THE WOW-EFFECT

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

DIMENSION - THE WHOLE DIMENSION - THE WHOLE DIMENSION - THE WHOLE DIM

Christian Wojner, CERT.at

Wh01am

Person

- Christian Wojner
- Malware Analysis, Reverse Engineering, Computer Forensics
- 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)
  - Densityscout (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
- SANS Forensic Summit Prague 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!

THIS IS AN **AWARENESS** TALK!

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: an acronym 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 executables
  - SysWOW64 => 32 Bit executables

File System Redirector

- 32 Bit applications need to be DIRECTED to use this backpacked 32 Bit Windows
- ... or more precisely: REDIRECTED

Access to ...	... is redirected to ...
Folders	
%windir%\System32\\	%windir%\SysWOW64\\
%windir%\\lastgood\system32\\	%windir%\\lastgood\SysWOW64\\
Files	
%windir%\regedit.exe	%windir%\\SysWOW64\regedit.exe

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**"

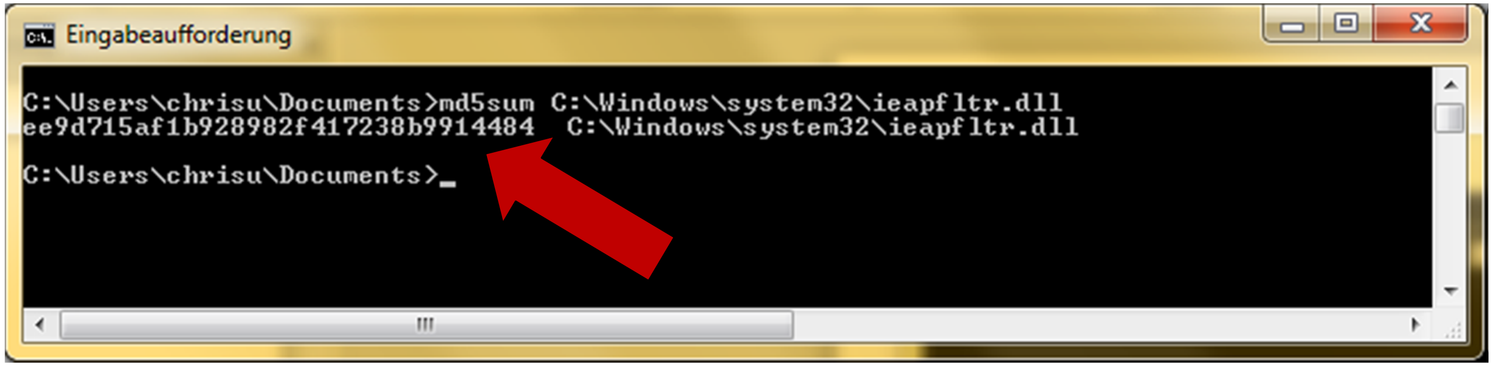
32 Bit	64 Bit
C:\Windows\SysWOW64\ieapfltr.dll	C:\Windows\system32\ieapfltr.dll
ee9d715af1b928982f417238b9914484	8eada158d964e3fd1999ad96c9c507ff

Good!

Malicious!

Impact: MD5 tool

- Yet another MD5 tool (32 Bit)



```
C:\Users\chrisu\Documents>md5sum C:\Windows\system32\ieapfltr.dll
ee9d715af1b928982f417238b9914484  C:\Windows\system32\ieapfltr.dll

C:\Users\chrisu\Documents>_
```

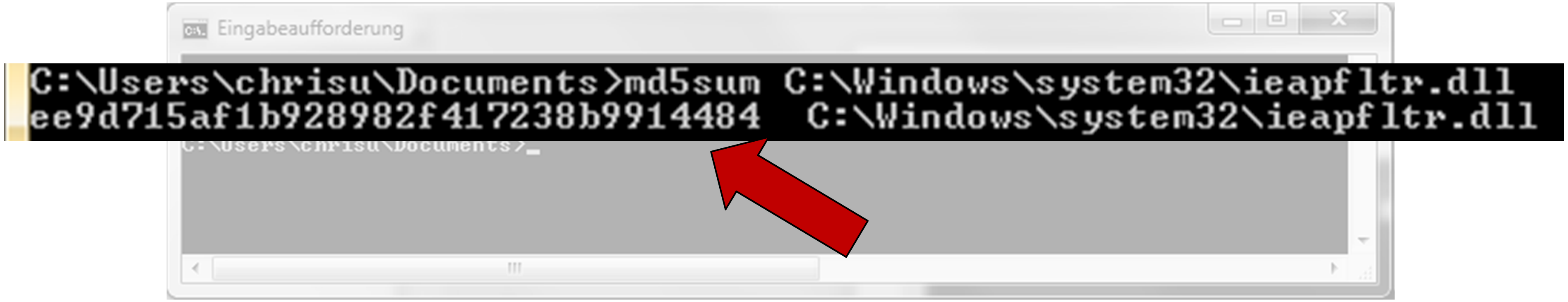
Good!

Malicious!

32 Bit	64 Bit
C:\Windows\SysWOW64\ieapfltr.dll	C:\Windows\system32\ieapfltr.dll
ee9d715af1b928982f417238b9914484	8eada158d964e3fd1999ad96c9c507ff

Impact: MD5 tool

- Yet another MD5 tool (32 Bit)



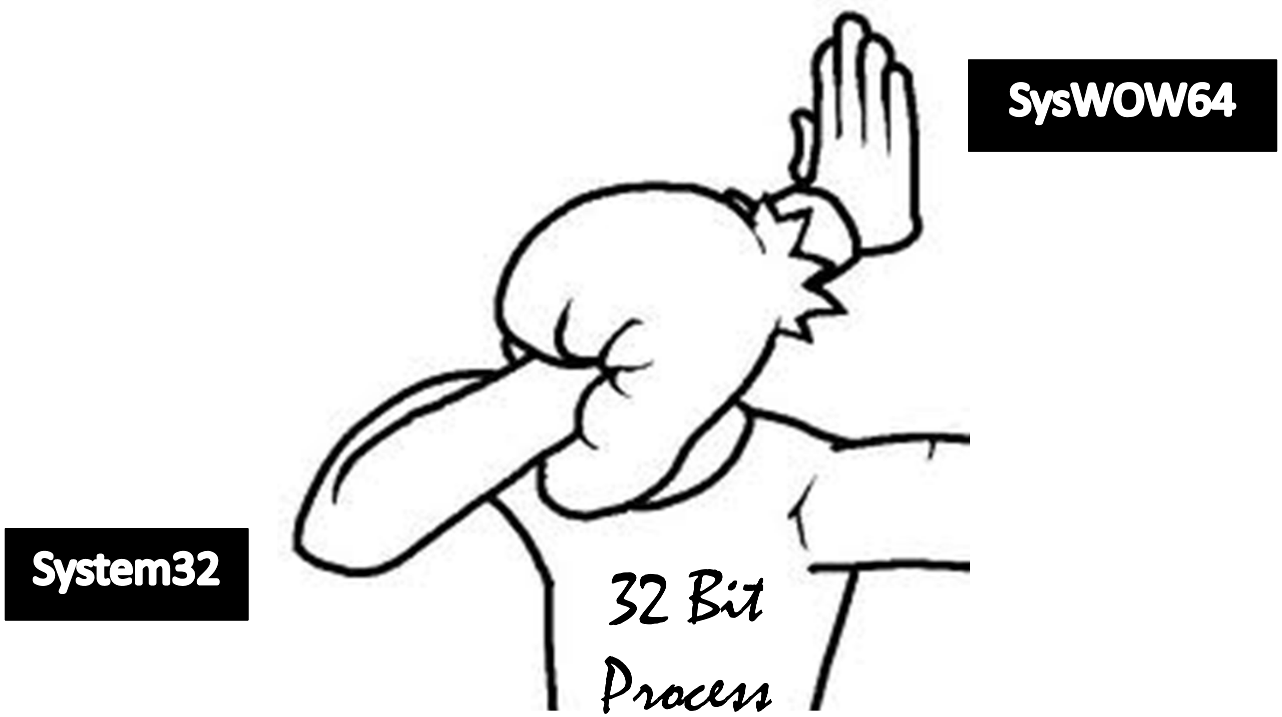
```
C:\Users\chrisu\Documents>md5sum C:\Windows\system32\ieapfltr.dll
ee9d715af1b928982f417238b9914484  C:\Windows\system32\ieapfltr.dll
C:\Users\chrisu\Documents>_
```

Good!

Malicious!

32 Bit	64 Bit
C:\Windows\SysWOW64\ieapfltr.dll	C:\Windows\system32\ieapfltr.dll
ee9d715af1b928982f417238b9914484	8eada158d964e3fd1999ad96c9c507ff

That's the WOW-Effect!



The root of our problem ...

File System Redirection

... is done centrally!

This should be done selectively!

Centrally? Selectively? WTF? ...

- Some Background:
  - 2 major things developers learn:
    - Keep your code modular
    - Try to avoid redundances

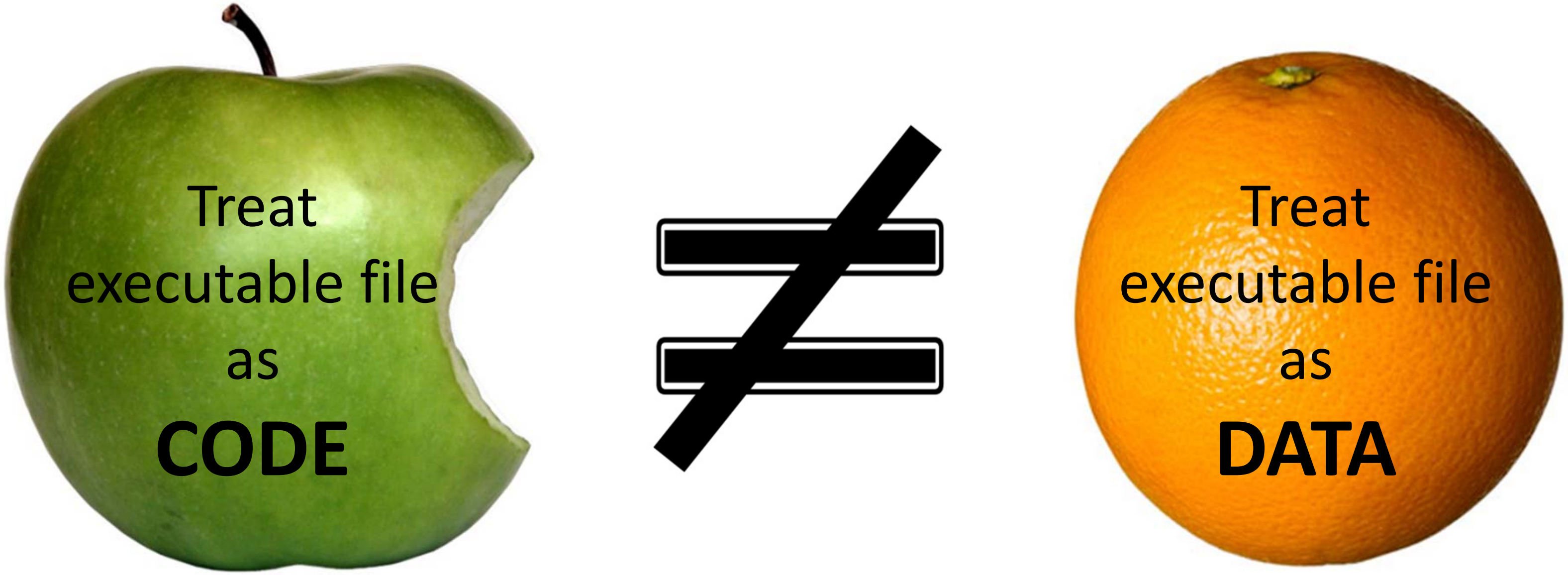
Best practice:

Changes are done in one "central" location.

➔ That's just the way WOW64 is doing redirection.

Don't compare apples and oranges ...

- BUT: This approach is only true when dealing with **only one unified view**
- But here we have **two views**!
- Comparing apples and oranges → Bad idea!

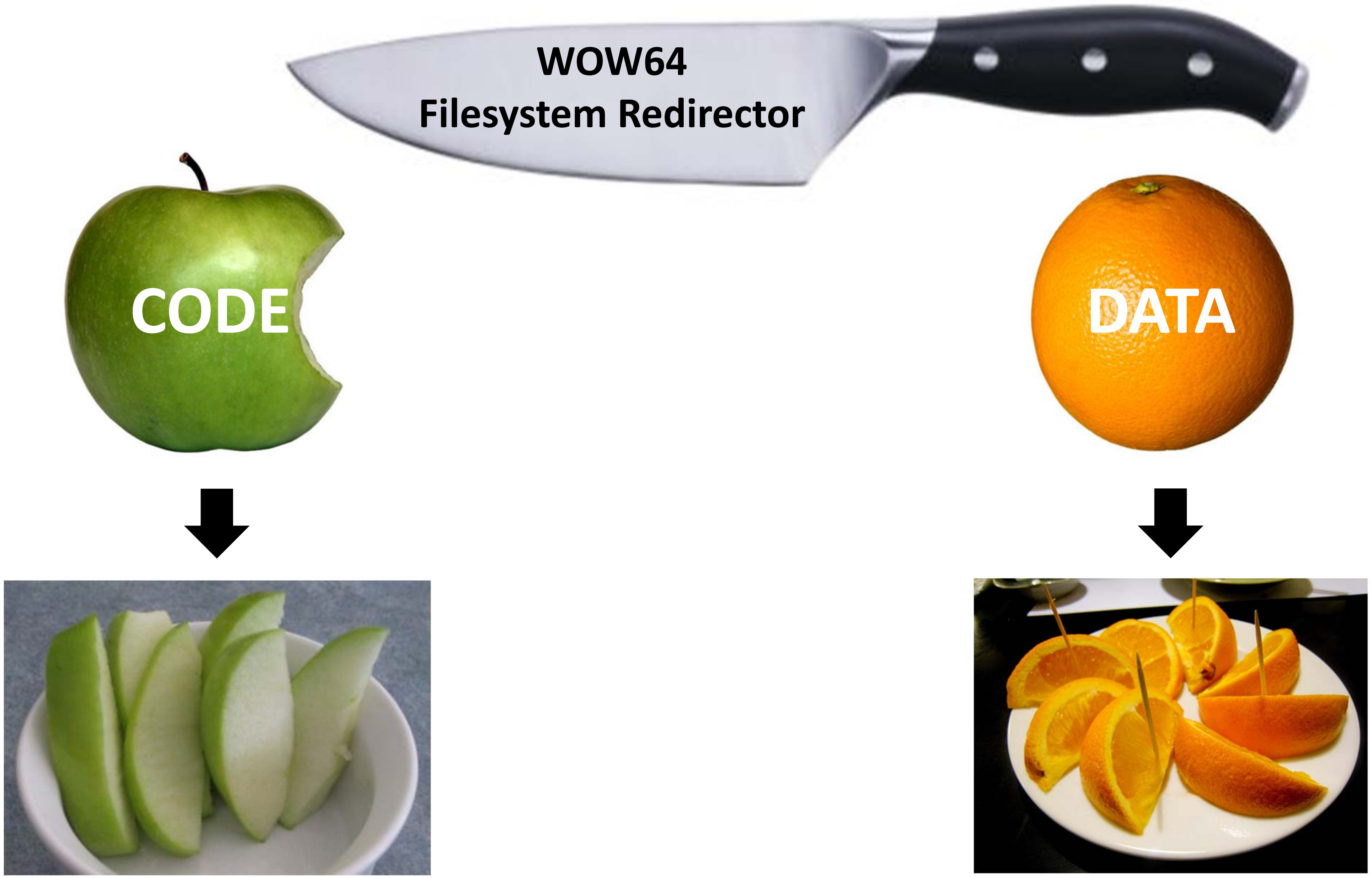


Treat executable file as **CODE**

≠

Treat executable file as **DATA**

How it SHOULD be done ...

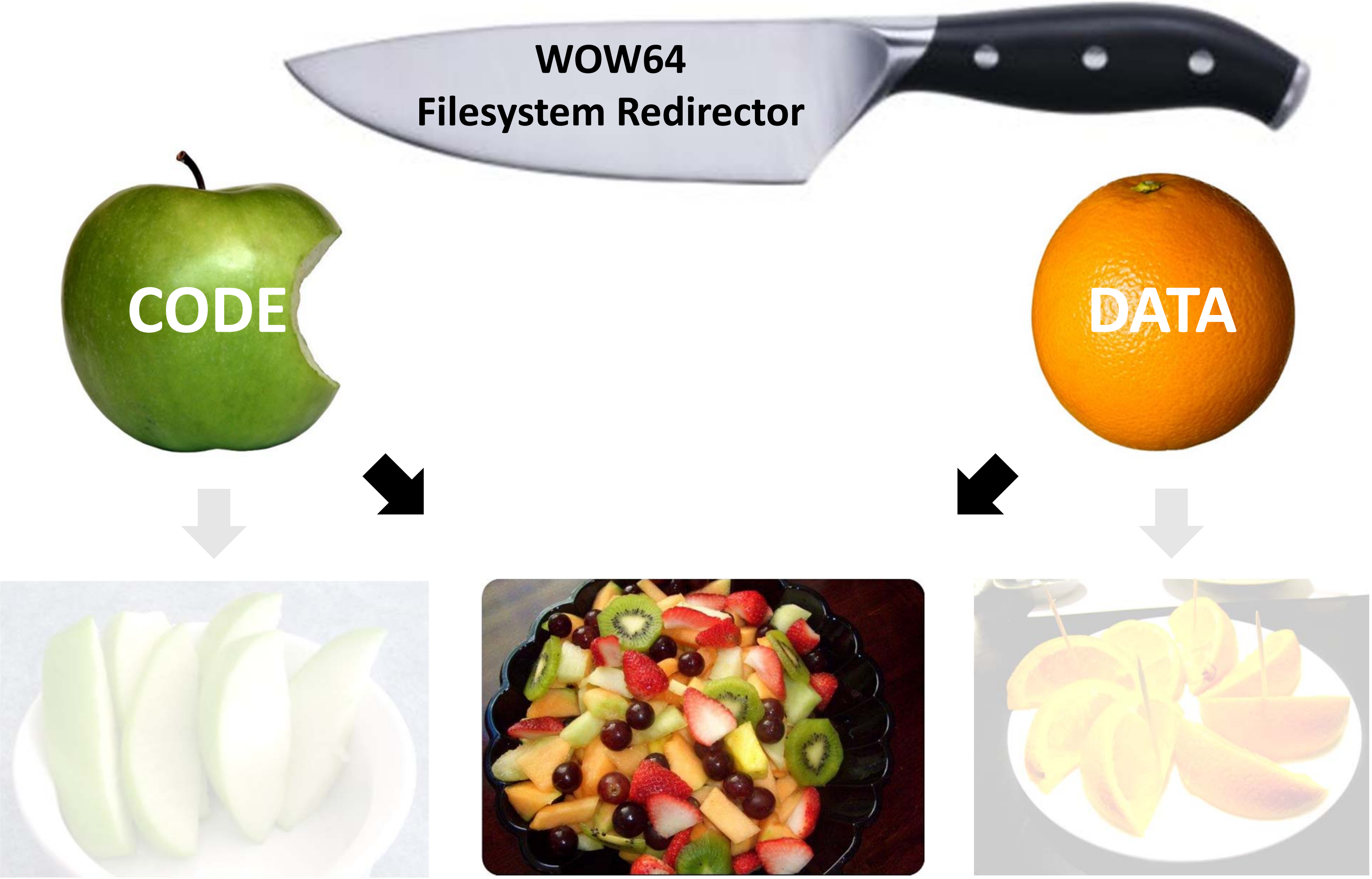


WOW64
Filesystem Redirector

CODE

DATA

How it IS done ...



WOW64
Filesystem Redirector

CODE

DATA

CODE or DATA access?

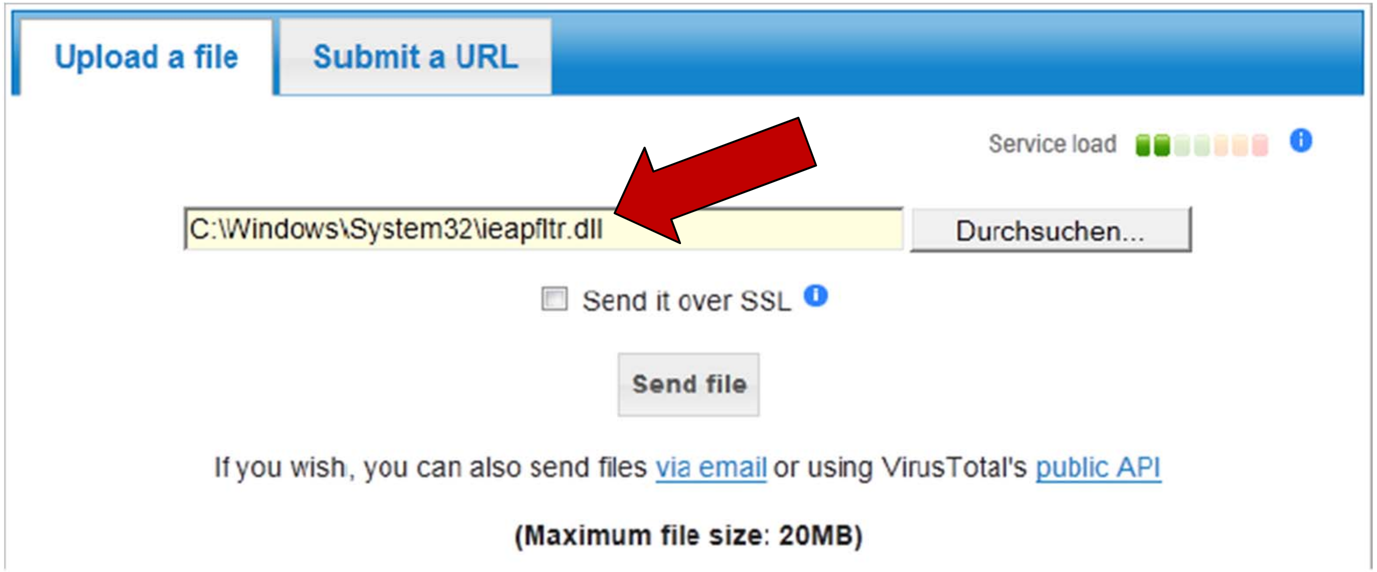
- How could Microsoft restrict WOW64 filesystem redirection to "code treatment" only?

⬇

- My suggestion: They should focus on the specifically "code-flavored" file-handling API functions
  - LoadLibrary
  - CreateProcess
  - ...
- ... instead of doing this centrally during PATH handling

Impact: Virus Total

- Checking via Virus Total



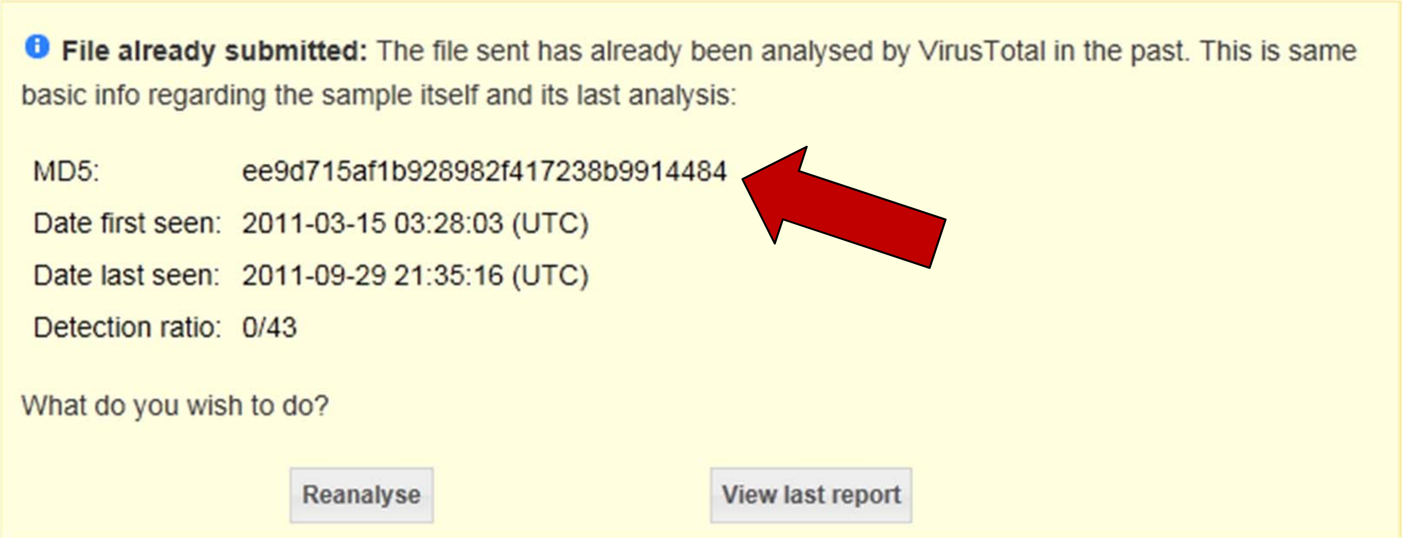
C:\Windows\System32\ieapfltr.dll

□ Send it over SSL

If you wish, you can also send files via email or using VirusTotal's public API

(Maximum file size: 20MB)

Impact: Virus Total



File already submitted: The file sent has already been analysed by VirusTotal in the past. This is same basic info regarding the sample itself and its last analysis:

MD5:	ee9d715af1b928982f417238b9914484
Date first seen:	2011-03-15 03:28:03 (UTC)
Date last seen:	2011-09-29 21:35:16 (UTC)
Detection ratio:	0/43

What do you wish to do?

Good!

Malicious!

32 Bit	64 Bit
C:\Windows\SysWOW64\ieapfltr.dll	C:\Windows\system32\ieapfltr.dll
ee9d715af1b928982f417238b9914484	8eada158d964e3fd1999ad96c9c507ff

Browsers?!

- Most of the browsers out there are 32 Bit
  - 64 Bit versions are becoming available, eventually.
- 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
- So, depending on the scenario
  - you get wrong files or
  - entirely miss files

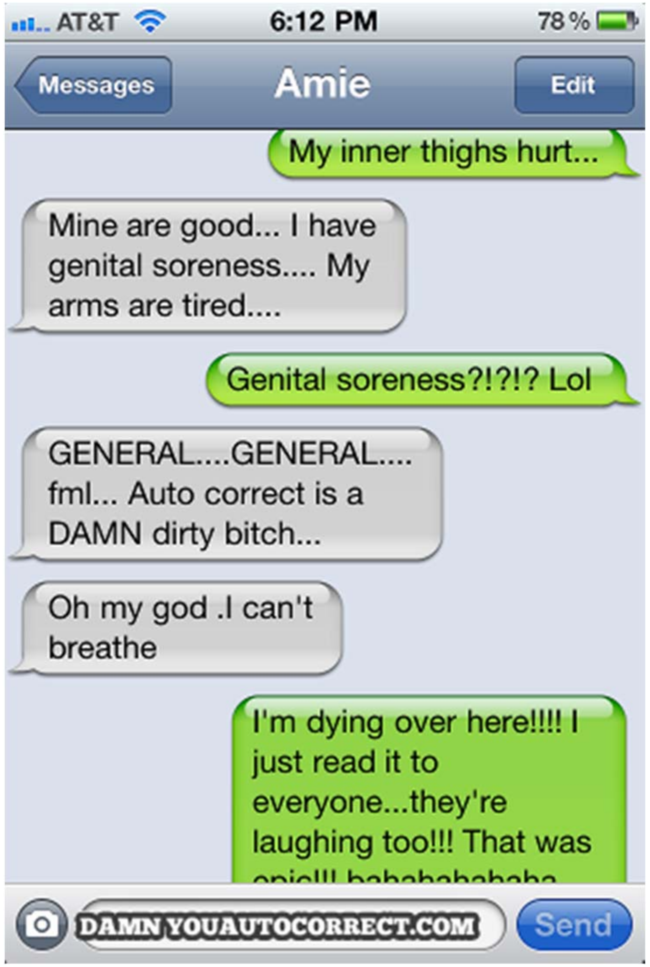
Registry Redirector

- 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
- WOW64 knows 3 Modes to handle Registry access. Specific Registry keys are ...
    - shared
      ≡ same object
    - reflected (< Windows 7 / Server 2008 R2)
      ≡ same value (automatically synchronized)
    - **redirected** (← Not so awesome!)

Redirected Keys

Registry-Key	Before Windows 7 and Server 2008 R2	Since Windows 7 and Server 2008 R2
HKLM\SOFTWARE	Redirected	Redirected
HKLM\SOFTWARE\Classes	Redirected and reflected	Shared
HKLM\SOFTWARE\Classes\Appid	Redirected and reflected	Shared
HKLM\SOFTWARE\Classes\CLSID	Redirected and reflected	Redirected
HKLM\SOFTWARE\Classes\DirectShow	Redirected and reflected	Redirected
HKLM\SOFTWARE\Classes\Interface	Redirected and reflected	Redirected
HKLM\SOFTWARE\Classes\Media Type	Redirected and reflected	Redirected
HKLM\SOFTWARE\Classes\MediaFoundation	Redirected and reflected	Redirected
HKLM\SOFTWARE\Clients	Redirected	Shared
HKLM\SOFTWARE\Microsoft\COM3	Redirected and reflected	Shared
HKLM\SOFTWARE\Microsoft\EventSystem	Redirected and reflected	Shared
HKLM\SOFTWARE\Microsoft\Notepad\DefaultFonts	Redirected	Shared
HKLM\SOFTWARE\Microsoft\OLE	Redirected and reflected	Shared
HKLM\SOFTWARE\Microsoft\RPC	Redirected and reflected	Shared
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths	Redirected	Shared
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers	Redirected	Shared
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\DriveIcons	Redirected	Shared
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\KindMap	Redirected	Shared
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\PreviewHandlers	Redirected	Shared
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Console	Redirected	Shared
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink	Redirected	Shared
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Gre_Initialize	Redirected	Shared
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	Redirected	Shared
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Language Pack	Redirected	Shared
HKCU\SOFTWARE\Classes	Redirected and reflected	Shared
HKCU\SOFTWARE\Classes\Appid	Redirected and reflected	Shared
HKCU\SOFTWARE\Classes\CLSID	Redirected and reflected	Redirected
HKCU\SOFTWARE\Classes\DirectShow	Redirected and reflected	Redirected
HKCU\SOFTWARE\Classes\Interface	Redirected and reflected	Redirected
HKCU\SOFTWARE\Classes\Media Type	Redirected and reflected	Redirected
HKCU\SOFTWARE\Classes\MediaFoundation	Redirected and reflected	Redirected

"Damn autocorrect!"



My inner thighs hurt...

Mine are good... I have genital soreness.... My arms are tired....

Genital soreness?!?!? Lol

GENERAL....GENERAL.... fml... Auto correct is a DAMN dirty bitch...

Oh my god .I can't breathe

I'm dying over here!!!! I just read it to everyone...they're laughing too!!! That was epic!!! hahahahahaha

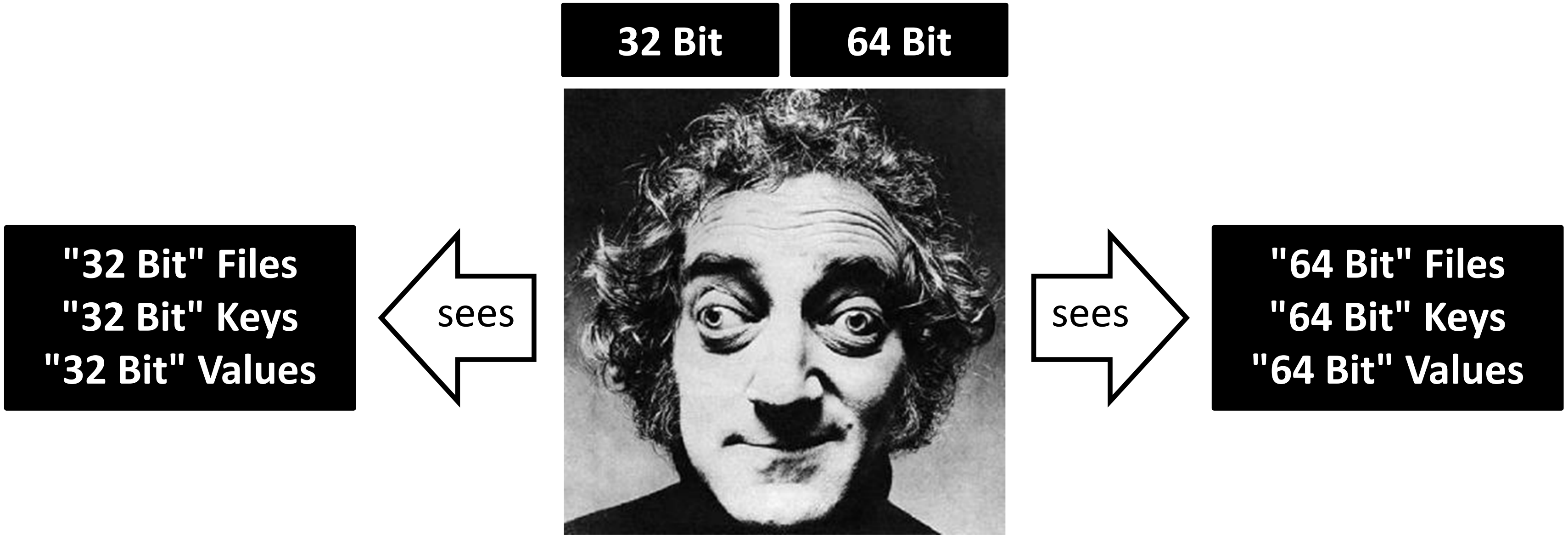
Autocorrected Values → Now, this must be a joke!?

- 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

64 Bit

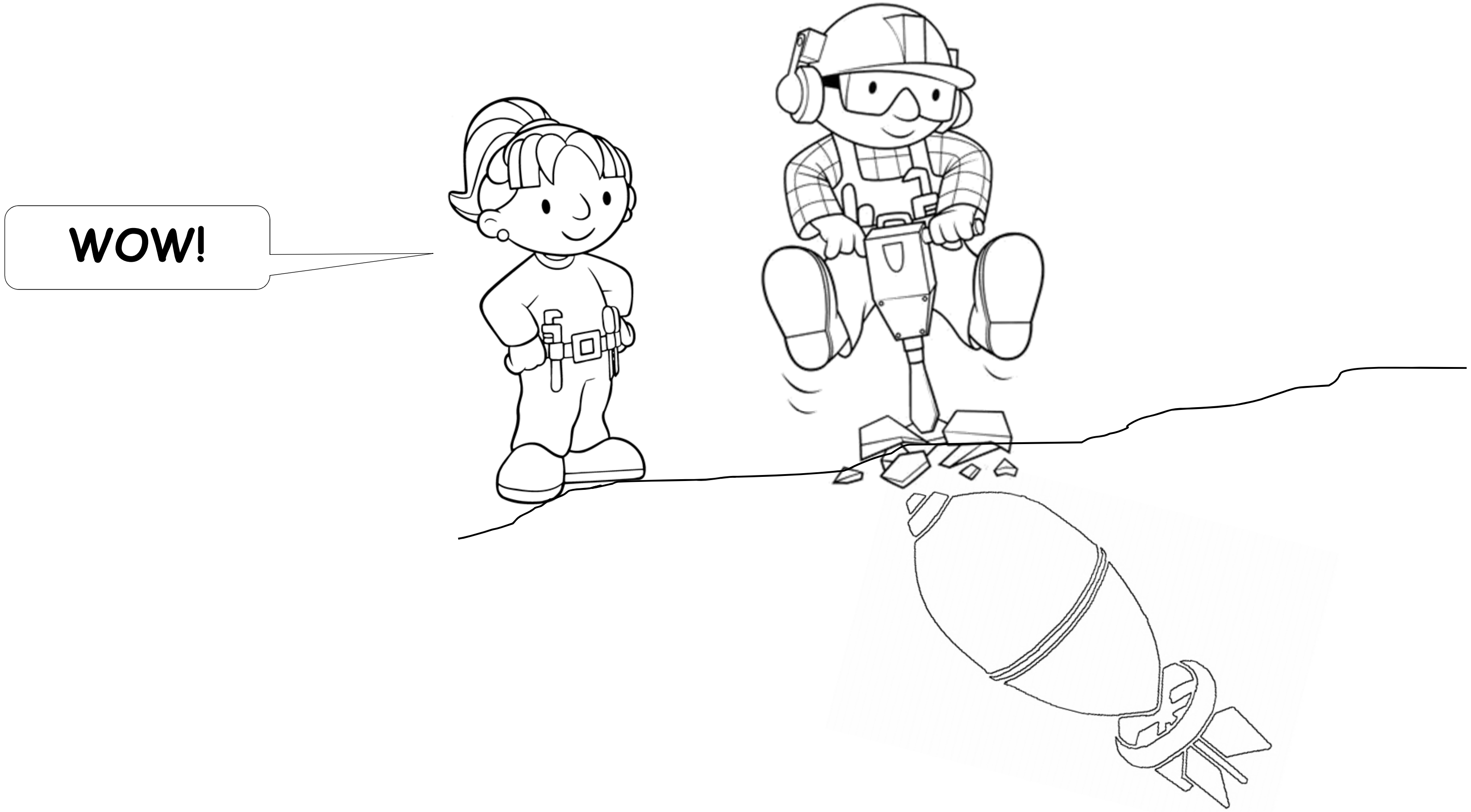
"32 Bit" Files
"32 Bit" Keys
"32 Bit" Values

sees

sees

"64 Bit" Files
"64 Bit" Keys
"64 Bit" Values

Impacts ...



Impact: Our toolsets

→ Most of our tools are 32 Bit based!

- Why? ...
  - Everyone concentrated on 32 Bit in the past
  - Old, approved tools
  - Third-party tools (unknown author, no source) → cannot recompile
  - "Outdated" tools

Examples: Hexeditors, Disassemblers, Debuggers, PE Viewers, Resource Editors, ...

Impact: Quick'n'dirty tools

- ... might have a problem
  - Small, specialized removers/detectors for specific malware looking for files, filehashes, Registry keys and values
  - Filelist differs
  - Recursive copy tools
  - Signature scanning tools
  - ...
- 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 victim's system?
- Cygwin => only 32 Bit!

What about Anti-Virus?

- Easy to answer:
  "They know what they are doing." ... Hm?
- Multiple components → all of them safe?
- 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
- Do they care for both worlds? - in the right way?

Solutions?

- None, in terms of patches
  - It's a **feature** not a bug
- Just be **AWARE**!
- Use **64 Bit tools** on 64 Bit Windows
- Bulletproof solution?
  - If you ask me: Be "**redundant**" (always both, 32 Bit and 64 Bit)
- Or, 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 ...

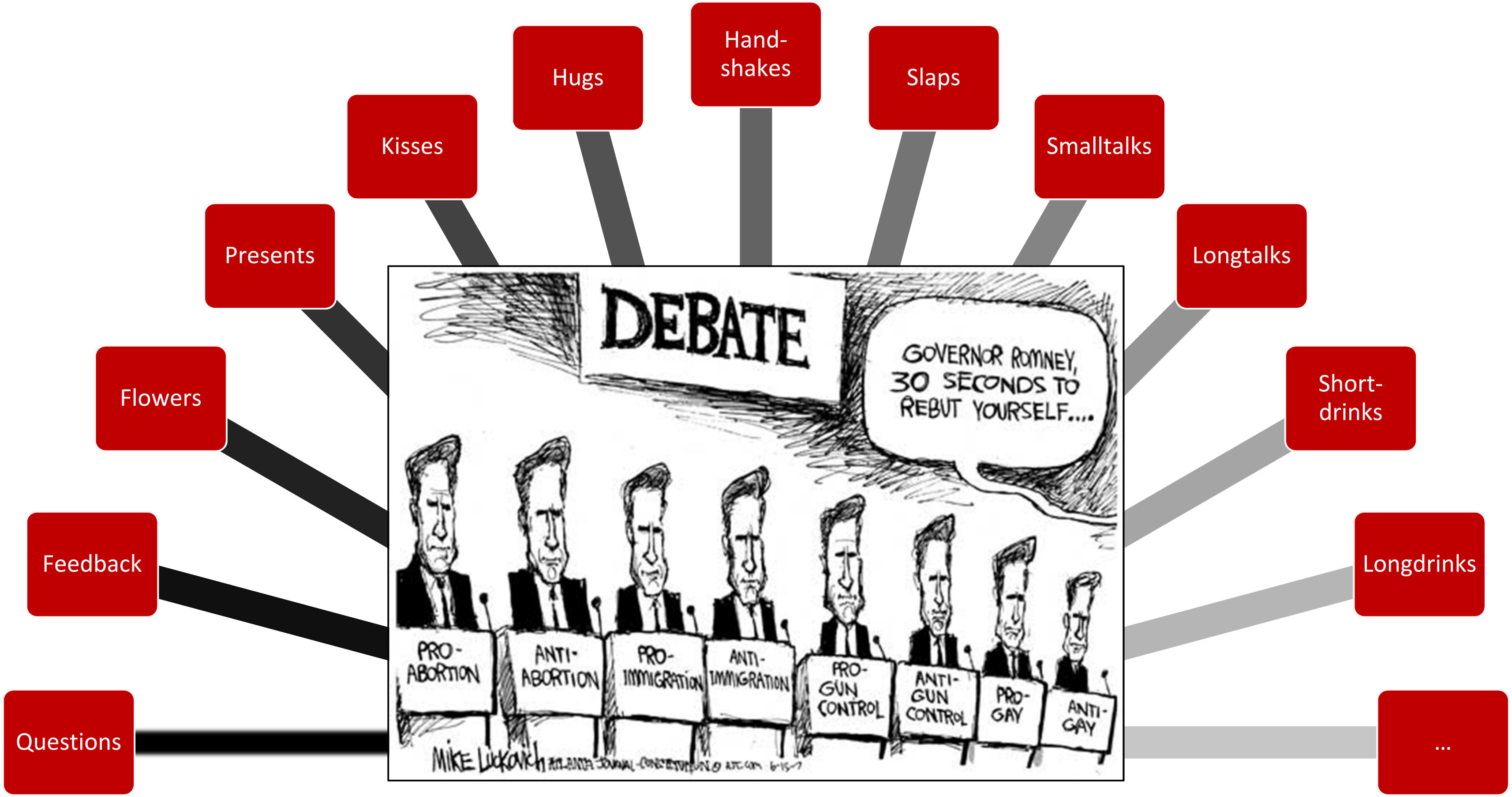
Choose your road to Rome

- 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

Action-Items	Progress
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?



Questions

Feedback

Flowers

Presents

Kisses

Hugs

Hand-shakes

Slaps

Smalltalks

Longtalks

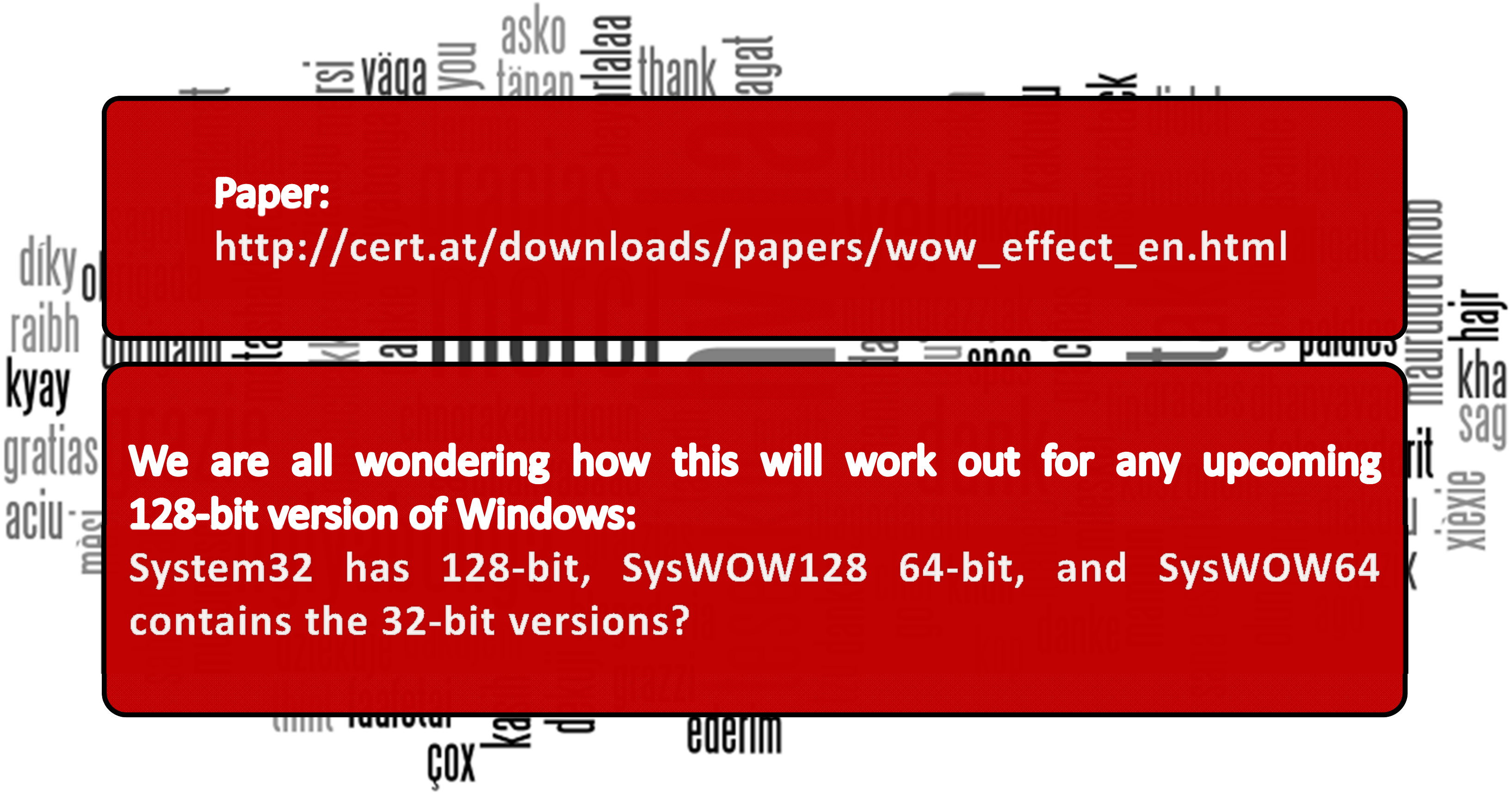
Short-drinks

Longdrinks

…

asko
bayarlalaa
thank
agat
väga
tänan
you
mersi
terima
salamat
leat
dziakuju
siyabonga
gracias
hvala
merci
wel
kiitos
vinaka
kakhulu
misaotra
tack
diolch
muchas
asante
lava
dankewol
arigatô
khob
sagolun
díky
obrigada
motashakkeram
dankie
mochchakkeram
raibh
obrigado
kyay
grazie
gratias
aciu
mèsi
chokrane
sah
multumesc
ngiyabonga
chnorakaloutioun
kam
dhanyabaad
tapadh
maith
tesekkur
nirringrazzjak
hamnida
tau
spas
dank
graciñas
takk
spacibo
paldies
mauruuru
hajr
kha
sag
tin
gràcies
dhanyavad
faleminderit
milesker
köszönöm
mahalo
mamnun
eskerrik
sana
edirem
olun
diakuiu
nizzik
ago
xièxie
gratzias
blagodaram
chai
khun
dankon
tzu
go
kop
danke
blagodaria
dziekuje
dakujem
thint
faafetai
kasih
dekuji
grazzi
ederim
çox

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



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?