Malware

Sven Strickroth

TU Clausthal

5. April 2007

Was ist Malware?

Woher kommt das Wort Malware?

engl. **mal**icious „boshaft“ und Soft**ware**

Was ist Malware?

Woher kommt das Wort Malware?

engl. **mal**icious „boshaft“ und Soft**ware**

Allgemein

Programme, die unerwünschte (schädliche) Funktionen ausführen
ABER: keine fehlerhafte Software

Wie viel Malware existiert?

Produkt	**Bekannte Malware**	**Bekannte Malware**
AntiVir	577 987	706 481
BitDefender	328 327	405 790
ClamAV	80 524	100 740
DrWeb	154 595	168 299
F-Prot	347 443	419 306
Kaspersky	235 272	267 250
Norton AV	73 010	73 221
Stand:	10. Dezember 2006	19. März 2007

„Tausende“ von Varianten $\Rightarrow$ Anzahl besagt nichts über die Qualität

Arten von Malware

- Virus
- Wurm
- Trojaner
- Exploits
- Makro
- Adware bzw. Spyware
- Dialer
- Phishings

Arten von Malware

- Virus
- Wurm
- Trojaner
- Exploits
- Makro
- Adware bzw. Spyware
- Dialer
- Phishings

Virus

Infiziert andere Programme
d.h. verändert Entrypoint,
kopiert sich an Anfang oder Ende;
eher passiv.
älteste Art der Malware

Arten von Malware

- Virus
- Wurm
- Trojaner
- Exploits
- Makro
- Adware bzw. Spyware
- Dialer
- Phishings

Wurm

Verbreitet sich selbstständig weiter über Netzwerke, Internet (Mail, IM, P2P, . . .)

Arten von Malware

- Virus
- Wurm
- Trojaner
- Exploits
- Makro
- Adware bzw. Spyware
- Dialer
- Phishings

Trojaner

Bots, Downloader, Backdoors, Keylogger, Rootkits, ...

Arten von Malware

- Virus
- Wurm
- Trojaner
- Exploits
- Makro
- Adware bzw. Spyware
- Dialer
- Phishings

Exploits

dringen über Sicherheitslücken (z.B. Buffer Overflows) in Systeme ein

Arten von Malware

- Virus
- Wurm
- Trojaner
- Exploits
- Makro
- Adware bzw. Spyware
- Dialer
- Phishings

Makro

sind in z.B. Office-Dokumenten enthalten
verbreiten sich i.d.R. auch selbstständig weiter
seltener, u.A: wegen Schutzmaßnahmen
am langlebigsten

Arten von Malware

- Virus
- Wurm
- Trojaner
- Exploits
- Makro
- Adware bzw. Spyware
- Dialer
- Phishings

Adware bzw. Spyware

Blenden Werbung ein
Verändern Startseite, Lesezeichen
Sammeln personenbezogene Daten

Arten von Malware

- Virus
- Wurm
- Trojaner
- Exploits
- Makro
- Adware bzw. Spyware
- Dialer
- Phishings

Dialer

Einwahlprogramme zu Mehrwertdiensten

Arten von Malware

- Virus
- Wurm
- Trojaner
- Exploits
- Makro
- Adware bzw. Spyware
- Dialer
- Phishings

Phishings

Password-Fishing $\Rightarrow$ Phishing

Basiert auf „Social Enginering“

Wer schreibt Schadprogramme und warum?

Autoren

- Skript-Kiddies
- Professionelle Malware-Autoren
- Virenforscher

Wer schreibt Schadprogramme und warum?

Autoren

- Skript-Kiddies
- Professionelle Malware-Autoren
- Virenforscher

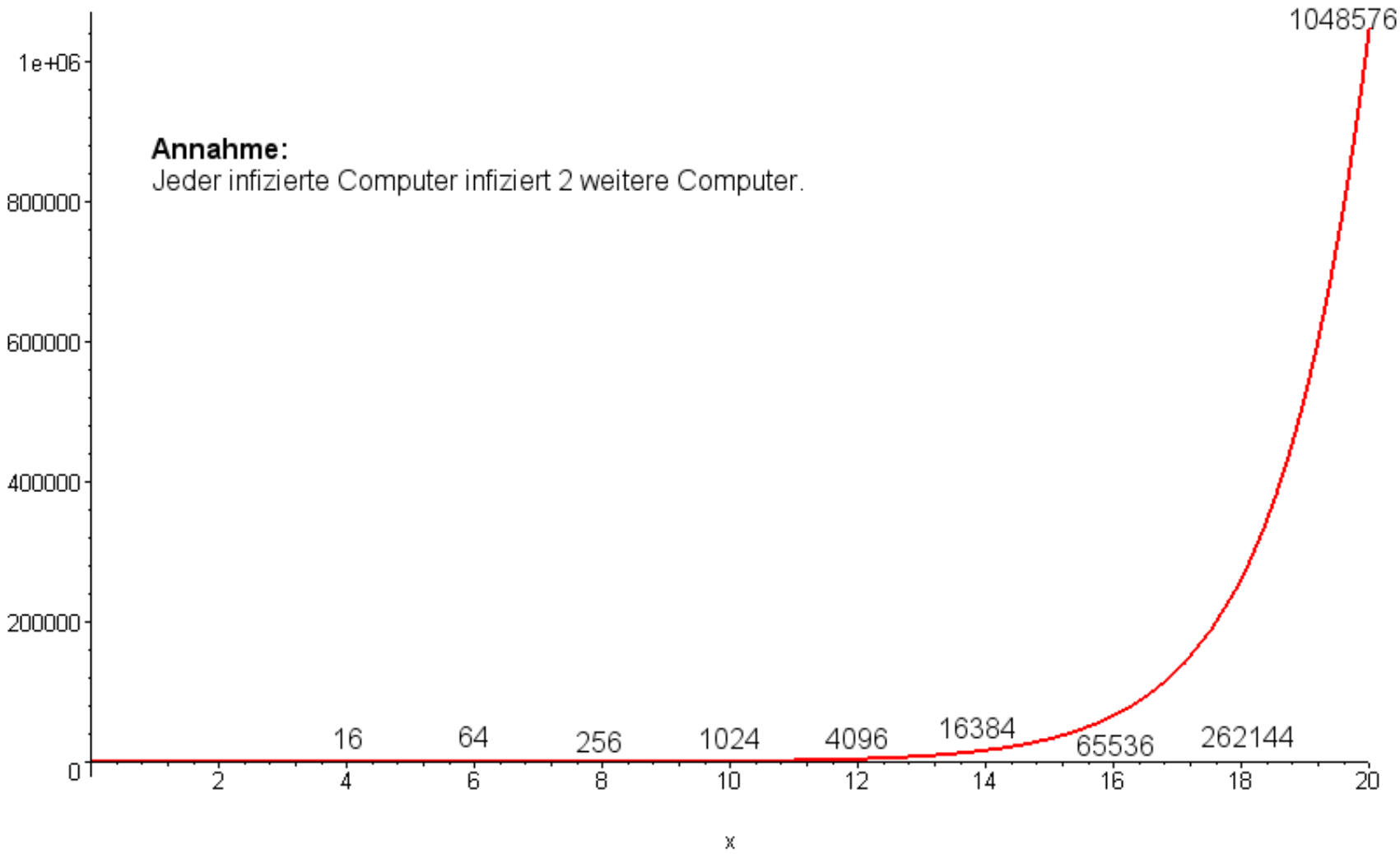
Gründe

- Geltungsbedürfnis (aka. „Bekannt werden“)
- Erschleichung von kostenpflichtigen Leistungen
- direkter finanzieller Gewinn
- Organisierte Cyber-Kriminalität

Schutz vor Malware

1. Verantwortungsvoller Umgang mit dem Computer
2. aktuelle Antivirussoftware
3. Firewall
4. nur vertrauenswürdige Software einsetzen
5. Arbeiten mit eingeschränkten Rechten

Verbreitung erfolgt exponentiell



Von der Entstehung zur Erkennung

1. Malware wird in Umlauf gebracht
2. Kenntnisnahme vom AV-Vendor
   - Honeypots
   - Users
3. Analyse der eingesandten Daten
4. Erarbeiten einer Erkennungsmethode
5. Prüfen einer Erkennungsmethode (False-Positive-Check)
6. Veröffentlichen einer Erkennungsmethode

Analyse

- HexEditor
- Disassemblieren
- VirtualMachine oder dedizierte Hardware
  - Debuggen
  - Veränderungen am System und Netzwerkverkehr aufzeichnen

HexDump
Backdoor mit AV-Killer

```
00042208|4333 322E 4558 452A 4156 504D 2E45 5845|C32.EXE*AVPM.EXE
00042224|2A41 5650 444F 5333 322E 4558 452A 4156|*AVPDOS32.EXE*AV
00042240|5043 432E 4558 452A 4156 5033 322E 4558|PCC.EXE*AVP32.EX
00042256|452A 4156 502E 4558 452A 2A41 564E 542E|E*AVP.EXE**AVNT.
00042272|4558 452A 4156 4B53 4552 562E 4558 452A|EXE*AVKSERV.EXE*
00042288|4156 4743 5452 4C2E 4558 452A 4156 4533|AVGCTRL.EXE*AVE3
00042304|322E 4558 452A 4156 434F 4E53 4F4C 2E45|2.EXE*AVCONSOL.E
00042320|5845 2A41 5554 4F44 4F57 4E2E 4558 452A|XE*AUTODOWN.EXE*
00042336|4150 5658 4457 494E 2E45 5845 2A41 4E54|APVXDWIN.EXE*ANT
00042352|492D 5452 4F4A 414E 2E45 5845 2A41 434B|I-TROJAN.EXE*ACK
00042368|5749 4E33 322E 4558 452A 5F41 5650 4D2E|WIN32.EXE*_AVPM.
00042384|4558 452A 5F41 5650 4343 2E45 5845 2A52|EXE*_AVPCC.EXE*R
00042400|4547 4544 4954 2E45 5845 2A00 5356 57BF|EGEDIT.EXE*.SVW.
00042416|0428 4100 5768 3F00 0F00 6A01 6830 B240|.(A.Wh?...j.h0.@
00042432|0068 0200 0080 E81D A3FF FFBB 2200 0000|.h.........."....
00042448|BE00 1341 008B 06E8 1491 FFFF 508B 0750|...A........P..P
00042464|E8FB A2FF FF83 C604 4B75 EA57 683F 000F|........Ku.Wh?..
00042480|006A 0168 60B2 4000 6802 0000 80E8 E6A2|.j.h`.@.h.......
00042496|FFFF BB22 0000 00BE 0013 4100 8B06 E8DD|..."......A.....
00042512|90FF FF50 8B07 50E8 C4A2 FFFF 83C6 044B|...P..P........K
00042528|75EA 8B07 50E8 A6A2 FFFF 5F5E 5BC3 0000|u...P....._^[...
00042544|536F 6674 7761 7265 5C4D 6963 726F 736F|Software\Microso
00042560|6674 5C57 696E 646F 7773 5C43 7572 7265|ft\Windows\Curre
00042576|6E74 5665 7273 696F 6E5C 5275 6E00 0000|ntVersion\Run...
00042592|536F 6674 7761 7265 5C4D 6963 726F 736F|Software\Microso
00042608|6674 5C57 696E 646F 7773 5C43 7572 7265|ft\Windows\Curre
00042624|6E74 5665 7273 696F 6E5C 5275 6E53 6572|ntVersion\RunSer
00042640|7669 6365 7300 0000 558B EC33 C055 68D4|vices...U..3.Uh.
```

HexDump
Backdoor mit AV-Killer

```
00042208 4333 322E 4558 452A 4156 504D 2E45 5845 C32.EXE*AVPM.EXE
00042224 2A41 5650 444F 5333 322E 4558 452A 4156 *AVPDOS32.EXE*AV
00042240 5043 432E 4558 452A 4156 5033 322E 4558 PCC.EXE*AVP32.EX
00042256 452A 4156 502E 4558 452A 2A41 564E 542E E*AVP.EXE**AVNT.
00042272 4558 452A 4156 4B53 4552 562E 4558 452A EXE*AVKSERV.EXE*
00042288 4156 4743 5452 4C2E 4558 452A 4156 4533 AVGCTRL.EXE*AVE3
00042304 322E 4558 452A 4156 434F 4E53 4F4C 2E45 2.EXE*AVCONSOL.E
00042320 5845 2A41 5554 4F44 4F57 4E2E 4558 452A XE*AUTODOWN.EXE*
00042336 4150 5658 4457 494E 2E45 5845 2A41 4E54 APVXDWIN.EXE*ANT
00042352 492D 5452 4F4A 414E 2E45 5845 2A41 434B I-TROJAN.EXE*ACK
00042368 5749 4E33 322E 4558 452A 5F41 5650 4D2E WIN32.EXE*_AVPM.
00042384 4558 452A 5F41 5650 4343 2E45 5845 2A52 EXE*_AVPCC.EXE*R
00042400 4547 4544 4954 2E45 5845 2A00 5356 57BF EGEDIT.EXE*.SVW.
00042416 0428 4100 5768 3F00 0F00 6A01 6830 B240 .(A.Wh?...j.h0.@
00042432 0068 0200 0080 E81D A3FF FFBB 2200 0000 .h.........."....
00042448 BE00 1341 008B 06E8 1491 FFFF 508B 0750 ...A........P..P
00042464 E8FB A2FF FF83 C604 4B75 EA57 683F 000F ........Ku.Wh?..
00042480 006A 0168 60B2 4000 6802 0000 80E8 E6A2 .j.h`.@.h.......
00042496 FFFF BB22 0000 00BE 0013 4100 8B06 E8DD ...".......A.....
00042512 90FF FF50 8B07 50E8 C4A2 FFFF 83C6 044B ...P..P........K
00042528 75EA 8B07 50E8 A6A2 FFFF 5F5E 5BC3 0000 u...P....._^[...
00042544 536F 6674 7761 7265 5C4D 6963 726F 736F Software\Microso
00042560 6674 5C57 696E 646F 7773 5C43 7572 7265 ft\Windows\Curre
00042576 6E74 5665 7273 696F 6E5C 5275 6E00 0000 ntVersion\Run...
00042592 536F 6674 7761 7265 5C4D 6963 726F 736F Software\Microso
00042608 6674 5C57 696E 646F 7773 5C43 7572 7265 ft\Windows\Curre
00042624 6E74 5665 7273 696F 6E5C 5275 6E53 6572 ntVersion\RunSer
00042640 7669 6365 7300 0000 558B EC33 C055 68D4 vices...U..3.Uh.
```

Signatur mittels der markierten Bytes.

Disassembler-Ausgabe

Virus W32.Ramm.F

```
CODE:0040388C    mov     ss:dword_0_403FC3[ebp], 4203h
CODE:00403896    lea     eax, sub_0_403A1C[ebp]
CODE:0040389C    mov     ss:dword_0_403FC7[ebp], eax
CODE:004038A2    mov     ss:dword_0_403FCB[ebp], 0
CODE:004038AC    mov     ss:dword_0_403FCF[ebp], 0
CODE:004038B6    mov     eax, ss:dword_0_403FF3[ebp]
CODE:004038BC    mov     ss:dword_0_403FD3[ebp], eax
CODE:004038C2    push    7F00h
CODE:004038C7    push    ss:dword_0_403FF3[ebp]
CODE:004038CD    call    ss:dword_0_404A89[ebp]
CODE:004038D3    mov     ss:dword_0_403FFF[ebp], eax
CODE:004038D9    mov     ss:dword_0_403FD7[ebp], eax
CODE:004038DF    mov     ss:dword_0_403FEB[ebp], eax
CODE:004038E5    push    7F00h
CODE:004038EA    push    0
CODE:004038EC    call    ss:dword_0_404A8D[ebp]
CODE:004038F2    mov     ss:dword_0_403FDB[ebp], eax
CODE:004038F8    mov     ss:dword_0_403FDF[ebp], 6
CODE:00403902    mov     ss:dword_0_403FE3[ebp], 0
CODE:0040390C    lea     eax, aRammstein[ebp] ; "RAMMSTEIN"
CODE:00403912    mov     ss:dword_0_403FE7[ebp], eax
CODE:00403918    lea     eax, dword_0_403FBF[ebp]
CODE:0040391E    push    eax
CODE:0040391F    call    ss:dword_0_404AC9[ebp]
CODE:00403925    mov     eax, ss:dword_0_40407E[ebp]
CODE:0040392B    sub     eax, ss:dword_0_404086[ebp]
CODE:00403931    call    sub_0_40429A
CODE:00403936    mov     ss:dword_0_40408E[ebp], eax
CODE:0040393C    mov     eax, ss:dword_0_404082[ebp]
CODE:00403942    sub     eax, ss:dword_0_40408A[ebp]
CODE:00403948    call    sub_0_40429A
CODE:0040394D    mov     ss:dword_0_404092[ebp], eax
CODE:00403953    lea     eax, aRammstein[ebp] ; "RAMMSTEIN"
CODE:00403959    lea     ebx, aWin32_rammstei[ebp] ; "Win32.Rammstein"
CODE:0040395F    push    0
CODE:00403961    push    ss:dword_0_403FF3[ebp]
```

Erkennung von Malware und Gegenbewegung

- Statische Malware
  - (spezifische) Signaturen

Erkennung von Malware und Gegenbewegung

- Statische Malware
  - (spezifische) Signaturen
- Leicht veränderte statische Malware, neue Varianten
  - generische Signaturen
  - Heuristik

Erkennung von Malware und Gegenbewegung

- Statische Malware
  - (spezifische) Signaturen
- Leicht veränderte statische Malware, neue Varianten
  - generische Signaturen
  - Heuristik
- Encrypting (z.B. UPX, Aspack, Petite, veränderte, . . .)
  - Signaturen und Heuristik sehr stark eingeschränkt
  - Entwicklung von Unpackern

Erkennung von Malware und Gegenbewegung

- Statische Malware
  - (spezifische) Signaturen
- Leicht veränderte statische Malware, neue Varianten
  - generische Signaturen
  - Heuristik
- Encrypting (z.B. UPX, Aspack, Petite, veränderte, . . .)
  - Signaturen und Heuristik sehr stark eingeschränkt
  - Entwicklung von Unpackern
- Polymorph bzw. Metamorph
  - Heuristik und Signaturen meist machtlos
  - Algorithmische Erkennung

Was heisst Polymorph?

Polymorpher Wurm: JS.Feebs.AC

```
<html>
<body>
<script language=JavaScript>
zncf=''EdLL4zmvL1(md(;/ylzd*(Q4z,j4(*8v2(Q4ja4jlll<Qzjv-m(28L1,814z9(qd,j(HLm4j(
:
4zmvdL(8L+(mjq(818vLl<Qz%5C%22;if(d%3D=%22%5E%22)d=%22%5C%22%22;g%2B%3Dd%7D%7D;
%64oc%75ment%2Ewr%69%74%65%28%67)%%7D``;
qld=zncf.substring(2280,2887);qld=unescape(qld);
eval(qld);f(zncf.substring(0,2280));</script></body></html>
```

Hier: Zufällige Variablennamen, Kodierung des Unpackers variiert...

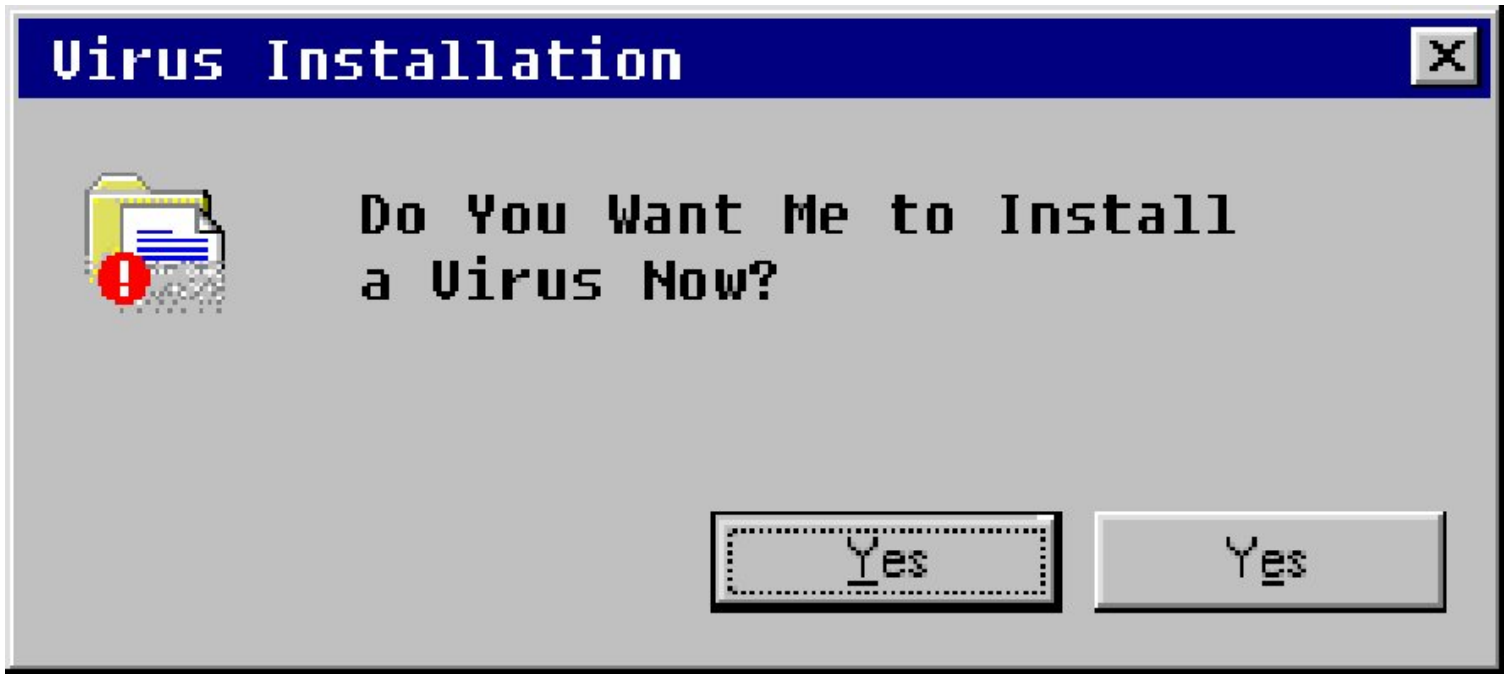
Erkennungsmethoden im Vergleich

Bessere Erkennung

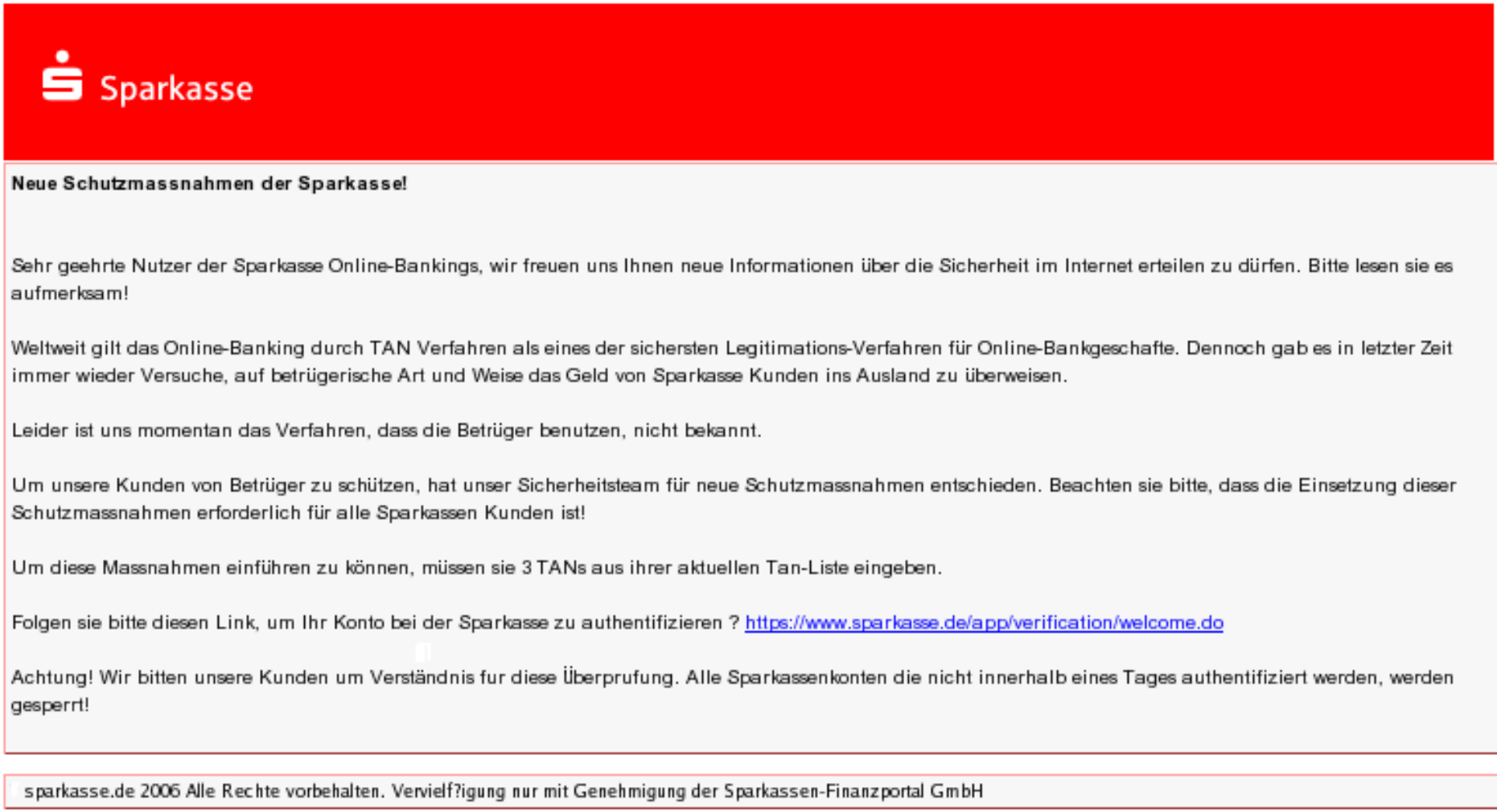
- Signaturen
- generische Signaturen
- Heuristik
- Behavior Blocking

mehr False-Positives

Tarnung


Virus Installation
Do You Want Me to Install
a Virus Now?
Yes
Yes

Tarnung
Phishing-Mail



Sparkasse

Neue Schutzmassnahmen der Sparkasse!

Sehr geehrte Nutzer der Sparkasse Online-Bankings, wir freuen uns Ihnen neue Informationen über die Sicherheit im Internet erteilen zu dürfen. Bitte lesen sie es aufmerksam!

Weltweit gilt das Online-Banking durch TAN Verfahren als eines der sichersten Legitimations-Verfahren für Online-Bankgeschafte. Dennoch gab es in letzter Zeit immer wieder Versuche, auf betrügerische Art und Weise das Geld von Sparkasse Kunden ins Ausland zu überweisen.

Leider ist uns momentan das Verfahren, dass die Betrüger benutzen, nicht bekannt.

Um unsere Kunden von Betrüger zu schützen, hat unser Sicherheitsteam für neue Schutzmassnahmen entschieden. Beachten sie bitte, dass die Einsetzung dieser Schutzmassnahmen erforderlich für alle Sparkassen Kunden ist!

Um diese Massnahmen einführen zu können, müssen sie 3 TANs aus ihrer aktuellen Tan-Liste eingeben.

Folgen sie bitte diesen Link, um Ihr Konto bei der Sparkasse zu authentifizieren ? https://www.sparkasse.de/app/verification/welcome.do

Achtung! Wir bitten unsere Kunden um Verständnis fur diese Überprufung. Alle Sparkassenkonten die nicht innerhalb eines Tages authentifiziert werden, werden gesperrt!

sparkasse.de 2006 Alle Rechte vorbehalten. Vervielf?igung nur mit Genehmigung der Sparkassen-Finanzportal GmbH

Tarnung
Doppelte Dateiendungen

- irreführendes/falsches Symbol
- Ausblenden von bekannten Dateiendungen problematisch

Symbolansicht:

Rechnung.pdf

Detailansicht mit allen Dateiendungen eingeblendet:

Name	Größe	Typ
Rechnung.pdf ...	64 KB	Anwendung

Detailansicht:

Name	Größe	Typ
Rechnung.pdf .exe	64 KB	Anwendung

doppelte Endung meist durch hunderte von Leerzeichen trennt

Tarnung
Verschiedene Endungen für Executables

- .exe
- .com
- .bat
- .cmd
- .pif
- .scr
- .cpl

- .hta
- .vbs
- .vbe
- .chm
- .wsh
- ...

Warum so viel Windows-Malware?

- sehr weite Verbreitung von Windows (ca. 90% der Clientsysteme)
- „schlechtes“ Sicherheitsdesign bzw. fast nie vollständig ausgenutzt
- Windows wird von vielen „Anfängern“ benutzt
- fragwürdige Standard-Einstellungen

Desinfektion

einzelne „infizierte“ Datei

Desinfektion bzw. Löschung i.d.R. problemlos möglich

Desinfektion

einzelne „infizierte“ Datei

Desinfektion bzw. Löschung i.d.R. problemlos möglich

„infiziertes“ System

Desinfektion nicht sicher möglich $\Rightarrow$ Neuinstallation

AV-Software testen

Eicar-„Testvirus“

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Download unter: http://www.eicar.org

Virentest

http://www.virustotal.com

Complete scanning result of "Trojan.BAT.Delwin.ao", received in VirusTotal at 12.21.2006, 01:18:57 (CET).

STATUS: FINISHED

Antivirus	Version	Update	Result
AntiVir	7.3.0.19	12.20.2006	BAT/Delwin.wb
Authentium	4.93.8	12.20.2006	BAT/DelWin@troj
Avast	4.7.892.0	12.20.2006	BV:Malware
AVG	386	12.20.2006	no virus found
BitDefender	7.2	12.21.2006	BAT.Trojan.DelSys.AB
CAT-QuickHeal	8.00	12.20.2006	no virus found
ClamAV	devel-20060426	12.20.2006	Trojan.Bat.DelWin-12
DrWeb	4.33	12.20.2006	Trojan.DelWin.243
eSafe	7.0.14.0	12.19.2006	Win32.BAT.Delwin.ao
eTrust-InoculateIT	23.73.91	12.20.2006	Bat/Lovenot.A!Trojan
eTrust-Vet	30.3.3264	12.20.2006	no virus found
Ewido	4.0	12.20.2006	Trojan.Delwin.ao
Fortinet	2.82.0.0	12.20.2006	BAT/Delwin.AO!tr
F-Prot	3.16f	12.20.2006	BAT/DelWin@troj
F-Prot4	4.2.1.29	12.20.2006	BAT/DelWin@troj
Ikarus	T3.1.0.27	12.20.2006	Trojan.BAT.Delwin.ao
Kaspersky	4.0.2.24	12.20.2006	Trojan.BAT.Delwin.ao
McAfee	4923	12.20.2006	Bat/qd16
Microsoft	1.1904	12.21.2006	BAT/LoveLetter
NOD32v2	1932	12.20.2006	BAT/Delwin.AO
Norman	5.80.02	12.20.2006	BAT/Trojan.gen
Panda	9.0.0.4	12.21.2006	Trj/Bat.Gen
Prevx1	V2	12.21.2006	Trojan:BAT:(Delwin.ap)
Sophos	4.12.0	12.18.2006	Troj/LoveNote-A
Sunbelt	2.2.907.0	12.18.2006	no virus found
TheHacker	6.0.3.135	12.20.2006	no virus found
UNA	1.83	12.20.2006	no virus found
VBA32	3.11.1	12.20.2006	Trojan.BAT.Delwin.ao#1

Ausblick

- andere Systeme (PDA, Handy)
- Methodisch neue Angriffe
- gezielte Angriffe
- regional begrenzte Angriffe

Zusammenfassung

- „kein Virus gefunden“ $\neq$ „kein Virus vorhanden“
- keine 100%ige Sicherheit möglich
- gefährlichste Zeit zw. Outbreak und Erkennung durch AVs

Noch Fragen?

eMail: sven@clamav.net