AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

VOM SPAM ZUM TEST

Malware-Analyse bei der AV-TEST GmbH

Ulf Lösche
Head of Malware Research,
AV-TEST GmbH

- Unabhängig
- Herkunft
- Umfassend

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Wissen aus einer Hand!

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

> 100.000 URLs
> 1.000.000 Mails
> 1.700.000 Dateien
pro Tag

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

1.700.000

AV-TEST
multi scan

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

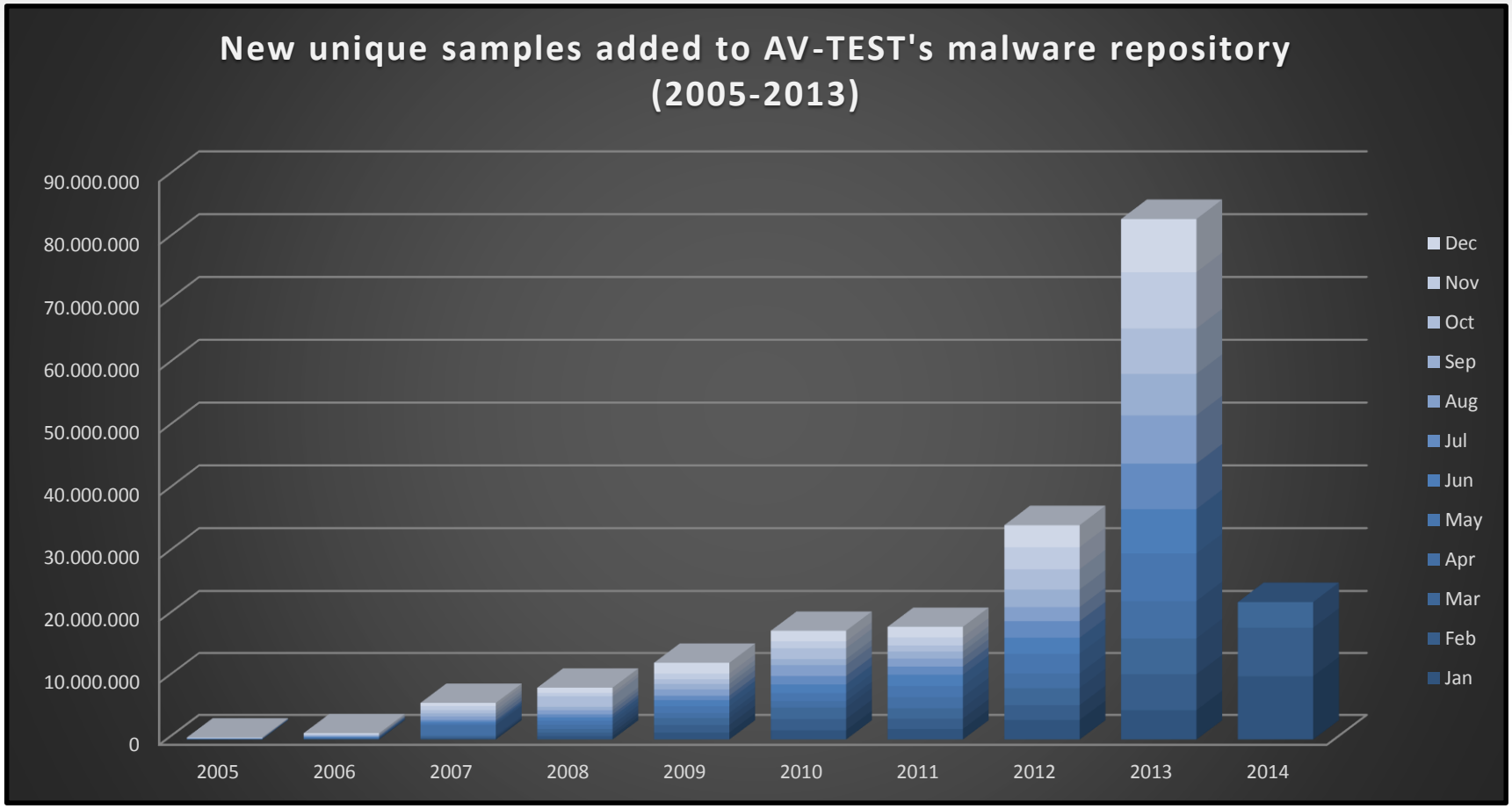
220.000

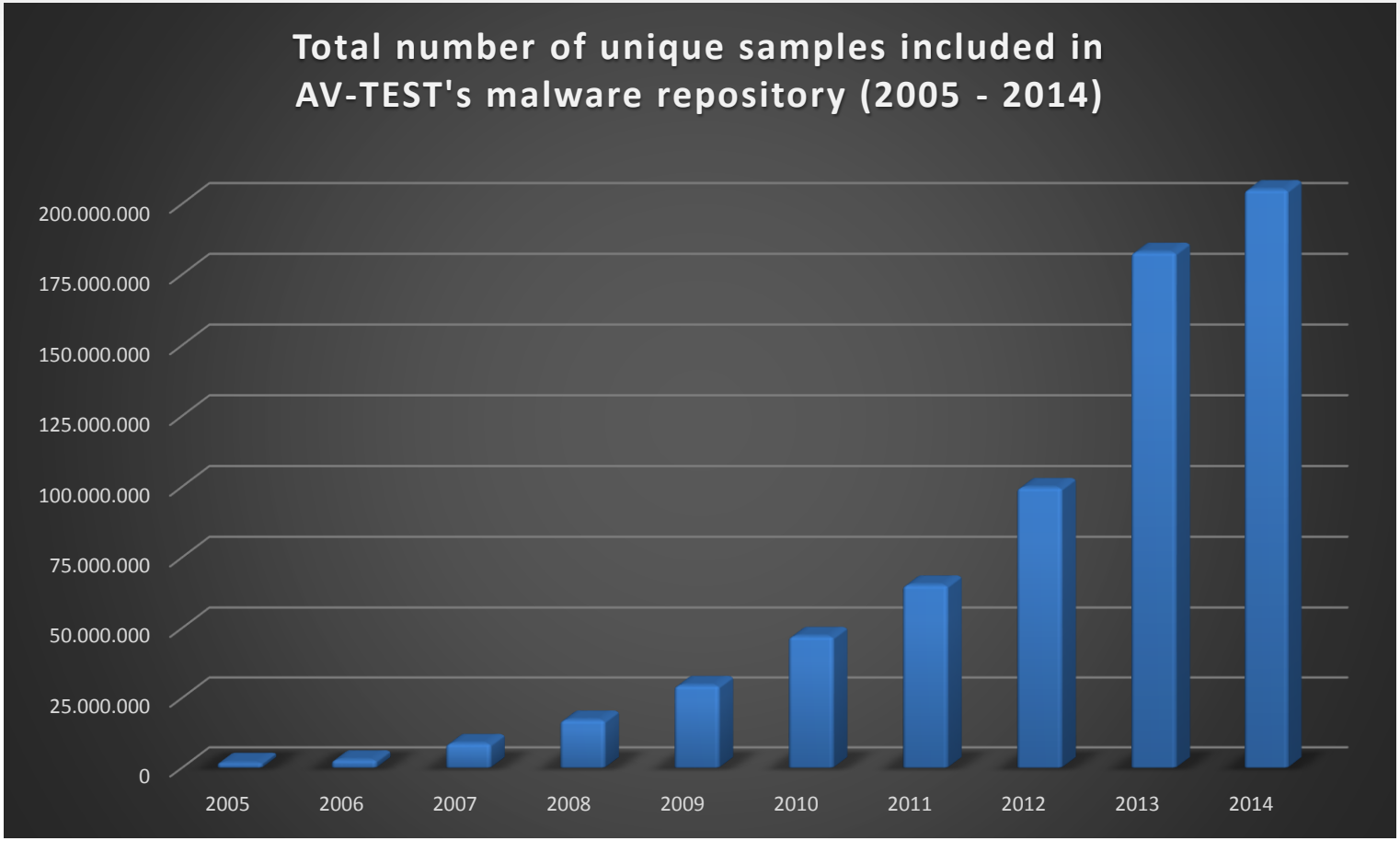
neue Malware-Samples

pro Tag

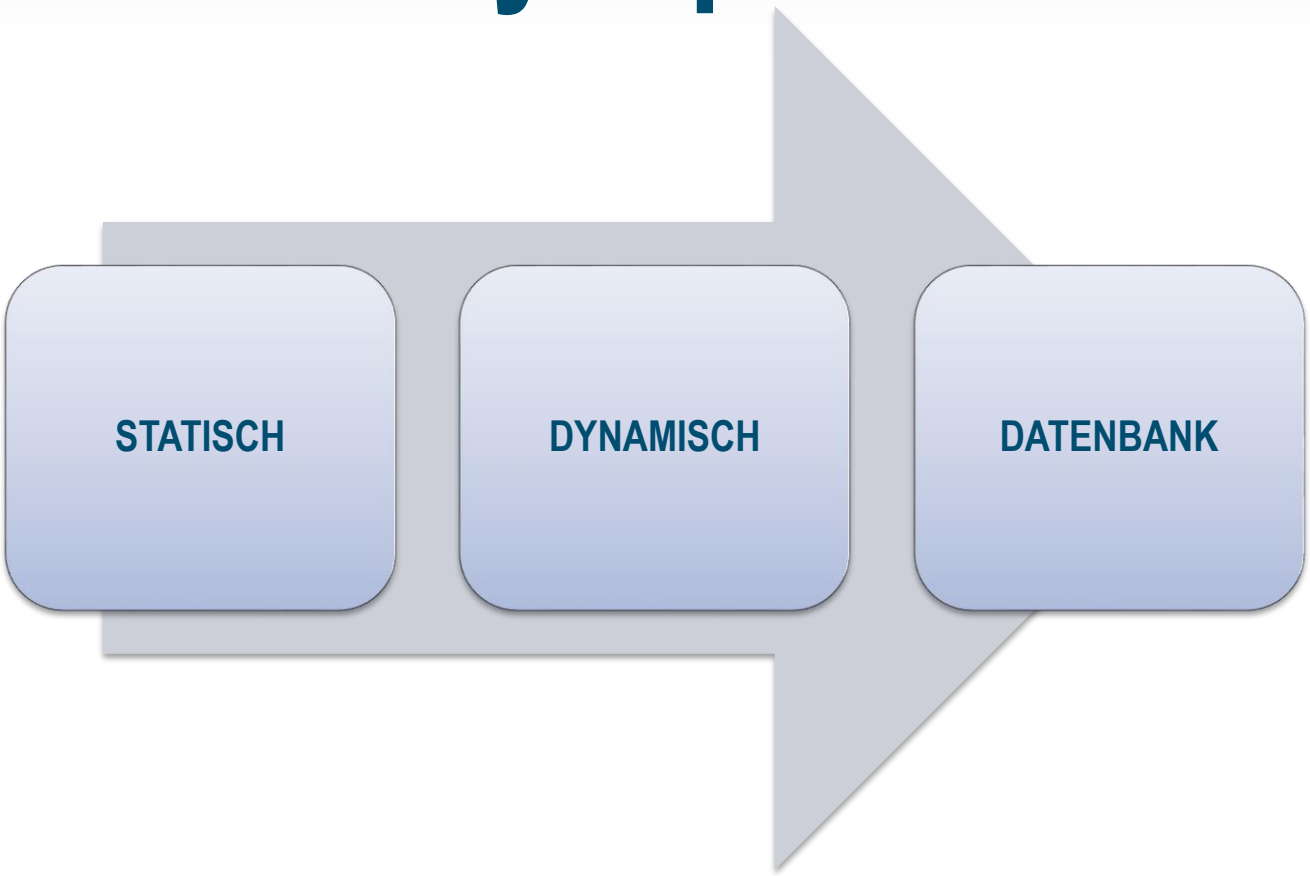
> 9.000

WIEVIEL?

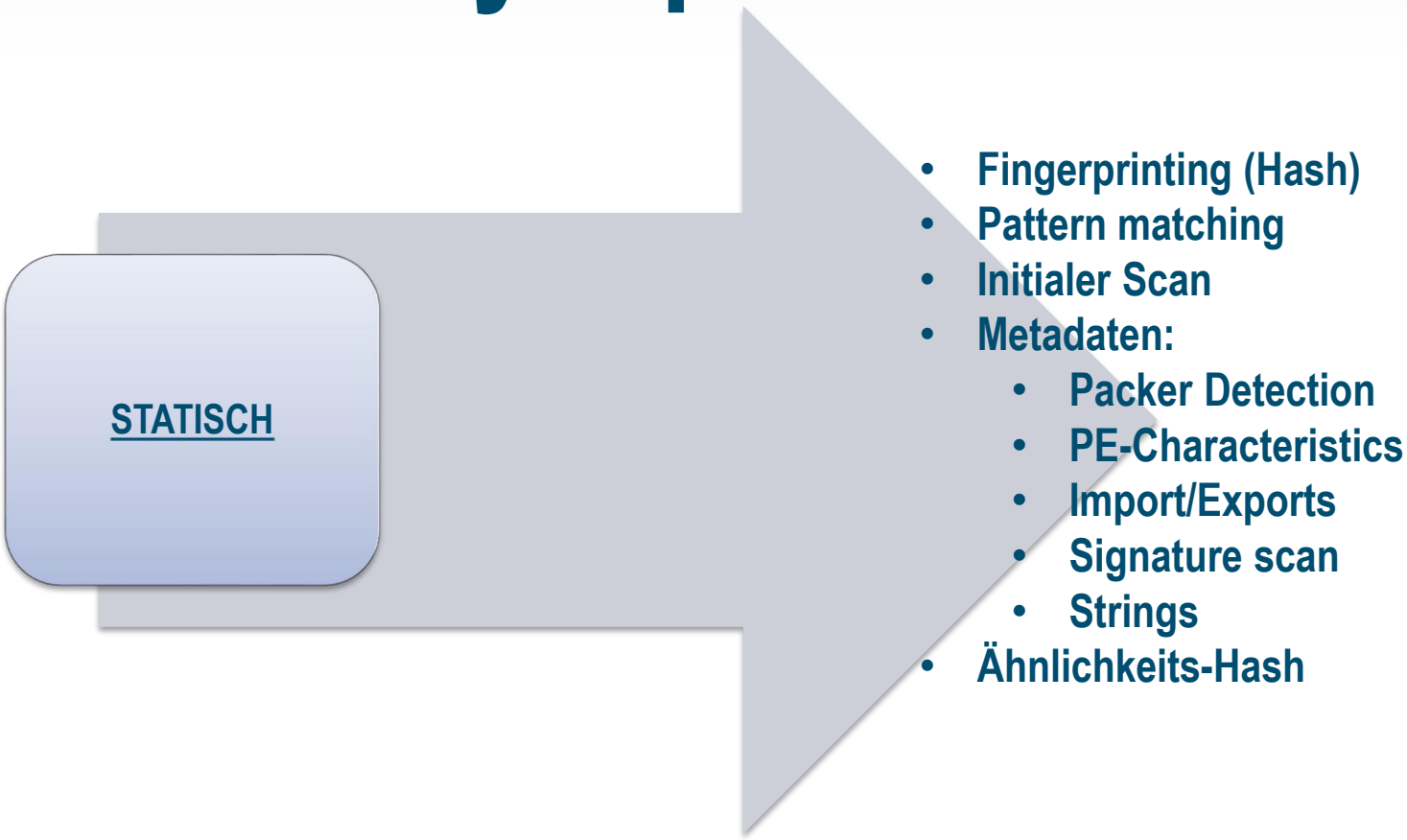

New unique samples added to AV-TEST's malware repository (2005-2013)
90.000.000
80.000.000
70.000.000
60.000.000
50.000.000
40.000.000
30.000.000
20.000.000
10.000.000
0
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
Dec
Nov
Oct
Sep
Aug
Jul
Jun
May
Apr
Mar
Feb
Jan


Total number of unique samples included in AV-TEST's malware repository (2005 - 2014)
200.000.000
175.000.000
150.000.000
125.000.000
100.000.000
75.000.000
50.000.000
25.000.000
0
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014

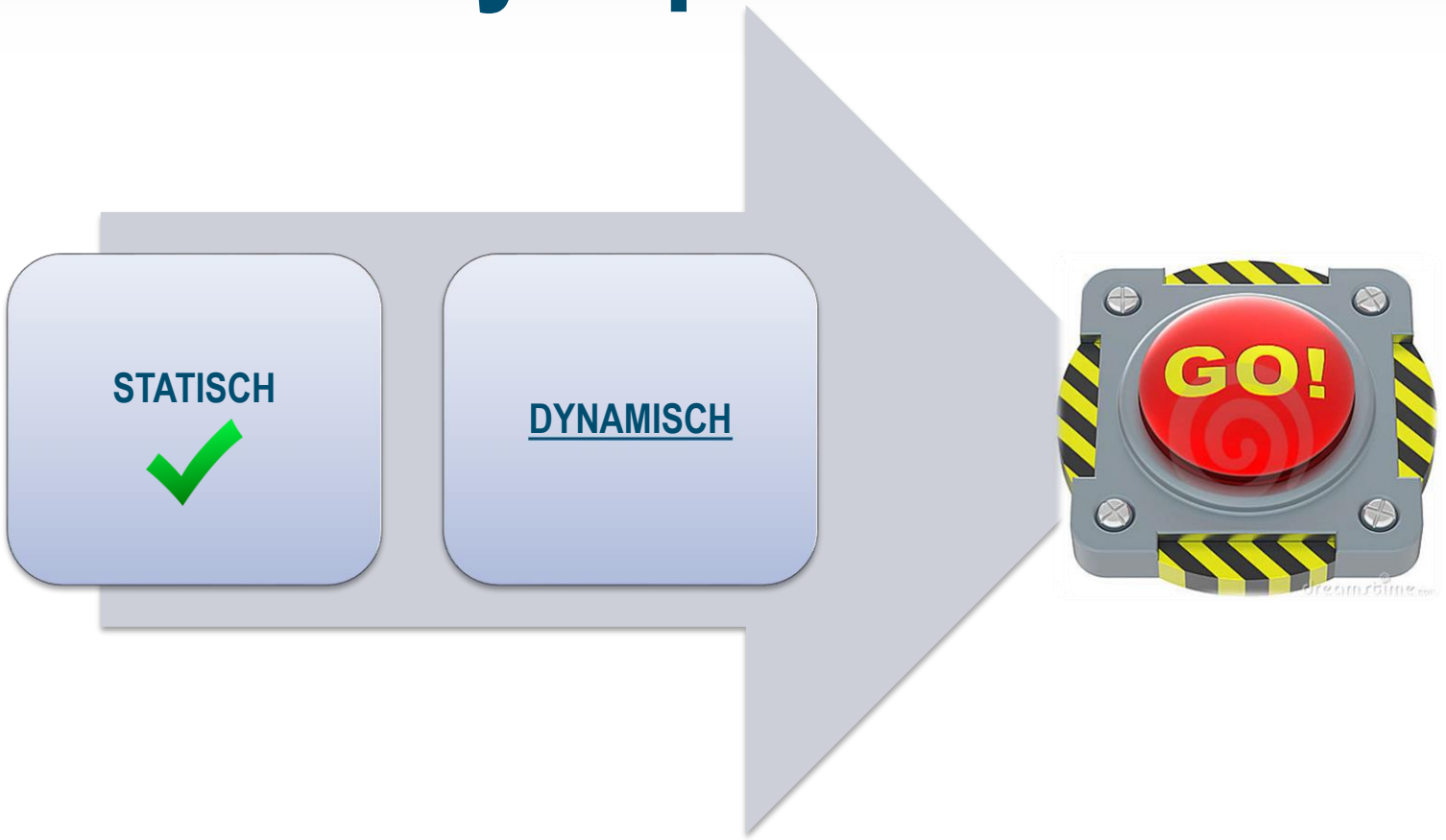
Analyseprozess



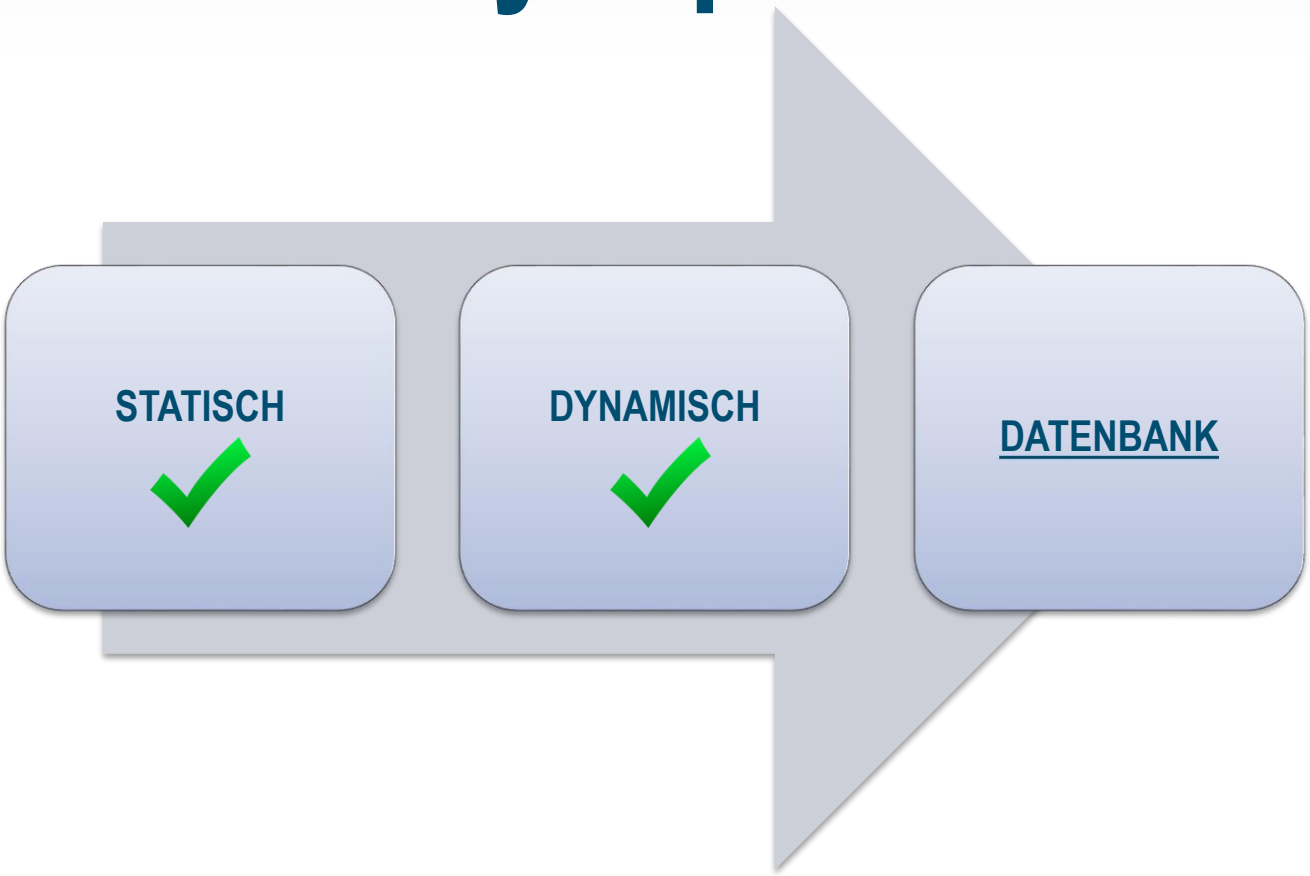
Analyseprozess



Analyseprozess



Analyseprozess



WIE?


Sapas - AV-TEST - The Ind
:8080/sapas-web/index.jsf
Classify ▸ ClassifyGrid ▸ SampleView
Statistics
Type | WAITING | READY | RUNNING | FAILED | DONE
VTEST | 0 | 0 | 46 | 61 | 1289934
EXIF | 0 | 0 | 0 | 291 | 1289750
PE | 0 | 0 | 0 | 53 | 1289988
PE_INFO | 0 | 0 | 0 | 87 | 1289954
PE_DUMP | 0 | 0 | 0 | 2282 | 1288481
SOLAR | 329472 | 0 | 13 | 50275 | 910281
CLASSIFY | 378486 | 0 | 0 | 1139 | 910416
Tasks (lastRefresh: 14:28:53 UTC)
Last | MALWARE | JUNK | GOODWARE | UNDEFINED
DAY | 683 (75 %) | 54 (5 %) | 171 (18 %) | 1 (0 %)
WEEK | 5890 (55 %) | 2835 (26 %) | 1811 (17 %) | 8 (0 %)
MONTH | 15849 (41 %) | 12733 (33 %) | 9847 (25 %) | 15 (0 %)
QUARTER | 34357 (28 %) | 61101 (50 %) | 25418 (20 %) | 940 (0 %)
YEAR | 209811 (27 %) | 415123 (55 %) | 126158 (16 %) | 1900 (0 %)
Classifiers
URLs
Samples
URLs / new Samples acquired last 24hrs
UNDEFINED
MALWARE
JUNK
GOODWARE
Classifiers acquired last 24hrs
Latest Samples (initial sorting and filtering of * columns can take some time)
url-prefilters (use % and !)
name-prefilters (use % and !)
sha256-prefilters
pedHash-prefilters
vtest-prefilters (use % and !)
WebdustPE
WebdustMail
MALWARE
JUNK
GOODWARE
Sample Date min 14-02-14 13:48 max 14-03-04 14:28
Load max 300
Zip selected
Select All
Deselect All
Reset Site
(10 of 10)
*Path URL | *Incident Name | Sample Date | Sha256 | Size | Sample notPe* | PEDHash | *VTest | *Class. | *Conf.
http://.../1393561140/setup_21_ | setup_21_15530380.exe | 14-03-03 11:19 | 859c3db5 | 518072 | view | e5bb386b53 | 0 % | | |
http://.../exes/2.3.80.2.au. | mwsauto.exe | 14-03-03 11:16 | 68635346 | 75456 | view* | 31d651d4a8 | 40 % | | |
http://...38/down/802/se2611-10 | se2611-105-1-45188.exe | 14-03-03 11:14 | 18eaffbca | 91760 | view | 6d6d11b414 | 40 % | GOODWARE | 95,78 %
http://.../backup/UserRese | UserReset_infoclear.exe | 14-03-03 11:12 | 633ca6ef | 205376 | view | 958b056a1b | 24 % | JUNK | 0,00 %
http://.../down/1244/%E5%9 | 在线看HI片38J-101-700.exe | 14-03-03 11:10 | 2a0a405d | 92786 | view | 06237579d9 | 40 % | GOODWARE | 95,78 %
http://.../hx/pskin(0.0.909.1 | pskin(0.0.909.1-0.0.911.2)_360.exe | 14-03-03 11:09 | 75cb3c6b | 7221880 | view | 04c5e8dd6d | 0 % | | |
mail://.../2fb5985 | vkr.jpg | 14-03-03 11:08 | f103d5f0 | 37560 | view* | | 0 % | | |
http://.../300/SE2814-10 | SE2814-105-1-34835.exe | 14-03-03 11:07 | 7402a4f4 | 65643 | view | 22f82f74fa8 | 24 % | GOODWARE | 52,79 %
http://.../mediaview/exe/MediaV | MediaViewV1alpha3360Installer.exe | 14-03-03 11:03 | 00cf41f03 | 647925 | view | e4a6a1f886 | 68 % | MALWARE | 80,42 %
http://.../radio/player.exe | player.exe | 14-03-03 11:03 | 5cd07f5f5 | 1904640 | view | f432b8e84d5 | 4 % | JUNK | 0,00 %
http://...99/hezi/dnfbox. | dnfbox.exe | 14-03-03 11:03 | c3d74d1f | 4186045 | view | 70769c8202 | 92 % | JUNK | 0,00 %
http://.../exe/MediaV | MediaViewV1alpha2428Installer.exe | 14-03-03 11:02 | 2be85a37 | 647888 | view | 13981be94e | 68 % | MALWARE | 80,42 %
http://.../new8/ÎçÒ¹ÐiµçÓº¾I | ÎçÒ¹ÐiµçÓº¾IxDh_48_103.exe | 14-03-03 11:01 | 331ababb | 1274656 | view | 7a76751433 | 4 % | GOODWARE | 95,78 %
http://.../mediaview/exe/MediaV | MediaViewV1alpha2298Installer.exe | 14-03-03 11:00 | 37b9b93 | 647893 | view | 439c7df5db6 | 64 % | MALWARE | 80,42 %
http://.../v0_silent/qsyysetup | qsyysetupslientad_1024.exe | 14-03-03 11:00 | d31ca248 | 1864047 | view | 0f1c82943c7 | 28 % | MALWARE | 80,42 %
http://.../yrekzs.exe | yrekzs.exe | 14-03-03 11:00 | fb496bcd | 688810 | view | 2e756d272b | 12 % | MALWARE | 99,11 %
http://.../kplay.exe?_upd=setu | setup_28054250.exe | 14-03-03 10:59 | 51352e8 | 98121 | view | 17ef94cb491 | 0 % | MALWARE | 80,42 %
http://.../mediaview/exe/MediaV | MediaViewV1alpha3523Installer.exe | 14-03-03 10:58 | 9a9eb349 | 647911 | view | 94b92e5382 | 72 % | MALWARE | 80,42 %
http://.../mediaview/exe/MediaV | MediaViewV1alpha3097Installer.exe | 14-03-03 10:58 | 1c2ff75a4 | 647901 | view | 847deef615 | 64 % | MALWARE | 80,42 %
http://.../installer | ZeNiX2014-01-11_downloader-6NlC6wLV.exe | 14-03-03 10:58 | 4c0d3d3c | 237016 | view | 874aff945e8 | 32 % | | |
http://.../n/3.0.30 | Anti-Malware.exe | 14-03-03 10:57 | bad9092e | 293608 | view | 6f39f410c8e | 28 % | | |
http://.../exe/MediaV | MediaViewV1alpha1166Installer.exe | 14-03-03 10:56 | a3539fb1 | 647889 | view | 25da2bc52b | 64 % | MALWARE | 80,42 %
http://.../lay.exe?_upd=setu | setup_28010849.exe | 14-03-03 10:55 | 0a2a28ef | 96127 | view | 3f5ff96276b | 0 % | GOODWARE | 88,26 %
http://.../down/324/vip%C2%A | vip | 14-03-03 10:49 | c85aa9f7 | 75312 | view | 8c47625988 | 28 % | | |
http://...88/down/123/vip-101-2 | vip-101-204-207477.exe | 14-03-03 10:49 | b4fdafeb | 66675 | view | 6cf7acbec27 | 28 % | | |
http://...com/n/3.0.3 | Smilebox.exe | 14-03-03 10:49 | eadd23e | 293608 | view | 6ae9de5eed | 28 % | | |
http://...n/3.0.3 | Camtasia.exe | 14-03-03 10:49 | e60826c0 | 295328 | view | e3a7990761 | 28 % | | |
http://...n/246/%E5%8D | 午夜小电影ef6-101-205-196942.exe | 14-03-03 10:49 | 0fad81d0 | 64623 | view | ac6ce379ea | 24 % | GOODWARE | 52,79 %
http://...n/335/AV1417-1 | AV1417-105-202-13251.exe | 14-03-03 10:49 | e54b97e | 62000 | view | 5ecf605a81c | 32 % | GOODWARE | 52,79 %
http://...n/267/??%C2%. | 267 | 14-03-03 10:49 | aad96e6c | 66160 | view | 1290f7cc21d | 28 % | GOODWARE | 52,79 %
(10 of 10)
Sapas - © 2013 AV-TEST - The Independent IT-Security Institute

Sample - 80f2ad148237030893761763e08cf2487dcb810087f2e0016a7630e054b7ad32	
Youngest Path Acquired	14-03-03 15:10
Youngest Path URI	mail:// [redacted] 25896cbb0c527925043e51a7b6453a48
Youngest Path Type	MAIL
Youngest Incident Acquired	14-03-03 15:10
Youngest Incident Name	2356869543.scr
Youngest Incident Extension	scr
Sample Acquired	14-03-03 15:10
Sample Size	142336
Sample MD5	4c91679bf60114f0f4015ae187fff599
Sample SHA1	f5512bc45c06cee9c3f3e2d48e7ea3bf4bebad18

[redacted]016a7630e054b7ad32	
[redacted]25	

avg	-	bitdefender	-
ca_av	-	clamav	-
esetnod32	Win32/Kryptik.BWFP trojan (variant)	fortinet	-
f_prot	W32/Trojan5.IYX	ikarus	Trojan-Spy.Zbot
k7computing	-	kaspersky	Trojan-Downloader.Win32.Agent.hebc
mcafee	Artemis!4C91679BF601 (trojan)	microsoft	-
norman	Heur.I	panda	-
quickheal	-	rising	-
sophos	Troj/Agent-AGFL	sunbelt	-
symantec	-	trendmicro	-
vba32	-	virusbuster	-
PE32 executable (GUI) Intel 80386, for MS Windows			

WIE?

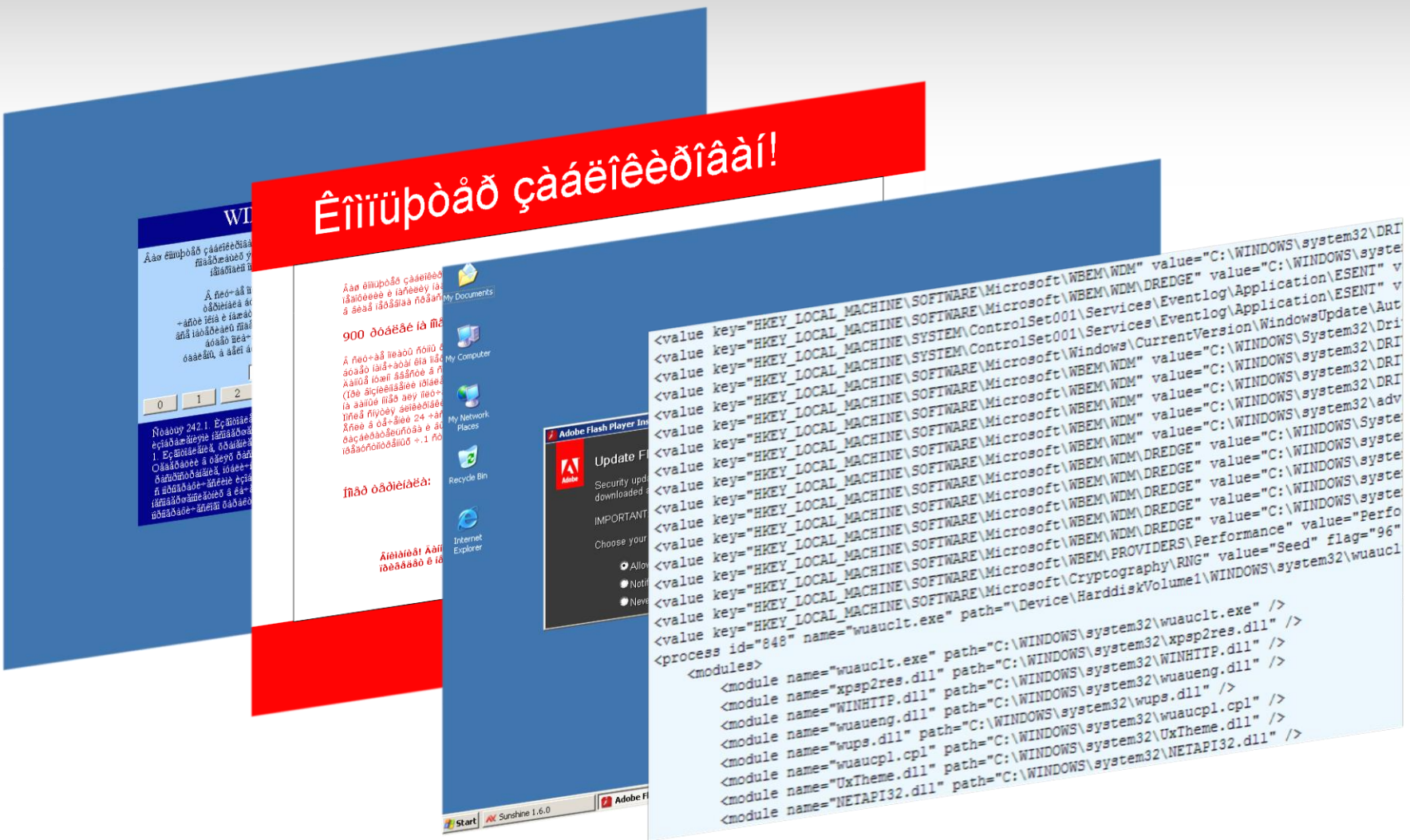
PEDump - 80f2ad14823703089376176 3e08cf2487dcb810087f2e0016a7630e054b7ad32

HashSha256	cb70f2bbde2d1c80a41686f4759f238aad0578ee2a549e8a893db51a78f209d3

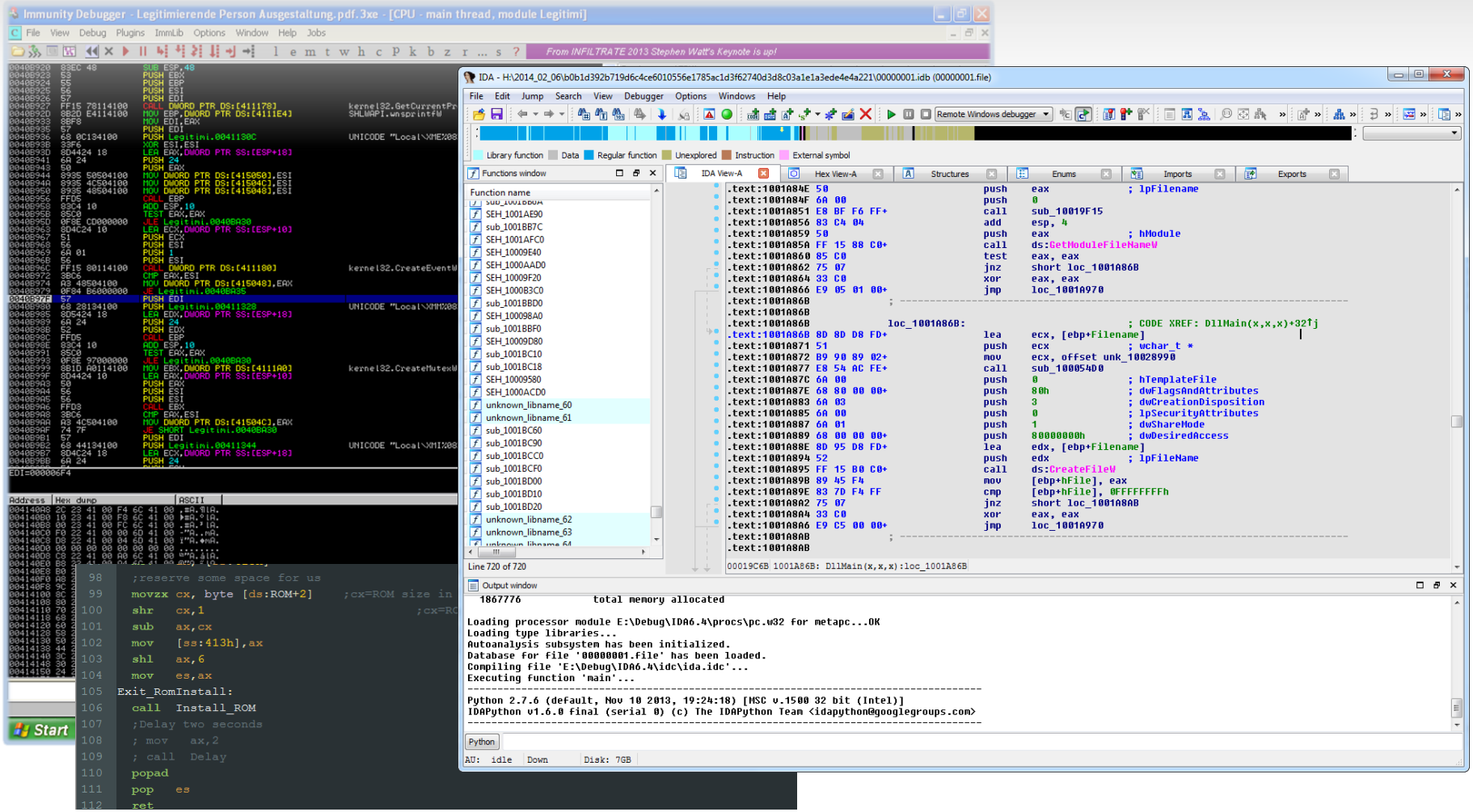
```
Dump of file  : S:\SAMPLES\80\F2\80F2AD14823703089376176 3E08CF2487DCB810087F2E0016A7630E054B7AD32
FileSize      : 0x0000000000022C00
PEDumpVersion : 0.2.7.63

<DOSHEADER
  DOSHeader Magic              0x5A4D 'MZ'
  DOSHeader size (para)        0x0004
  DOSHeader checks             0x0000
  DOSHeader STUBSize           0x00A8
DOSHEADER>

<File Header
  Machine:                     0x014C (I386)
  Number of Sections:          0x0004
  TimeDateStamp:               0x47274513 ->
  PointerToSymbolTable:        0x00000000
  NumberOfSymbols:             0x00000000
  SizeOfOptionalHeader:        0x00E0
  Characteristics:             0x0123
    IF_RELOCS_STRIPPED
    IF_EXECUTABLE_IMAGE
    IF_LARGE_ADDRESS_AWARE
    IF_32BIT_MACHINE
File Header>

<Optional Header
  Magic                        0x010B
  linker version               9.00
  size of code                 0x00018C00
  size of initialized data     0x0000CC00
  size of uninitialized data   0x00000000
  entrypoint RVA               0x00015AF6
  base of code                 0x00001000
  base of data                 0x0001A000
  image base                   0x00400000
  section alignment            0x00001000
  file alignment               0x00000200
  required OS version          5.00
  image version                7.01
  subsystem version            5.00
  Win32 Version                0x00000000
  size of image                0x00028000
  size of headers              0x00000400
  checksum                     0x0002B58C
```

File Modification	14-03-03 15:15:00
File Access	14-03-03 15:15:00
File Creation	14-03-03 15:15:00
File Type	Win32 EXE
MIME Type	application/octet-stream

Line	Name	Value
10	Machine Type	Intel 386 or later, and compatibles
11	Time Stamp	2007:10:30 14:52:03+00:00
12	PE Type	PE32
13	Linker Version	9.0
14	Code Size	101376
15	Initialized Data Size	52224
16	Uninitialized Data Size	0
17	Entry Point	0x15af6
18	OS Version	5.0
19	Image Version	7.1
20	Subsystem Version	5.0
21	Subsystem	Windows GUI
Line	Name	Value


Êîìïüþòåð çàáëîêèðîâàí!
My Documents
My Computer
My Network Places
Recycle Bin
Internet Explorer
Adobe Flash Player
Update
Start
Sunshine 1.6.0
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM" value="C:\WINDOWS\system32\DRI
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\DREDGE" value="C:\WINDOWS\syste
<value key="HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Application\ESENT" v
<value key="HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Application\ESENT" v
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Aut
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM" value="C:\WINDOWS\System32\Dri
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM" value="C:\WINDOWS\system32\DRI
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM" value="C:\WINDOWS\system32\DRI
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM" value="C:\WINDOWS\system32\adv
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM" value="C:\WINDOWS\System
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\DREDGE" value="C:\WINDOWS\syste
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\DREDGE" value="C:\WINDOWS\syste
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\DREDGE" value="C:\WINDOWS\syste
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\DREDGE" value="C:\WINDOWS\syste
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\WDM\DREDGE" value="Perfo
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\PROVIDERS\Performance" value="Seed" flag="96"
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG" value="Seed" flag="96"
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Device\HarddiskVolume1\WINDOWS\system32\wuaucl
<process id="848" name="wuauclt.exe" path="C:\WINDOWS\system32\wuauclt.exe" />
<modules>
<module name="wuauclt.exe" path="C:\WINDOWS\system32\wuauclt.exe" />
<module name="xpsp2res.dll" path="C:\WINDOWS\system32\xpsp2res.dll" />
<module name="WINHTTP.dll" path="C:\WINDOWS\system32\WINHTTP.dll" />
<module name="wuaueng.dll" path="C:\WINDOWS\system32\wuaueng.dll" />
<module name="wups.dll" path="C:\WINDOWS\system32\wups.dll" />
<module name="wuaucpl.cpl" path="C:\WINDOWS\system32\wuaucpl.cpl" />
<module name="UxTheme.dll" path="C:\WINDOWS\system32\UxTheme.dll" />
<module name="NETAPI32.dll" path="C:\WINDOWS\system32\NETAPI32.dll" />

WIE?


Immunity Debugger - Legitimierende Person Ausgestaltung.pdf.3xe - [CPU - main thread, module Legitimi]
From INFILTRATE 2013 Stephen Watt's Keynote is up!
IDA - H:\2014_02_06\b0b1d392b719d6c4ce6010556e1785ac1d3f62740d3d8c03a1e1a3ede4e4a221\00000001.idb (00000001.file)
Functions window
IDA View-A
Hex View-A
Structures
Enums
Imports
Exports
Output window
Loading processor module E:\Debug\IDA6.4\procs\pc.w32 for metapc...OK
Loading type libraries...
Autoanalysis subsystem has been initialized.
Database for file '00000001.file' has been loaded.
Compiling file 'E:\Debug\IDA6.4\idc\ida.idc'...
Executing function 'main'...
Python 2.7.6 (default, Nov 10 2013, 19:24:18) [MSC v.1500 32 bit (Intel)]
IDAPython v1.6.0 final (serial 0) (c) The IDAPython Team <idapython@googlegroups.com>
Exit_RomInstall:
call Install_ROM
popad
pop es
ret

Folgen Sie uns auf Twitter @avtestorg

Finden Sie uns auf facebook.com/avtestorg

Aktuelle Testergebnisse auf www.av-test.org

Vielen Dank für Ihre Aufmerksamkeit!