Select language

Viren Info Produkte Support Partner Download Company Kontakt

Virensuche
Virenname eingeben:
Go

Service & Information
News
Sicherheitshinweise
Neue Viren
Virengeschichte
Virenkategorien
Glossar
G DATA Partnerweb
Links

Viren Top 10
1. Mytob
2. Netsky
3. Sober
4. Bagle
5. Zafi
6. Lovgate
7. Nyxem
8. Mydoom
9. Bankfraud
10. Pechkin

Wir suchen ...

Newsletter abonnieren

RSS *NewsFeed*

Viren Datenbank

Email-Worm.Win32.Nyxem.e

Alias: Email-Worm.Win32.Nyxem.e (Kaspersky), W32.Blackmal.E@mm (Symantec), W32/Nyxem-D (Sophos), W32/MyWife.d@MM (McAfee), W32/Grew.A!wm (Fortinet), W32/Small.KI@mm (Norman), Win32/Blackmal.F (Computer Associates), Tearec.A (Panda), WORM_GREW.{A, B} (Trend Micro)

Infektionsrisiko: (sehr häufig)

Schadenspotential: (zerstörerisch)

Erkannt seit AVK version: 16.5003, Datum 19.1.2006
(Hilfe: *Wie erkenne ich meine AVK version?*)

Allgemeine Beschreibung:

Bei Email-Worm.Win32.Nyxem.e handelt es sich um eine Variante von '*Email-Worm.Win32.Vb.bi*' mit einer gefährlichen Schadensfunktion. Er verbreitet sich in hohem Maß per E-Mail oder über die Standardfreigaben Admin$ und C$ im lokalen Netzwerk. Die E-Mails kommen mit Betreffs wie '*Hot Movie*', 'A Great Video', 'Arab sex DSC-00465.jpg', 'eBook.pdf', 'Fuckin Kama Sutra pics', 'Fw: DSC-00465.jpg', 'Fw: Funny :)', 'Fw: Picturs', 'Fw: Sexy', 'Fwd: image.jpg', 'Fwd: Photo', 'Miss Lebanon 2006', 'My photos', 'Part 1 of 6 Video clipe', 'Re: Sex Video', 'School girl fantasies gone bad', 'The Best Videoclip Ever', 'the file', 'Word file', 'You Must View This Videoclip!'. Der Dateianhang ist im Dateiformat PIF, SCR oder ZIP oder kann in MIME-Formaten wie MIM, HQX, B64, BHX, UUE, UU vorliegen.

Wer den Dateianhang öffnet startet den Wurm, der sich auf den Rechner kopiert, in die Registry einträgt. Dann beendet er Prozesse von Antiviren-Software und löscht deren Dateien und Registry-Einträge. Dann durchsucht er den Rechner nach E-Mailadressen an die er sich mit der integrierten SMTP-Engine versendet.

Email-Worm.Win32.Nyxem.e hat eine fiese Schadfunktion. An jedem 3. eines Monats überschreibt er auf allen zugänglichen Laufwerken (also auch

Netzlaufwerken) Dateien im Format "DMP", "DOC", "MDB", "MDE", "PDF", "PPS", "PPT", "PSD", "RAR", "XLS", "ZIP".

Schadensfunktionen:
Überschreibt Dateien im Format "DMP", "DOC", "MDB", "MDE", "PDF", "PPS", "PPT", "PSD", "RAR", "XLS", "ZIP" an jedem 3. eines Monats auf allen zugänglichen Laufwerken, inklusive Netzlaufwerke. Die Inhalte der Datei werden mit dem Text "DATA Error [47 0F 94 93 F4 K5]" überschrieben.

Systemvoraussetzungen:
Windows, VisualBasic Runtime

Symptome:
Dateien:
%WINDOWS%\rundll16.exe
%WINDOWS%\Winzipi_TMP.exe
%SYSTEM%\scanregw.exe
%SYSTEM%\Update.exe
%SYSTEM%\Winzip.exe
%SYSTEM%\Winzip_TMP.exe
%SYSTEM%\Sample.ZIP
%SYSTEM%\MSWINSCK.OCX (Internet Connectivity, 55.808 Bytes)
\C$\Dokumente und Einstellungen\All Users\StartMenü\Programme\AutoStart\WinZip Quick Pick.exe
\C$\Dokumente und Einstellungen\All Users\StartMenü\Programme\AutoStart\WinZip Quick Pick.lnk

Registry:
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
"ScanRegistry" = "%System%\scanregw.exe /scan"

Entfernung:
Mit unserem Removal tool: *Download*

Verbreitung:

Email-Worm.Win32.Nyxem.e nutzt drei Möglichkeiten sich zu verbreiten.
1. Netzwerkfreigaben
Er kopiert sich als "WINZIP_TMP.exe" in die Standard-Netzwerkfreigaben Admin$ und C$ oder als "WinZip Quick Pick.exe" in den Autostart-Ordner von "All users".

2. Active Desktop
Nyxem nutzt auch eine ungewöhnliche Art der Verbreitung. Er verändert die Einstellungen in der Datei "desktop.htt" so, dass bei jedem Start des Active Desktop die Datei C:\WINZIP_TMP.exe geladen wird. Auch die entsprechende desktop.ini Datei wird so modifiziert, dass sie auf eine verseuchte Datei namens "Temp.htt" verweist

3. Verbreitung per E-Mail

Email-Worm.Win32.Nyxem.e verbreitet sich per E-Mail mit seiner integrierten SMTP-Engine. Die Emailadressen sucht er auf dem lokalen Rechner in -Dateien. Er sendet sich nicht an Adressen, die folgende Zeichenketten enthalten:

"ANTI", "AVG", "BLOCKSENDER", "CA.COM", "CILLIN", "EEYE", "GROUPS.MSN", "HOTMAIL", "MICROSOFT", "MSN", "MYWAY", "NOMAIL.YAHOO.COM", "PANDA", "SCRIBE", "SECUR", "SPAM", "TREND", "YAHOOGROUPS"

Die E-Mails, in denen er sich versendet haben folgendes Format:
Betreff:

- ***Hot Movie***
- **A Great Video**
- **Arab sex DSC-00465.jpg**
- **eBook.pdf**
- **Fuckin Kama Sutra pics**
- **Fw:**
- **Fw: DSC-00465.jpg**
- **Fw: Funny :)**
- **Fw: Picturs**
- **Fw: Sexy**
- **Fwd: image.jpg**
- **Fwd: Photo**
- **give me a kiss**
- **Miss Lebanon 2006**
- **My photos**
- **Part 1 of 6 Video clipe**
- **Re:**
- **Re: Sex Video**
- **School girl fantasies gone bad**
- **The Best Videoclip Ever**
- **the file**
- **Word file**
- **You Must View This Videoclip!**

Nachrichtentext:

- **----- forwarded message -----**
- **>> forwarded message**
- **Fuckin Kama Sutra pics**
- **forwarded message attached.**
- **Hot XXX Yahoo Groups**
- **how are you?**
- **i just any one see my photos. It's Free :)**

i send the details.
Note: forwarded message attached.
OK ?
Please see the file.
ready to be FUCKED ;)
VIDEOS! FREE! (US$ 0,00)

Dateianhang:

"007.pif", "04.pif", "677.pif", "Adults_9,zip .sCR", "ATT01.zip .sCR", "Atta [001],zip .SCR", "Attachments,zip .SCR", "Attachments[001],B64 .sCr", "Attachments[001].B64", "Attachments00.HQX", "Attachments001.BHX", "Clipe,zip .sCr", "document.pif", "DSC-00465.Pif", "DSC-00465.pIf", "eBook.PIF", "eBook.Uu", "image04.pif", "New Video,zip .sCr", "New_Document_file.pif", "Original Message.B64", "photo.pif", "Photos,zip .sCR", "School.pif", "SeX,zip .scR", "SeX.mim", "Sex.mim", "Video_part.mim", "WinZip,zip .scR", "WinZip.BHX", "WinZip.zip .sCR", "Word.zip .sCR", "Word_Document.hqx", "Word_Document.uu"

Tarnung:
Um sich vor AntiViren-Software zu schützen löscht Email-Worm.Win32.Nyxem.e die Einträge in den Registry-Schlüsseln [Software\Microsoft\Windows\CurrentVersion\Run], [Software\Microsoft\Windows\CurrentVersion\Run] und [Software\Microsoft\Windows\CurrentVersion\RunServices], wenn sie eine der folgenden Zeichenketten enthalten: "APVXDWIN", "avast!", "AVG_CC", "AVG7_CC", "AVG7_EMC", "AVG7_Run", "Avgserv9.exe", "AVGW", "BearShare", "ccApp", "CleanUp", "defwatch", "DownloadAccelerator", "kaspersky", "KAVPersonal50", "McAfeeVirusScanService", "MCAgentExe", "McRegWiz", "MCUpdateExe", "McVsRte", "MPFExe", "MSKAGENTEXE", "MSKDetectorExe", "NAV Agent", "NPROTECT", "OfficeScanNT Monitor", "PCCClient.exe", "pccguide.exe", "PCCIOMON.exe", "PCClient.exe", "PccPfw", "Pop3trap.exe", "rtvscn95", "ScanInicio", "ScriptBlocking", "SSDPSRV", "TM Outbreak Agent", "tmproxy", "Vet Alert", "VetTray", "VirusScan Online", "vptray", "VSOCheckTask"

Historisches:
Email-Worm.Win32.Nyxem.e sorgte für die erste große Infektionswelle in 2006. Innerhalb weniger Tage hat er mehr als 500.000 Rechner infiziert. Mit seiner aggressiven Payload ist er der erste weit verbreitete Wurm seit langer Zeit, der die Dateien eines Rechners überschreibt.

Technische Details:

Programmiersprache: Visual Basic
Größe: 95744 Bytes komprimiert mit UPX

Copyright (c) 2006 by G DATA Software AG | *Impressum*

Select language

Viren Info Produkte Support Partner Download Company Kontakt

Virensuche
Virenname eingeben:
Go

Service & Information
News
Sicherheitshinweise
Neue Viren
Virengeschichte
Virenkategorien
Glossar
G DATA Partnerweb
Links

Viren Top 10
1. Mytob
2. Netsky
3. Sober
4. Bagle
5. Zafi
6. Lovgate
7. Nyxem
8. Mydoom
9. Bankfraud
10. Pechkin

Wir suchen ...

Newsletter abonnieren

RSS *NewsFeed*

Viren Datenbank

Worm.Win32.Feebs.gen

Alias: W32.Feebs, Worm.Win32.Feebs.gen, W32/Kmax
Typ: Wurm

Infektionsrisiko: (sehr häufig)

Schadenspotential: (gefährlich)

Erkannt seit AVK version: 16.4888, Datum 12.1.2006
(Hilfe: *Wie erkenne ich meine AVK version?*)

Allgemeine Beschreibung:
Die Würmer aus der Feebs-Familie verbreiten sich per E-Mail und Peer-to-Peer Tauschbörse. Normalerweise kommt Feebs als äußerst wandelbare, polymorphe Datei im Format HTA (HyperText Application). Diese Datei kopiert die ausführbaren Dateien auf den Rechner und führt sie aus.
Der Wurm registriert sich dann, kopiert sich in Freigaben von P2P-Programmen und beendet sicherheitsrelevante Software. Danach startet er einen HTTP-Server (Port 80), von dem andere Rechner die HTA-Dateien laden können. Auf einem zufälligen Port wird ein weitere Server installiert, der es ermöglicht den Rechner vollständig zu kontrollieren.

Mit der integrierten Rootkit-Technologie versteckt Feebs seine Dateien, Registry-Einträge und Netzwerkverbindungen.

Symptome:

Dateien:
%SYSTEM%\ms<zufällige Zeichenkette>32.dll
%SYSTEM%\ms<zufällige Zeichenkette>32.exe

Registry:
[HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad]

"%SYSTEM%\ms<zufällige Zeichenkette>32.dll" = "{[zufällige CLSID]}"

[HKML\CLSID\{[zufällige CLSID]}\InprocServer32]
"(default)" = "%SYSTEM%\ms<zufällige Zeichenkette>32.dll"

Copyright (c) 2006 by G DATA Software AG | *Impressum*

Select language

Viren Info Produkte Support Partner Download Company Kontakt

Virensuche
Virenname eingeben:
Go

Service & Information
News
Sicherheitshinweise
Neue Viren
Virengeschichte
Virenkategorien
Glossar
G DATA Partnerweb
Links

Viren Top 10
1. Mytob
2. Netsky
3. Sober
4. Bagle
5. Zafi
6. Lovgate
7. Nyxem
8. Mydoom
9. Bankfraud
10. Pechkin

Wir suchen ...

Newsletter abonnieren
RSS *NewsFeed*

Viren Datenbank

Win32.Worm.Mytob.BT

Alias: Net-Worm.Win32.Mytob.bt (Kaspersky Lab), Win32.Worm.Mytob.BT (BitDefender), W32/Mytob.el@MM (McAfee), W32/Mytob-DI (Sophos), WORM_MYTOB.HS (Trend Micro)

Erkannt seit AVK version: BD 15.0.1006, Datum 19.5.2005
(Hilfe: *Wie erkenne ich meine AVK version?*)

Allgemeine Beschreibung:
Diese Version des Mytob-Wurms verbreitet sich per Email. Die Betreffs lauten Your password has been updated
Your password has been successfully updated
You have successfully updated your password
Your new account password is approved
Warning MessageYour services near to be closed
Important notification
***DETECTED* Online User Validation**
Notice of account limitation
Your account is suspended
Your account is suspended for security reasons
Members support
Security measures
[ZUFALLSZEICHEN] Der Absender ist gefälscht. Der Name der Datei im Anhang lautet "updated-password", "important-details", "urph", "wmoke", "account-report", "account-details", "updated-password", "readme", "document", "password", "accepted-password", "email-details", "account-password", "new password", "[4 bis 8 ZUFALLSZEICHEN]" Die Dateiendung lautet "zip" oder besteht aus einer Kombination der folgenden doppelten Dateiendung.
"(htm|txt|doc)[VIELE LEERZEICHEN].(pif|exe|scr|cmd|bat)"

Schadensfunktionen:

Reduziert die Sicherheit des Rechners durch Manipulation der HOSTS-Datei

Öffnet eine Backdoor auf TCP Port 7745, die vollen Zugriff auf den Rechner erlaubt.

Systemvoraussetzungen:
alle Win 32 bit

Symptome:
Dateien:
%SYSTEM%\M0USE.exe

Registry:
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"Userinterface Report3r" = "%SYSTEM%\M0USE.exe"
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices]
"Userinterface Report3r" = "%SYSTEM%\M0USE.exe"
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"Userinterface Report3r" = "%SYSTEM%\M0USE.exe"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"Shell" = "Explorer.exe M0USE.exe"

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess]
"Start" = "4"
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess]
"Start" = "4"

Verbreitung:
Win32.Worm.Mytob.BT sucht auf dem lokalen Rechner in zahlreichen Dateitypen nach Emailadressen und versendet sich an diese, sofern sie nicht bestimmten Filterkriterien entsprechen. So vermeidet es der Wurm sich an Antivirenhersteller und Sicherheitsexperten zu versenden.

Technische Details:
Größe: 32.804 Byte

Copyright (c) 2006 by G DATA Software AG | *Impressum*