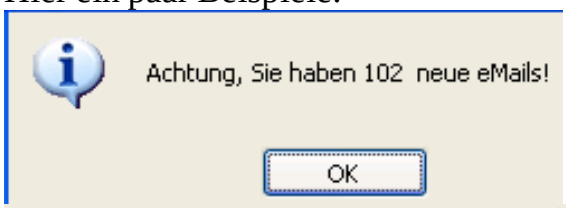
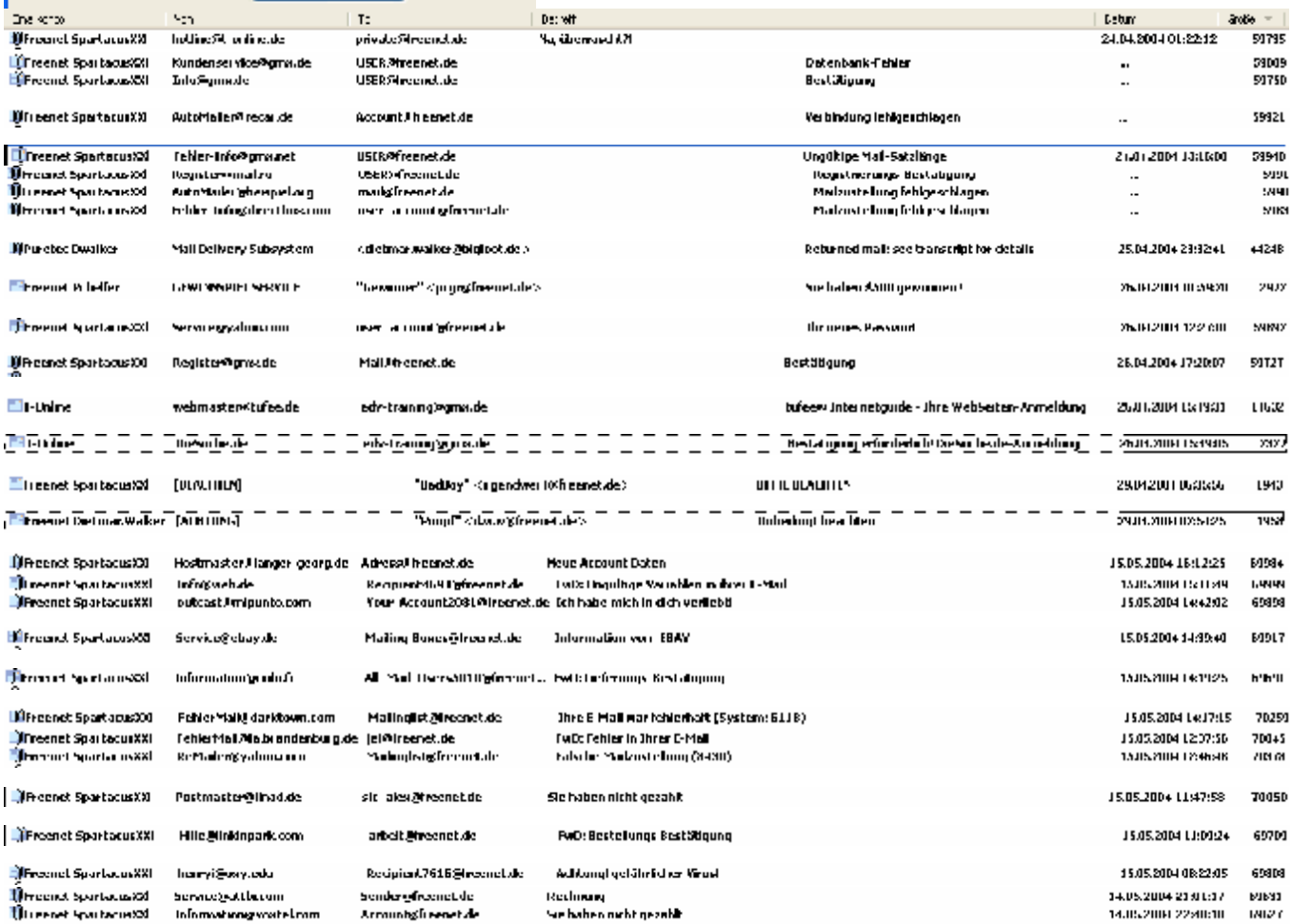
Beispiele von virenverseuchten Emails

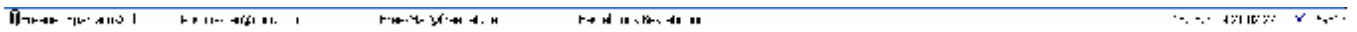
Die Virenverseuchten Email-Betreffs werden immer raffinierter. Jetzt auch in Deutsch!
Hier ein paar Beispiele:

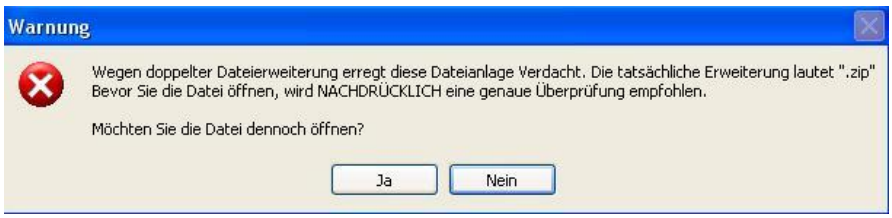


Ein Service von
www.pc-blitzhelfer.de



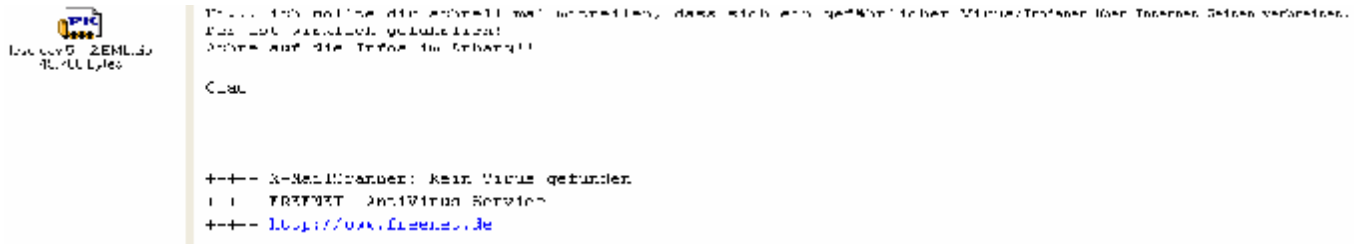
Wenn man die Emails öffnet
1. Bsp:



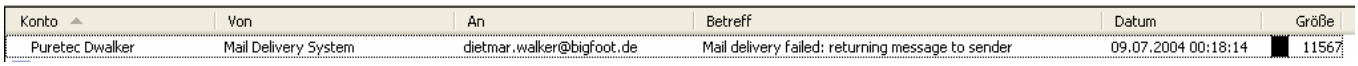


Das klassische Beispiel, doppelte Dateinamen zur Verschleierung der Dateierweiterung.

2. Bsp:



Man siehe die Frechheit, es wird behauptet „Kein Virus gefunden“.
Natürlich ist in beiden Email ein Virus enthalten!!!



Konto	Von	An	Betreff	Datum	Größe
Puretec Dwalker	Mail Delivery System	dietmar.walker@bigfoot.de	Mail delivery failed: returning message to sender	09.07.2004 00:18:14	11567

Quelle: text.zip
Beschreibung: Der E-Mail-Anhang text.zip innerhalb von Unknown00000000.data ist mit dem Virus W32.Netsky.P.dam infiziert.
Klicken Sie hier, um weitere Informationen über diese Bedrohung zu erhalten:
W32.Netsky.P.dam

Netsky war enthalten

W32/Netsky-O

Alias

Win32/Netsky.P, WORM_NETSKY.GEN

Typ

Win32-Wurm

Erkennung

Wird seit März 2004 von Sophos Anti-Virus erkannt.

Erläuterung

W32/Netsky-O ist ein Wurm, der sich per E-Mail verbreitet.

Damit er automatisch beim Start von Windows aktiviert wird, kopiert sich der Wurm in die Datei AVBgle.exe im Windows-Ordner und erstellt den folgenden Registrierungseintrag:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MsInfo
= C:\Windows\AVBgle.exe.

Der Wurm versucht, verschiedene Antiviren- und Sicherheitsanwendungen zu deaktivieren, indem er Registrierungseinträge löscht, die von diesen Anwendungen verwendet werden.

Im Besonderen versucht er, die folgenden Einträge zu löschen:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\
für Taskmon, Explorer, KasperskyAv, system., msgsvr32, DELETE ME,
service, Sentry, Windows Service Host

sowie unter Einträge unter HKCU\Software\Microsoft\Windows\CurrentVersion\Run\
für Taskmon, Explorer, KasperskyAv, d3dupdate.exe, au.exe, OLE,
Windows Service Host, gouday.exe, rate.exe, sysmon.exe, srate.exe
und ssate.exe.

Der Wurm löscht außerdem die folgenden Einträge:

HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices\system
HKCR\CLSID\E6FB5E20-DE35-11CF-9C87-00AA005127ED\InProcServer32
HKCU\System\CurrentControlSet\Services\WksPatch
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\PINF

Diese Einträge werden teilweise von den verschiedenen Varianten der Würmer aus der Familie von W32/Bagle erzeugt.

W32/Netsky-O durchsucht alle lokalen Laufwerke nach Dateien mit der Erweiterung XML, WSH, JSP, DHTM, CGI, SHTM, MSG, OFT, SHT, DBX, TBB, ADB, DOC, WAB, ASP, UIN, RTF, VBS, HTML, HTM, PL, PHP, TXT oder EML und versucht, in diesen Dateien an E-Mail-Adressen zu gelangen.

Um sich zu verbreiten, erstellt der Wurm 16 Threads, die E-Mails mit dem Wurm als Attachment an die aufgespürten Adressen senden. W32/Netsky-O verwendet zum Versenden der E-Mails seine eigene SMTP-Engine. Die Betreffzeilen, die Texte und die Dateinamen der Attachments werden zufällig aus den folgenden Möglichkeiten ausgewählt:

Betreffzeilen:
Re: Encrypted Mail
Re: Extended Mail
Re: Status
Re: Notify
Re: SMTP Server
Re: Mail Server
Re: Delivery Server
Re: Bad Request
Re: Failure
Re: Thank you for delivery
Re: Test
Re: Administration
Re: Message Error
Re: Error
Re: Extended Mail System
Re: Secure SMTP Message
Re: Protected Mail Request
Re: Protected Mail System
Re: Protected Mail Delivery
Re: Secure delivery
Re: Delivery Protection
Re: Mail Authentification

Texte:
Please confirm my request.
ESMTP [Secure Mail System #334]: Secure message is attached.
Partial message is available.
Waiting for a Response. Please read the attachment.
First part of the secure mail is available.
For more details see the attachment.
For further details see the attachment.
Your requested mail has been attached.
Protected Mail System Test.
Secure Mail System Beta Test.
Forwarded message is available.
Delivered message is attached.
Encrypted message is available.
Please read the attachment to get the message.
Follow the instructions to read the message.
Please authenticate the secure message.
Protected message is attached.
Waiting for authentification.
Protected message is available.
Bad Gateway: The message has been attached.
SMTP: Please confirm the attached message.
You got a new message.
Now a new message is available.
New message is available.
You have received an extended message. Please read the instructions.

Namen der angehängten Datei:
readme.pif
document.pif
data.pif
details.pif
message.pif

Der Text enthält außerdem eine der folgenden gefälschten Antiviren-Signaturen:

+++ Attachment: No Virus found
+++ Panda AntiVirus - You are protected
+++ www.pandasoftware.com

+++ Attachment: No Virus found
+++ Norman AntiVirus - You are protected
+++ www.norman.com

+++ Attachment: No Virus found
+++ F-Secure AntiVirus - You are protected
+++ www.f-secure.com

+++ Attachment: No Virus found
+++ Norton AntiVirus - You are protected
+++ www.symantec.de.

Sogar der allseits bekannte Loveletter tummelt sich noch irgendwo …