
<thead>
<tr>
<th>Registry-Key</th>
<th>Before Windows 7 and Server 2008 R2</th>
<th>Since Windows 7 and Server 2008 R2</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKLM\SOFTWARE\Classes</td>
<td>Redirected</td>
<td>Redirected</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Classes\Appid</td>
<td>Redirected and reflected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Classes\CLSID</td>
<td>Redirected and reflected</td>
<td>Redirected</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Classes\DirectShow</td>
<td>Redirected and reflected</td>
<td>Redirected</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Classes\Interface</td>
<td>Redirected and reflected</td>
<td>Redirected</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Classes\Media Type</td>
<td>Redirected and reflected</td>
<td>Redirected</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Classes\MediaFoundation</td>
<td>Redirected and reflected</td>
<td>Redirected</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Clients</td>
<td>Redirected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\COM3</td>
<td>Redirected and reflected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\EventSystem</td>
<td>Redirected and reflected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Notepad\DefaultFonts</td>
<td>Redirected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\OLE</td>
<td>Redirected and reflected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\RPC</td>
<td>Redirected and reflected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths</td>
<td>Redirected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers</td>
<td>Redirected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\DriveIcons</td>
<td>Redirected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\KindMap</td>
<td>Redirected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\PreviewHandlers</td>
<td>Redirected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Console</td>
<td>Redirected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink</td>
<td>Redirected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Gre_Initialize</td>
<td>Redirected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options</td>
<td>Redirected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Language Pack</td>
<td>Redirected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKCU\SOFTWARE\Classes</td>
<td>Redirected and reflected</td>
<td>Shared</td>
</tr>
<tr>
<td>HKCU\SOFTWARE\Classes\Appid</td>
<td>Redirected and reflected</td>
<td>Redirected</td>
</tr>
<tr>
<td>HKCU\SOFTWARE\Classes\CLSID</td>
<td>Redirected and reflected</td>
<td>Redirected</td>
</tr>
<tr>
<td>HKCU\SOFTWARE\Classes\DirectShow</td>
<td>Redirected and reflected</td>
<td>Redirected</td>
</tr>
<tr>
<td>HKCU\SOFTWARE\Classes\Interface</td>
<td>Redirected and reflected</td>
<td>Redirected</td>
</tr>
<tr>
<td>HKCU\SOFTWARE\Classes\Media Type</td>
<td>Redirected and reflected</td>
<td>Redirected</td>
</tr>
<tr>
<td>HKCU\SOFTWARE\Classes\MediaFoundation</td>
<td>Redirected and reflected</td>
<td>Redirected</td>
</tr>
</tbody>
</table>
Now, this must be a joke!? 

- From the WOW64 specs on MSDN ...
  - To help 32-bit applications that write REG_SZ or REG_EXPAND_SZ data containing %ProgramFiles% or %commonprogramfiles% to the registry, WOW64 intercepts these write operations and replaces them with "%ProgramFiles(x86)%" and "%commonprogramfiles(x86)%". For example, if the Program Files directory is on the C drive, then "%ProgramFiles(x86)%" expands to "C:\Program Files (x86)".
  - "Only" under specific (but common) conditions!
... Apparently!

- From the WOW64 specs on MSDN, again ...
  - In addition, REG_SZ or REG_EXPAND_SZ keys containing system32 are replaced with syswow64. The string must begin with the path pointing to or under \%windir\%\system32. The string comparison is not case-sensitive. Environment variables are expanded before matching the path, so all of the following paths are replaced:
    \%windir\%\system32, %SystemRoot%\system32, and C:\windows\system32.
Selective Blindness?

32 Bit sees 64 Bit
"32 Bit" Files
"32 Bit" Keys
"32 Bit" Values

sees "64 Bit" Files
"64 Bit" Keys
"64 Bit" Values
Impacts ...
Impact: Quick'n'dirty tools

- ... might have a problem
- Example:
  - Small, specialized removers/detectors for specific malware
- Who would really compile them to 64 Bit??
  - ... well, maybe this changes now
Impact: (Runtime) Environments

- Interpreters, Scripting Languages
  - Java
  - Perl
  - Python
  - ...
  32 Bit and 64 Bit versions are available!
  => Which one have you installed?
  => Which one is on the target system?
- Cygwin => only 32 Bit!
What about Anti-Virus?

- Easy to answer:
  "They know what they are doing." ... Hm?
- Multiple components
- A friend of mine worked in the AV industries
  - 64 Bit issues/solutions => well-hidden knowledge between AV companies
  - There **ARE** AV products out there with 32 Bit file-system components
Solutions?

- None, in terms of patches
  - It's a **feature** not a bug
- Be AWARE!
- Use **64 Bit tools** on 64 Bit Windows
- Bulletproof solution?
  - Be "**redundant**" (always both, 32 Bit and 64 Bit)
- Use the according **kill switches** ...
Redirection Killswitch(es)

- Disabling File System Redirection
  - API-Call `Wow64DisableWow64FsRedirection` (kernel32.dll)
    M$: Be careful with this – when it's off, it's off!

- Disabling Registry Redirection
  - Impossible!
    If you google ...
    Since Vista there should be 2 new functions
    - RegSetKeyFlags
    - RegQueryKeyFlags
    to be used with the according flag `KEY_FLAG_DISABLE_REDIRECTION`
    → No documentations, not in the API header-files, no trace at all → Rumor?

- ... or choose your way on demand ...
Choose your road to Rome

- Anti-redirection-alias `%windir%\Sysnative`
  - One-Way-Translation to c:\windows\system32
  - Will not show up in (recursive) listings!
- Selecting the desired mode in the extended Registry functions ...
  - RegCreateKeyEx, RegDeleteKeyEx, RegOpenKeyEx
  - by the flags:
    - KEY_WOW64_64KEY
    - KEY_WOW64_32KEY
Conclusion

1. Be aware of the WOW-Effect.
2. Consider the WOW-Effect.
3. Check and (eventually) revise your working processes/procedures/tools before dealing with 64 Bit based Microsoft Windows systems.
Reactions?
Paper:
http://cert.at/downloads/papers/wow_effect_en.html
We are all wondering how this will work out for any upcoming 128-bit version of Windows: System32 has 128-bit, SysWOW128 64-bit, and SysWOW64 contains the 32-bit versions?

Paper:
http://cert.at/downloads/papers/wow_effect_en.html