Fraunhofer FKIE

Übungen zu ClamAV
- Musterlösung -

Aufgabe 1

```
0f8816902a5bd1c10a87e06100e68d68:128804:Hello_World.exe
d0a06af0ee01544da7a44450803a1ff9:128804:HeLLo_WoRld_1.exe

/home/signature/suspiciousFiles/PA: Hello_World.exe.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/ABFZ: Hello_World.exe.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/OYL: HeLLo_WoRld_1.exe.UNOFFICIAL FOUND
```

Aufgabe 2

```
aufgabe2:0:*:4920616d204d616c77617265

/home/signature/suspiciousFiles/HRZ: aufgabe2.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/YH: aufgabe2.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/ZURSCQIYR: aufgabe2.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/KULMJBG: aufgabe2.UNOFFICIAL FOUND
```

Aufgabe 3

```
aufgabe3:0:*:(21|49)20(34|61)6d204d(34|61)(31|6c)77(34|61)72(33|65)

/home/signature/suspiciousFiles/HRZ: aufgabe3.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/YH: aufgabe3.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/ZURSCQIYR: aufgabe3.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/KULMJBG: aufgabe3.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/IAY: aufgabe3.UNOFFICIAL FOUND
```

Aufgabe 4

```
aufgabe4a:0:*:6920(61|41)(6d|4d)20(6d|4d)(61|41)(6c|4c)(77|57)(61|41)(72|52)(65|45)
aufgabe4b:0:*:4920(61|41)(6d|4d)20(6d|4d)(61|41)(6c|4c)(77|57)(61|41)(72|52)(65|45)

/home/signature/suspiciousFiles/HRZ: aufgabe4b.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/YH: aufgabe4b.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/IYPZ: aufgabe4a.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/ZURSCQIYR: aufgabe4b.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/KULMJBG: aufgabe4b.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/GLEORJDOLI: aufgabe4a.UNOFFICIAL FOUND
```

Aufgabe 5

```
aufgabe5;Target:0;0&1&2;*:4920;*:616d;*:4d616c77617265

/home/signature/suspiciousFiles/YJLANYNF: aufgabe5.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/HRZ: aufgabe5.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/YH: aufgabe5.UNOFFICIAL FOUND
```

/home/signature/suspiciousFiles/MLIGOM: aufgabe5.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/ZURSCQIYR: aufgabe5.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/KULMJBG: aufgabe5.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/GOVJUL: aufgabe5.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/GLEORJDOLI: aufgabe5.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/JVTCCWOQ: aufgabe5.UNOFFICIAL FOUND

Aufgabe 6

aufgabe6:0:*:4920*616d*4d616c77617265

/home/signature/suspiciousFiles/YJLANYNF: aufgabe6.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/HRZ: aufgabe6.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/YH: aufgabe6.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/ZURSCQIYR: aufgabe6.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/KULMJBG: aufgabe6.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/GOVJUL: aufgabe6.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/GLEORJDOLI: aufgabe6.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/JVTCCWOQ: aufgabe6.UNOFFICIAL FOUND

Aufgabe 10

aufgabe10;Target:1;0&(1|2);EP+5,12:8bff55*6a01{5}596a00;*:48656c6c6f20576f726c6421;\\
*:4920616d204d616c7761726521

/home/signature/suspiciousFiles/KULMJBG: aufgabe10.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/YHKT: aufgabe10.UNOFFICIAL FOUND

Aufgabe 11

43008:a306be00d53d2bb7ad289064d07b495e:aufgabe11_trojan.swissor

/home/signature/suspiciousFiles/UVOXF: aufgabe11_trojan.swissor.UNOFFICIAL FOUND

Aufgabe 13

/home/signature/suspiciousFiles/ZJFTOLCWPD: aufgabe13_trojan-bankerAB.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/RX: aufgabe13_ZeroAccess.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/PXRYY: aufgabe13_BKA-Trojaner.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/UMYSOGQFK: aufgabe13_ZeroAccess.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/AZCQYEUQ: aufgabe13_sality.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/APDRRK: aufgabe13_enerlam.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/IOXMVC: aufgabe13_sality.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/GXHNVGKZNV: aufgabe13_Rbot.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/XZDWF: aufgabe13_heathen.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/DDB: aufgabe13_parite.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/UVOXF: aufgabe13_siwzzor.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/PW: aufgabe13_spybot.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/PJJX: Trojan-Banker-other1.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/OUAD: aufgabe13_ZeroAccess.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/HOADCZ: aufgabe13_getpass.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/LL: aufgabe13_trojan-bankerAB.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/WLAXOSJYR: aufgabe13_ZeroAccess.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/OBTWVMMHJ: Trojan-Banker-other2.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/RI: aufgabe13_parite.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/FTR: aufgabe13_sdbot.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/NF: aufgabe13_alman.UNOFFICIAL FOUND

```
/home/signature/suspiciousFiles/KPW: aufgabe13_sality.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/JDWUZCQFQ: aufgabe13_orez.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/OYBPRYEX: aufgabe13_Rbot.UNOFFICIAL FOUND
/home/signature/suspiciousFiles/HJJXTS: aufgabe13_conficker.UNOFFICIAL FOUND
```