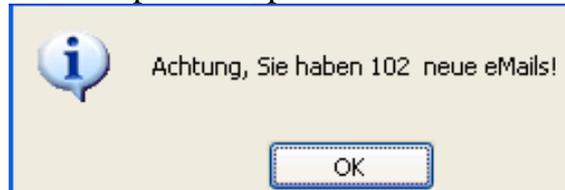


Beispiele von virenverseuchten Emails

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



Ein Service von www.pc-blitzhelfer.de

Objekt	Von	Nach	Datum	Größe	
Freenet SpartacusXXI	Info@freenet.de	private@freenet.de	24.04.2004 01:22:12	59795	
Freenet SpartacusXXI	Kundenservice@freenet.de	USER@freenet.de	..	59009	
Freenet SpartacusXXI	Info@freenet.de	USER@freenet.de	..	59750	
Freenet SpartacusXXI	AutoMails@freenet.de	Account@freenet.de	..	59921	
Freenet SpartacusXXI	Fehler-Info@freenet.de	USER@freenet.de	24.04.2004 13:16:00	59910	
Freenet SpartacusXXI	Registrierung@freenet.de	USER@freenet.de	..	59921	
Freenet SpartacusXXI	AutoMails@freenet.de	mail@freenet.de	..	59901	
Freenet SpartacusXXI	Fehler-Info@freenet.de	user-account@freenet.de	..	59921	
FreeNet Walker	Mail-Delivery-Subsystem	red@mar.walker2@freenet.de	25.04.2004 23:22:41	44248	
Freenet Walker	LEW@freenet.de	"freenet" <ping@freenet.de>	26.04.2004 00:04:20	2407	
Freenet SpartacusXXI	Service@freenet.de	user-account@freenet.de	26.04.2004 12:27:00	59907	
Freenet SpartacusXXI	Register@freenet.de	Mail@freenet.de	26.04.2004 17:20:07	59727	
i-Online	webmaster@freenet.de	odr-training@freenet.de	26.04.2004 16:19:03	11632	
Freenet	user@freenet.de	user-account@freenet.de	26.04.2004 15:49:05	2527	
Freenet SpartacusXXI	[UNREKANN]	"Uedley" <gedwin10@freenet.de>	29.04.2004 16:35:36	1943	
Freenet FreeNet Walker	[UNREKANN]	"Munip" <blau@freenet.de>	29.04.2004 03:51:25	1452	
Freenet SpartacusXXI	Hostmaster@fanger-georg.de	Adress@freenet.de	Neue Account Daten	15.05.2004 16:11:25	69584
Freenet SpartacusXXI	Info@freenet.de	Request@freenet.de	Für die Inquiries-Mails wählen wir Ihren E-Mail	15.05.2004 15:11:34	14998
Freenet SpartacusXXI	outcast@freenet.de	Your Account 2081@freenet.de	Ich habe mich in dich verliebt!	15.05.2004 14:42:02	69858
Freenet SpartacusXXI	Service@ebay.de	Mail@ebay.de	Information von EBAY	15.05.2004 14:35:40	69917
Freenet SpartacusXXI	Information@freenet.de	All-Mail-User@freenet.de	FW: E-Mail-Formular Bestätigung	15.05.2004 14:31:25	69910
Freenet SpartacusXXI	Fehler-Mail@darktown.com	Mail@freenet.de	Ihre E-Mail war fehlerhaft (System: 6118)	15.05.2004 14:17:15	70259
Freenet SpartacusXXI	Fehler-Mail@darktown.com	jei@freenet.de	Fw: Fehler in Ihrer E-Mail	15.05.2004 12:37:36	70045
Freenet SpartacusXXI	Request@freenet.de	Mail@freenet.de	Falsche Mailzustellung (8430)	15.05.2004 12:06:06	70101
Freenet SpartacusXXI	Postmaster@freenet.de	st-alex@freenet.de	Sie haben nicht gezahlt	15.05.2004 11:47:58	70050
Freenet SpartacusXXI	Hille@freenet.de	arbeit@freenet.de	Fw: Bestellungen Bestätigung	15.05.2004 11:09:24	69709
Freenet SpartacusXXI	harry@freenet.de	Request@freenet.de	Achtung gefährlicher Virus!	15.05.2004 08:22:05	69808
Freenet SpartacusXXI	Service@freenet.de	benutzer@freenet.de	Rechnung	14.05.2004 23:01:37	69893
Freenet SpartacusXXI	Information@freenet.de	Account@freenet.de	Sie haben nicht gezahlt	14.05.2004 22:40:30	69977

Wenn man die Emails öffnet

1. Bsp:

Objekt	Von	Nach	Datum	Größe
Freenet SpartacusXXI	Info@freenet.de	private@freenet.de	24.04.2004 01:22:12	59795



Das klassische Beispiel, doppelte Dateinamen zur Verschleierung der Dateierweiterung.

2. Bsp:



Bitte nicht die Antwort mit einstellen, dass sich ein gefährlicher Virus/Trojaner über Internet Seiten verbreitet.
Es ist ziemlich gefährlich!
Bitte auf die Infos im Anhang!!!

CaL

```
+++ K-Scan-Scanner: kein Virus gefunden
+--- FREEMIT Antivirus Service
+++ 100177000@free.de
```

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 Authentication

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 authentication.
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 ...

The screenshot shows two windows from a Windows operating system. The top window is 'Norton AntiVirus'. On the left, there is a yellow sidebar with the text '1 Status der Prüfung', '2 Reparaturassistent', and 'Beheben'. The main area shows a pop-up window titled 'E-Mail-Informationen:' with the following details: 'Absender: rwinkler@wolters-kluwer.de', 'Empfänger: dietmar.walker@bigfoot.de', and 'Betreff: I love you!'. Below this, a table lists detected items:

<input checked="" type="checkbox"/>	Dateiname	Name der Bedro...	Aktion	Status
<input checked="" type="checkbox"/>	CCD6.tmp	W32.Netsky.P@...	Virus gefunden	Reparat...

The bottom window is 'Posteingang' (Inbox). It shows a list of emails with the following columns: 'Von', 'Betreff', 'Erhalten', 'Größe', 'An', 'Erstellt', and 'E...'. One email is visible: 'Symantec E-Mail-Proxy' with the subject 'Symantec E-Mail-Proxy hat eine Nachricht gelöscht', received on 'Do 15.07.2004 12:13', size '1 KB', and created on 'Do 15.07.2004 12:12'.