

# How to convince a malware to avoid us?

Csaba Fitzl



**SECURITY**  
**20 FEST 17**

# whoami

- blue teamer
- security researcher, blogger
- certification monkey
- husband, father
- hiker



What is this talk about?



# Agenda

- part #1 - What malware authors afraid of and how they detect it?
- part #2 - Real world examples
- part #3 - My POC tools for vaccination

What malware authors are  
afraid of?

- security researchers
- sandboxes
- virtual machines
- hardened machines
- => malware hates being analyzed
- also tries to avoid certain targets

How they detect it?

# Debuggers

- IsDebuggerPresent
- PEB!IsDebugged
- PEB!NtGlobalFlags
- OutputDebugString
- timing (RDTSC)
- self debug
- INT3
- actual windows names
- etc...

OllyDbg - d9a3f5fdc35645e6f098ebd7ae0b3c9d14500730600e51f49d86539a4418001d.exe - [CPU]

C File View Debug Plugins Options Window Help

L E M T W H C / K B R + S

```

00E210AC CC INT3
00E210AD CC INT3
00E210AE CC INT3
00E210AF CC INT3
00E210B0 $S PUSH EBP
00E210B1 . 8BEC MOV EBP,ESP
00E210B3 . 33C0 SUB ESP,30
00E210B6 . A1 0430E200 MOV EAX,DWORD PTR DS:[E23004]
00E210B8 . 33C5 XOR EAX,EBP
00E210BD . 0945 FC MOV DWORD PTR SS:[EBP-4],EAX
00E210C0 FF15 0020E200 CALL DWORD PTR DS:[&KERNEL32.IsDebuggerPresent]
00E210C6 85C0 TEST EAX,EAX
00E210C8 . 74 10 JE SHORT d9a3f5fd.00E210DA
00E210CA . 33C0 XOR EAX,EAX
00E210CC . 8B4D FC MOV ECX,DWORD PTR SS:[EBP-4]
00E210CF . 33CD XOR ECX,EBP
00E210D1 . E8 61000000 CALL d9a3f5fd.00E21137
00E210D6 . 8BE5 MOV ESP,EBP
00E210D8 . 5D POP EBP
00E210D9 . C3 RETN
00E210DA > 0F2805 0021E200 MOVAPS XMM0,DQWORD PTR DS:[E22100]
00E210E1 . 8D55 D0 LEA EDX,DWORD PTR SS:[EBP-30]
00E210E4 . 51 PUSH ECX
00E210E5 . 8D4D EC LEA ECX,DWORD PTR SS:[EBP-14]
00E210E8 . C745 EC 426561 MOV DWORD PTR SS:[EBP-14],6E696542
00E210EF . C745 F0 674461 MOV DWORD PTR SS:[EBP-10],62654467
00E210F6 . C745 F4 756761 MOV DWORD PTR SS:[EBP-C],65676775
00E210FD . 66:C745 F8 64 MOV WORD PTR SS:[EBP-8],64
00E21103 . 0F1145 D8 MOVUPS DQWORD PTR SS:[EBP-80],XMM0
00E21107 . C745 E0 1C152 MOV DWORD PTR SS:[EBP-20],1521151C
00E2110E . C745 E4 0E140 MOV DWORD PTR SS:[EBP-1C],204140E
00E21115 . C745 E8 040621 MOV DWORD PTR SS:[EBP-18],2E0604
00E2111C . E8 0FFEFFFF CALL d9a3f5fd.00E21000
00E21121 . 8B4D FC MOV ECX,DWORD PTR SS:[EBP-4]
00E21124 . 33C4 04 ADD ESP,4
00E21127 . 33CD XOR ECX,EBP
00E21129 . B8 01000000 MOV EAX,1
00E2112E . E8 04000000 CALL d9a3f5fd.00E21137
00E21133 . 8BE5 MOV ESP,EBP
00E21135 . 5D POP EBP
00E21136 . C3 RETN
00E21137 $ 3B00 0430E200 CMP ECX,DWORD PTR DS:[E23004]
00E21138

```

Arg1 d9a3f5fd.00E21000

# Virtual machines

- look for artifacts in:
  - registry
  - file system
  - processes
  - MAC address...
  - VMware I/O ports
  - red pill

## Signatures

Detects virtualization software with SCSI Disk Identifier trick

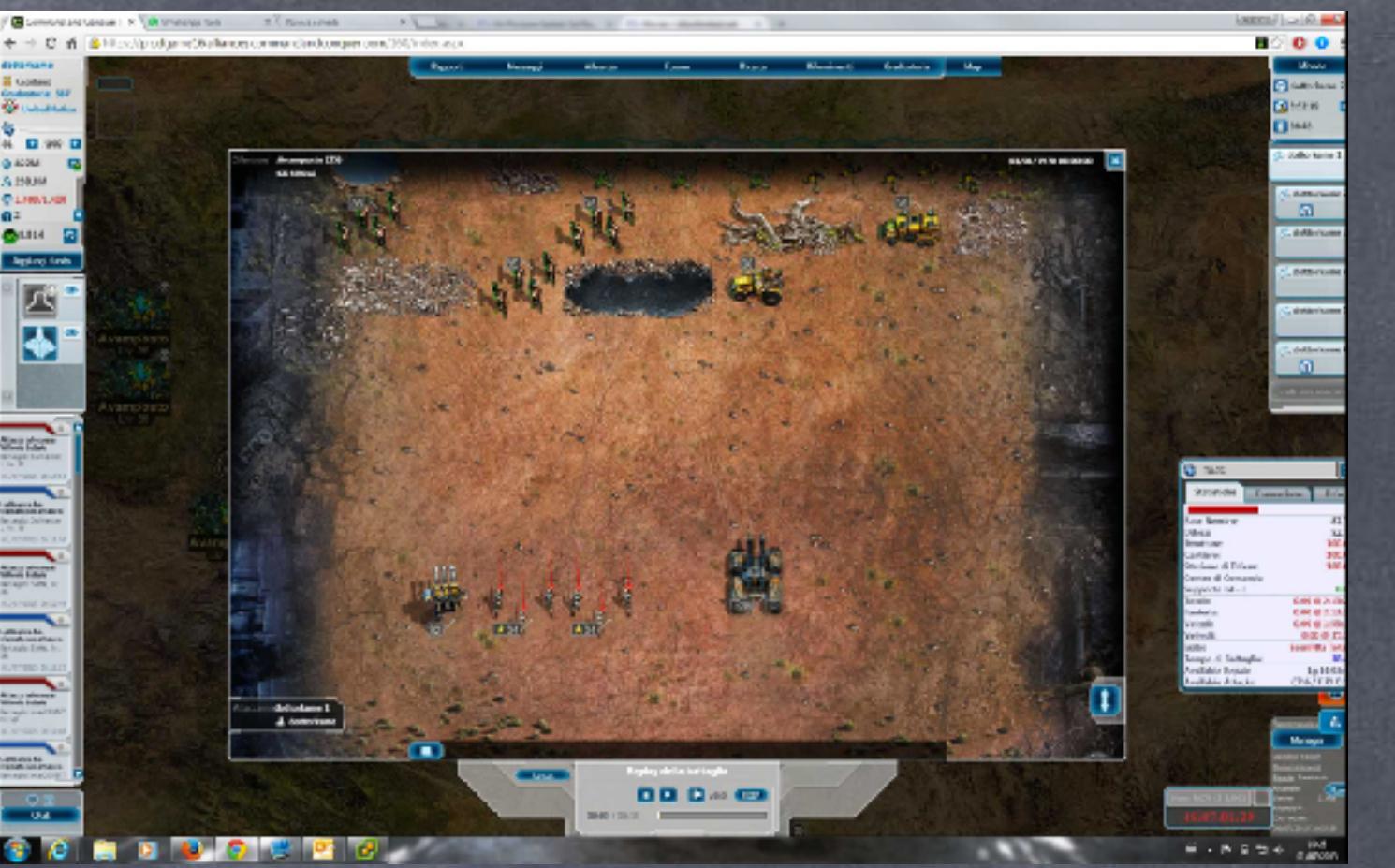
Checks the version of Bios, possibly for anti-virtualization

Detects VirtualBox through the presence of a registry key

Installs itself for autorun at Windows startup

# Sandboxes

- screen resolution (low)
- installed software (limited)
- number of cores
- memory
- desktop
- etc...
- ref: Zoltán Balázs -  
Sandbox detection for the  
masses: leak, abuse, test



# Antivirus

- registry
- file system
- antivirus product registered

## Suspicious Indicators

### Anti-Detection/Stealthyness

Possibly checks for the presence of an Antivirus engine

details "m AntiVirusProduct" (Indicator: "antivirus")

source String

relevance 3/10

research Show me all reports matching the same indicator

Real world samples



048fc07fb94a74990d2d2b8e92c099f3f986  
af185c32d74c857b07f7fcce7f8e

- Word dropper
- sandbox detection

```
Public Sub IuIxpp()
    If DKTxHE Then Error 101
    If qrNjY Then Error 102
    (...)

    Public Function DKTxHE() As Boolean
        DKTxHE = RecentFiles.Count < 3
    End Function
```

demo time

c279165952de10a5f715df706da26b2d5a57cc  
50e49dcab74fc91dba2ce1408b

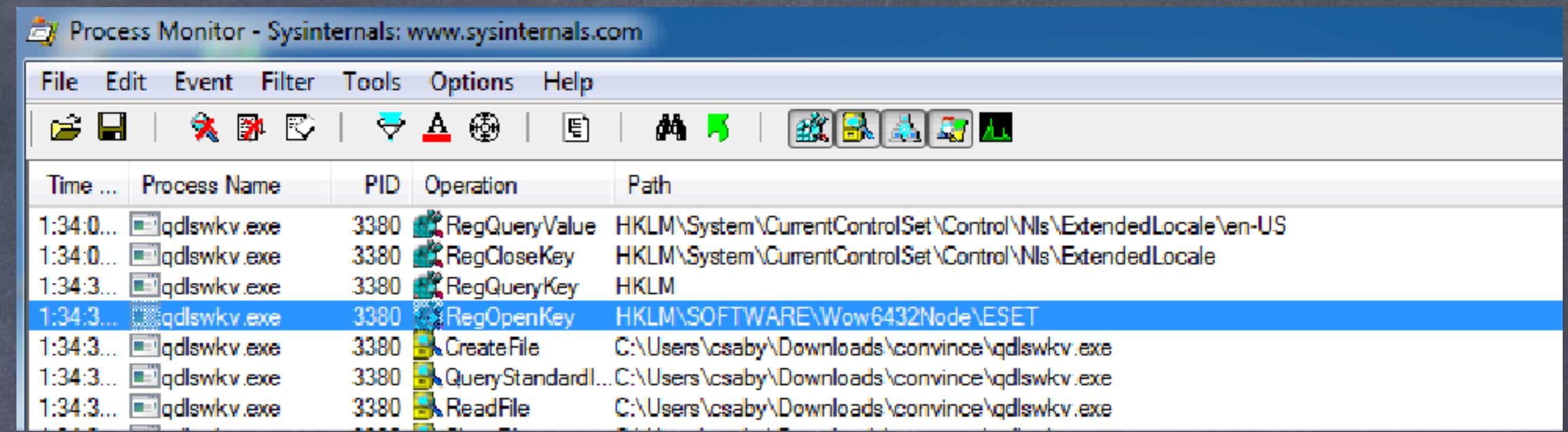
- generic trojan
- checks for plenty of analysis SW
- checks for anti malware

1728	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\Wireshark.exe	SUCCESS
1728	RegQueryKey	HKLM	SUCCESS
1728	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\ZxSniffer	NAME NOT FOUND
1728	RegQueryKey	HKLM	SUCCESS
1728	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Cygwin	NAME NOT FOUND
1728	RegQueryKey	HKCU	SUCCESS
1728	RegOpenKey	HKCU\SOFTWARE\Cygwin	NAME NOT FOUND
1728	RegQueryKey	HKLM	SUCCESS
1728	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\B Labs\Bopup Observer	NAME NOT FOUND
1728	RegQueryKey	HKCU	SUCCESS
1728	RegOpenKey	HKCU\AppEvents\Schemes\Apps\Bopup Observer	NAME NOT FOUND
1728	RegQueryKey	HKCU	SUCCESS
1728	RegOpenKey	HKCU\Software\B Labs\Bopup Observer	NAME NOT FOUND
1728	RegQueryKey	HKLM	SUCCESS
1728	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Win Sniffer_js1	NAME NOT FOUND
1728	RegQueryKey	HKCU	SUCCESS
1728	RegOpenKey	HKCU\Software\Win Sniffer	NAME NOT FOUND
1728	RegQueryKey	HKLM	SUCCESS
1728	RegOpenKey	HKCR\PEBrowseDotNETProfiler.DotNETProfiler	NAME NOT FOUND
1728	RegQueryKey	HKCU	SUCCESS
1728	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu2\Programs\Debugging Tools for...NAME NOT FOUND	SUCCESS
1728	RegQueryKey	HKLM	REPARSE
1728	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\SDbgMsg	NAME NOT FOUND
1728	RegQueryKey	HKLM\System\CurrentControlSet\Services\SDbgMsg	SUCCESS
1728	RegOpenKey	HKCU	SUCCESS
1728	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Start Menu2\Programs\API32	NAME NOT FOUND
1728	RegQueryKey	HKCU	SUCCESS
1728	RegOpenKey	HKCU\Software\Syser Soft	NAME NOT FOUND
1728	RegQueryKey	HKLM	SUCCESS
1728	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\API32	NAME NOT FOUND
1728	RegQueryKey	HKLM	SUCCESS
1728	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\API32	NAME NOT FOUND
1728	RegQueryKey	HKLM	SUCCESS
1728	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Oracle VM VirtualBox Guest Additio...NAME NOT FOUND	SUCCESS
1728	RegQueryKey	HKLM	REPARSE
1728	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\VBoxGuest	NAME NOT FOUND
1728	RegQueryKey	HKLM\System\CurrentControlSet\Services\VBoxGuest	SUCCESS
1728	RegOpenKey	HKLM	REPARSE
1728	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Sandboxie	NAME NOT FOUND
1728	RegQueryKey	HKLM	SUCCESS
1728	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\SbieDrv	REPARSE
1728	RegQueryKey	HKLM\System\CurrentControlSet\Services\SbieDrv	SUCCESS
1728	RegSetInfoKey	HKLM\System\CurrentControlSet\services\SbieDrv	SUCCESS
1728	RegCloseKey	HKLM\System\CurrentControlSet\services\SbieDrv	SUCCESS
1728	RegQueryKey	HKCU	SUCCESS
1728	RegOpenKey	HKCU\Software\Classes\Folder\shell\sandbox	REPARSE
1728	RegQueryKey	HKCU\Software\Classes\Folder\shell\sandbox	SUCCESS
1728	RegSetInfoKey	HKCU\Software\Classes\Folder\shell\sandbox	SUCCESS
1728	RegCloseKey	HKCU\Software\Classes\Folder\shell\sandbox	SUCCESS
1728	RegQueryKey	HKCU	SUCCESS
1728	RegOpenKey	HKCU\Software\Classes\*\shell\sandbox	REPARSE
1728	RegOpenKey	HKCU\Software\Classes\*\shell\sandbox	SUCCESS
1728	RegSetInfoKey	HKCU\Software\Classes\*\shell\sandbox	SUCCESS

demo time

ca7cbs6b9a254748e983929953df32f21990sf  
96486d91390e8d5d641dc9916d

- Teslacrypt
- antivirus detection



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ... Process Name PID Operation Path

Time ...	Process Name	PID	Operation	Path
1:34:0...	qdlswkv.exe	3380	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale\en-US
1:34:0...	qdlswkv.exe	3380	RegCloseKey	HKLM\System\CurrentControlSet\Control\Nls\ExtendedLocale
1:34:3...	qdlswkv.exe	3380	RegQueryKey	HKLM
1:34:3...	qdlswkv.exe	3380	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\ESET
1:34:3...	qdlswkv.exe	3380	CreateFile	C:\Users\csaby\Downloads\convince\qdlswkv.exe
1:34:3...	qdlswkv.exe	3380	QueryStandardI...	C:\Users\csaby\Downloads\convince\qdlswkv.exe
1:34:3...	qdlswkv.exe	3380	ReadFile	C:\Users\csaby\Downloads\convince\qdlswkv.exe

demo time

Today's research

# What is in the focus?

- mainly about hiding analysis tools
  - e.g.: zerofox
- ease researcher's job
- verify environment - pafish

# How about vaccination?

- let's try to emulate 'unhealthy' environment
- less researched
- malware might avoid us

# Previous research

- White Paper
  - Towards an Understanding of Anti-virtualization and Anti-debugging Behavior in Modern Malware, 2008
- Rapid7
  - Vaccinating systems against VM-aware malware, 2013
- Gal Bitensky
  - Demo Vaccination The Anti-Honeypot Approach, 2016
- various tools against specific malware

My PoC tools

*Cutting corners to meet arbitrary management deadlines*



*Essential*

# Copying and Pasting from Stack Overflow

O'REILLY®

*The Practical Developer*  
*@ThePracticalDev*

# tool #1: fakevm

- kernel driver w/ SSDT hooking
- up to Win7 x86
- can emulate VBOX / VMWARE files & registry keys
- easy to extend w/ other keys, files

demo time

## tool #2: FakeDebuggerWindows

- simple Windows app
- creates a window, and doesn't show it
- no conflict with other windows

demo time

# tool #3: mutex-grabber

- monitor [malwr.com](http://malwr.com) for mutexes
- dynamically add them to the system
- allows whitelisting
- saving / loading files

demo time

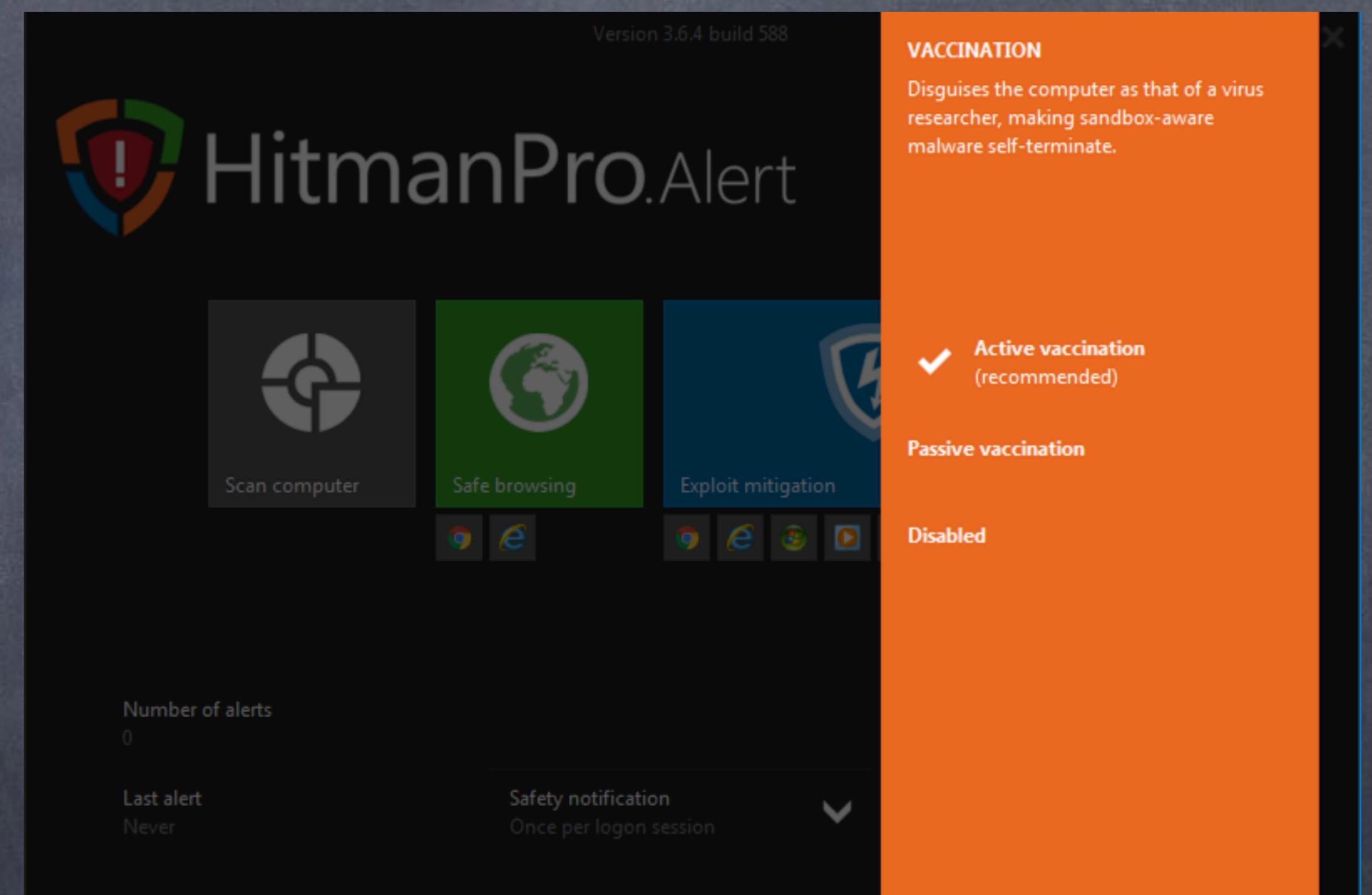
# Challenges

- software compatibility
- does normal sw care about VM / debuggers?
- system resources
- low level vaccination?
- needs to be done in clever way (e.g.: machine can't be VBOX and VMware at the same time)

Any production grade  
solution?

# Hitman Pro Alert

- uses vaccination
- other interesting protections as well
- tested w/ Pafish



demo time

# Minerva Labs

- sw dedicated for vaccination
- claims to stop many malware these days



New Carbanak Attack – PREVENTED by Minerva

November 21, 2016 |

Minerva Research Team

Protecting an enterprise from advanced cybercriminals is a major challenge. Carbanak-style attacks emphasize the difference between existing products which detect a compromise in a machine, unfortunately after it is already too late and Minerva's innovative Environment Simulation Technology (EST), which prevents the infection before any damage is done.

[Read More >>](#)

# Conclusion

- interesting area
- it is effective against malware
- should be more commonly researched
- could have two long term effects
  - malware stop caring about VM, etc.. -> this method won't be effective, but analysis might be easier
  - everything stays -> we can protect against malware

- twitter: @theevilbit
- tools:
- <https://github.com/theevilbit/vaccination>