IT Security

Security Day 2014

VON VIREN, WÜRMERN UND TROJANISCHEN PFERDEN...

Robert Luh & Paul Tavolato

DAS PROBLEM

Würmer

Trojanische Pferde

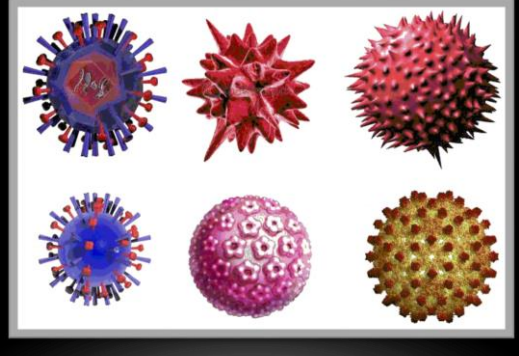
Viren

DAS ZIEL

Erkennen und bekämpfen!

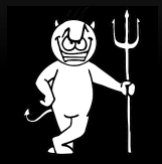
DIE GROSSE FRAGE

Wie sehen Viren aus?



MALWARE

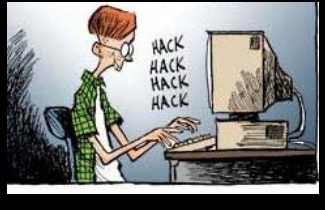
Malicious Soft**ware**



... einfach Software, die etwas tut, was der Besitzer des Computers nicht will!

MALWARE

Früher:



So genannte Script Kiddies versuchen in fremde Rechner einzudringen, um (zweifelhaften) Ruhm zu erlangen.

Heute:

Ein kriminelles Geschäft mit Mafia-artiger Struktur

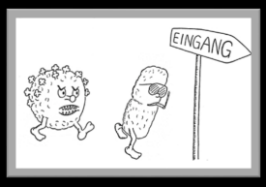
CYBER CRIME

- Daten Diebstahl
- Identitätsdiebstahl
- Missbrauch fremder Computer
- Erpressung
- Sabotage
- Hacktivsm
- Terrorismus
- Cyber War

Malware ist das Werkzeug dafür!

GRUNDPROBLEME

Herkommen ➡ *Eindringen* ➡ *Böses tun*



ZUGANGSKONTROLLEN ÜBERWINDEN

Video von Alexander Talos-Zens

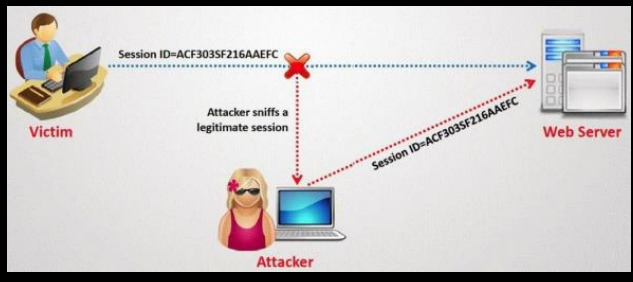
BRUTE FORCE ATTACKS

Alle möglichen Passwörter ausprobieren
Beliebte Passwörter ausprobieren

1. 123456
2. Password
3. 12345678
4. 1234
5. Pussy
6. 12345
7. Dragon
8. Qwerty
9. 696969
10. Mustang

SESSION HIJACKING

Mit einem legitimen Benutzer „mitfahren“



SOCIAL ENGINEERING

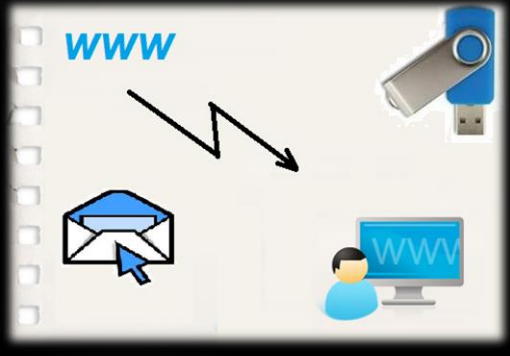
Ausnutzen menschlicher Schwächen

HARDWARE ATTACKEN

Manipulation von Hardware-Identifikation (Finger, Gesicht, Venen, ... oder Smart Cards)

HERKOMMEN

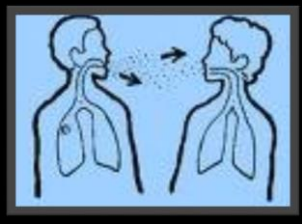
Die häufigsten Wege



INFEKTIONSKRANKHEIT

- ... das ist fast so wie bei einer Grippe

Es gibt die Viren überall;
und es gibt Abwehrkräfte;
aber die können auch
geschwächt sein.....



INFEKTIONSKRANKHEIT

EINDRINGEN:

VULNERABILITY

Schwachstelle

VULNERABILITIES - EXPLOITS

Vulnerability

↓

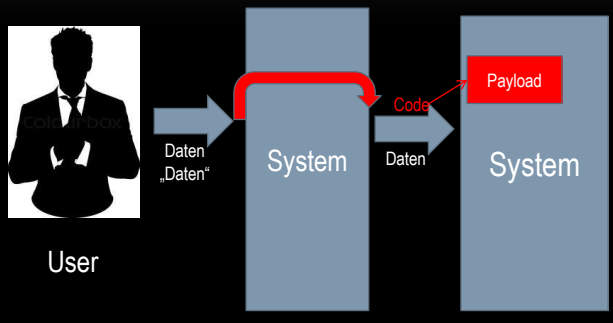
Exploit

.... mit Malware

EXPLOIT

Wie war das mit Siegfried und Hagen und der verwundbaren Stelle .....

EXPLOIT



EXPLOIT

Beispiel: SQL Injection

Wenn man sich wo einloggt wird DB gefragt…
SELECT * **FROM** users **WHERE** name = 'myUser';
Man muss aber nicht wirklich den Usernamen eingeben…
myUser → ' **OR** '1' = '1;
(und beim Passwort geht‘s genauso)

EXPLOIT

Beispiel: SQL Injection

Kann man das verhindern?

Natürlich! Durch saubere Programmierung.

(Dass eine solche SQL Injection überhaupt möglich ist, ist eigentlich ein Programmierfehler!)

MALWARE - BEISPIEL

Malware ist .....

Code

- *Meist verschlüsselt*
- *Oft gepackt*
- *Bisweilen polymorph*
- *Manchmal sogar metamorph*
- *Immer möglichst unkenntlich*

MALWARE - BEISPIEL

Der Zeus-Virus

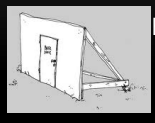
- *Ist derzeit noch immer aktiv*
- *Gibt‘s in vielen Varianten (zB auch in pdf-Doks)*
- *Gilt als eines der „erfolgeichsten“ Schadprogramme*

PAYLOAD

Zum Beispiel:
Daten stehlen
Daten zerstören
System zerstören
Hardware zerstören
Denial of Service Attack
Den Rechner kapern (Botnet)
.....

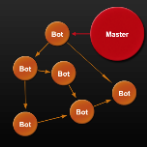
PAYLOAD

Backdoor



Trojaner

Botnet



Keylogger

System verlangsamen

System zerstören

(D)DOS

2007: Estland
2010: KK-Institute
2012: Frankfurt

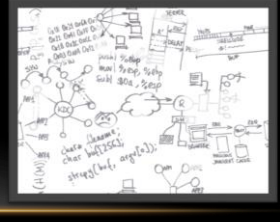
Daten ausspionieren

Hardware beschädigen

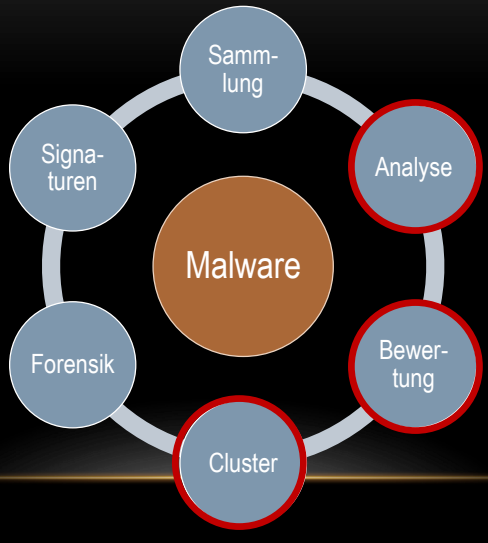
WAS MACHEN WIR AN DER FH?

Wir unterrichten Malware

Wir erforschen Malware



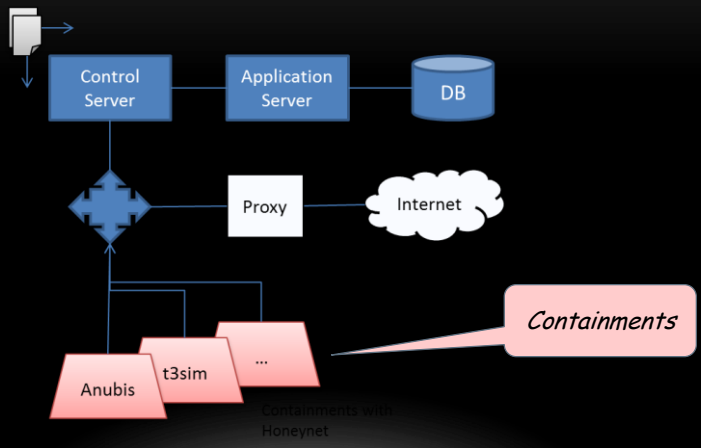
MALWARE-FORSCHUNG



DAS MALWARE LABOR

DAS MALWARE LABOR

DAS MALWARE LABOR



WAS BEOBACHTEN WIR?

Das Aussehen

Das Verhalten

VERHALTENSANALYSE

Verhaltensbasierte Malwareanalyse

- Wir bringen einem Programm bei, was gut und böse ist
- Wir lassen das Programm das selber herausfinden

BEISPIEL

Analysen können so aussehen…

```
...
00001035 >> 001b:01019e33 eb00                jmp         01019e35

00001036 >> 001b:01019e35 89c0                mov         EAX, EAX
00001037 >> 001b:01019e37 f5                  cmc
00001038 >> 001b:01019e38 87db                xchg        EBX, EBX
00001039 >> 001b:01019e3a 29db                sub         EBX, EBX
00001040 >> 001b:01019e3c 29c9                sub         ECX, ECX
00001041 >> 001b:01019e3e 89c9                mov         ECX, ECX
00001042 >> 001b:01019e40 89c0                mov         EAX, EAX
00001043 >> 001b:01019e42 f5                  cmc
00001044 >> 001b:01019e43 89c9                mov         ECX, ECX
00001045 >> 001b:01019e45 b1fa                mov         CL, fa
00001046 >> 001b:01019e47 8d5b01              lea         EBX, DS:[EBX + 01]
00001047 >> 001b:01019e4a e2fb                loop        01019e47

00001048 >> 001b:01019e47 8d5b01              lea         EBX, DS:[EBX + 01]
00001049 >> 001b:01019e4a e2fb                loop        01019e47
...
```

BEISPIEL

…oder so (3000 Zeilen+)

```
<reg_key_monitored count="1" key="HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5" notify_filter="Key Change
<reg_key_monitored count="1" key="HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9" notify_filter="Key Change"
</registry_activities>
<file_activities>
<file_created name="C:\Documents and Settings\user\Local Settings\Temporary Internet Files\Content.IE5\012N45I3\ccxebztz.exe"/>
<file_modified name="\Device\Afd\AsyncConnectHlp"/>
<file_modified name="\Device\Ip"/>
<file_modified name="\Device\RasAcd"/>
<file_read name="C:\Documents and Settings\user\Local Settings\Temporary Internet Files\Content.IE5\012N45I3\CAVR4E11.HTM"/>
<file_read name="C:\WINDOWS\system32\rsaenh.dll"/>
<file_read name="C:\WINDOWS\system32\urdvxc.exe"/>
<file_read name="pipe\net\NtControlPipe9"/>
<section_object_created file_name="C:\WINDOWS\system32\rsaenh.dll" section_name=""/>
<fs_control_communication control_code="0x00110018" count="1" file="\DosDevices\pipe\"/>
<device_control_communication control_code="AFD_SET_INFO (0x0001203B)" count="519" file="\Device\Afd\Endpoint"/>
<device_control_communication control_code="AFD_SET_CONTEXT (0x00012047)" count="1501" file="\Device\Afd\Endpoint"/>
<device_control_communication control_code="AFD_BIND (0x00012003)" count="519" file="\Device\Afd\Endpoint"/>
<device_control_communication control_code="AFD_GET_TDI_HANDLES (0x00012037)" count="1032" file="\Device\Afd\Endpoint"/>
<device_control_communication control_code="AFD_CONNECT (0x00012007)" count="519" file="\Device\Afd\AsyncConnectHlp"/>
<device_control_communication control_code="AFD_SELECT (0x00012024)" count="1275" file="\Device\Afd\Endpoint"/>
<device_control_communication control_code="AFD_DISCONNECT (0x0001202B)" count="503" file="\Device\Afd\Endpoint"/>
<device_control_communication control_code="AFD_SEND (0x0001201F)" count="513" file="\Device\Afd\Endpoint"/>
<device_control_communication control_code="AFD_RECV (0x00012017)" count="416" file="\Device\Afd\Endpoint"/>
<device_control_communication control_code="0x00F14014" count="6" file="\Device\RasAcd"/>
```