

ADVERTISEMENT



View demo





SUBSCRIBE TODAY



[Home](#) > [News and Analysis](#) > [Special Reports](#) > [Security Watch](#) > [SW Newsletter](#) > **Dumaru.Y—Very New and Very Dangerous**

Dumaru.Y—Very New and Very Dangerous

By Jay Munro

January 27, 2004

[Total posts: 1](#)

[Click here](#) to subscribe to our Security Watch newsletter.

 Print  Email  Save  Discuss  Subscribe

Dumaru.Y—Very New and Very Dangerous

This week's top threat is W32/Dumaru.Y-mm. Discovered on Saturday, Jan 23rd, it jumped from obscurity to one of the top 10 email viruses, Dumaru. Y-mm, like other Dumaru variants is a nasty character. Arriving in a .ZIP attachment promising provocative photos, it uses tricks to mask the true executable file. When victims try to look at the images, they find their machines infected, security products shut down, and more copies of Dumaru.Y being sent to everyone on their address list. Antivirus vendors scrambled to analyze it and by Sunday night most had issued warnings and had added detection to their latest updates. If you haven't updated lately, you should now to avoid this potentially dangerous threat. As a late breaking development, Monday saw another similar strain, W32/Dumaru.Z, as well as another Mimail variant, W32/Mimail.Q-mm. The antivirus vendors are analyzing them currently, and we'll be watching if they develop into a major threat in the week to come.

RELATED LINKS

► [Breaking Virus News: MyDoom Hobbles Internet E-mail](#)

Last week's Bagle virus is still making waves, especially in the media with the debate over whether it is hype or threat. In terms of distribution, the relatively harmless W32/Bagle.A-mm is the first significant virus of the New Year. While shooting blanks as far as damage to machines, it

does mine addresses, and does send out vast quantities of mail, filling up email servers and mail boxes. Industry magazine, Virus bulletin ([www.virusbtn.com](#)) noted "At first glance, W32/Bagle.A is not a particularly interesting virus from a technical point of view. Or, indeed, at a second glance." They did say that vendors are suggesting that the expiration date may mean future versions are planned, similar to the Sobig legacy of last year. Though scheduled to die tomorrow, Jan 28th, Bagle infection rates were already slowing down late last week according to MessageLabs and antivirus software vendors.

Other than Bagle and Dumaru.Y, the top ten virus threats according to MessageLabs are still the old favorites, Klez, Sobig, Dumaru.A, Mimail, and

table of contents

- [Introduction](#)
- [Top Threat](#)
- [Security Tip](#)
- [Top 10 E-Mail Viruses](#)
- [Top 5 Vulnerabilities](#)
- [Microsoft Security Updates](#)
- [Jargon Buster](#)
- [Security Watch Story Feed](#)

news

- [MyDoom.F-mm Starting Slow, But Has Scary Potential](#)
- [This Worm Only Wants to Heal](#)
- [A Front Row Seat to a Major Attack](#)
- [MyDoom.A: Fastest Spreading Virus in History](#)
- [Dumaru.Y—Very New and Very Dangerous](#)

[View All >](#)

new white papers

-  [Want to Let Customers Know Your Website is Safe?](#)
 -  [Looking for mission-critical server security?](#)
 -  [Protect Your Network from Corporate E-mail Threats](#)
- [All White Papers >](#)

ADVERTISEMENT

Baseline
THE PROJECT MANAGEMENT CENTER

COMPUTER NETWORKS SECURITY XML DATABASES AND MORE

CHECK OUT

PRIMERS @ BASELINE

CLICK HERE

FREE CD-Burner Upgrade with purchase of select new Dell Home Systems.

Offer expires 2/25.

DELL

► CLICK HERE

ADVERTISEMENT

Partner Services:

Swen. Antivirus vendors track threats based on various input, such as hits by free online scanners, or reporting mechanisms built into corporate and consumer antivirus utilities. Because each vendor uses a different metric, some threats may be more prevalent in one sector than another. We looked at some of the major vendors to see what else they were reporting. TrendMicro [reports](#) that WORM_LOVGATE.G, is the top worldwide threat as detected by their Housecall free online virus scanner. McAfee [reports](#) JS/NoClose is their top virus tracked by AVERT. JS/NoClose is a JavaScript threat that keeps an Internet Explorer window open, despite attempts to close it. The script is harmless, but irritating. Symantec (SARC) is reporting W32/Bugbear.B at the top of their list. As a risk level 4 (highest is 5), [Bugbear.B](#) is widely distributed, and very damaging. Sophos [reports](#) Sober.C as the top threat in December 2003. Sometimes a picture is better than words, and several antivirus vendors offer maps and/or graphs showing the state of the threat world. Here are a few daily maps and graphs you may find interesting -- [MessageLabs](#) , [F-secure](#), and [Panda Software](#).

TrendMicro is reporting a new Visa phish, [HTML_VISAFRAUD.A](#), which uses the Internet Explorer URL spoof to [mask](#) its fake Visa host web site. The pseudo site attempts to trick victims into giving up their credit card information. The e-mail message tells the user they can register for Visa's Zero Liability coverage, which covers them in case of credit card fraud (like phishing). Informed users will know, however, that Visa instituted Zero Liability in April of 2000 as a replacement for the original \$50 fraud liability. The coverage is free, and included automatically with the card.

While security is a big concern in the business world, sometimes it spills over into the network gamer world. On Friday Jan 23, Secunia reported a highly critical [vulnerability](#) in Need for Speed Hot Pursuit II, a multiplayer network game. An attacker could potentially exploit a "boundary error" in the client causing a buffer overflow and allowing arbitrary code to be run on the user's machine. The work-around is to play only on known secure networks.

Some good news on the fraud front: [Security Focus](#) is reporting that the Ohio woman who sent forged mails from "AOL Security" has been sentenced to 46 months in prison. The forged e-mails claimed that the victims' credit cards had failed on the last AOL bill and they needed to re-enter their information. The woman was caught soon after she spammed an off-duty FBI agent in.

[next >](#)

- ▶ [Dell Business Systems](#)
- ▶ [Dell Home Systems](#)
- ▶ [MPC \(MicronPC\)](#)

Baseline
THE PROJECT MANAGEMENT CENTER

@ BASELINE
CLICK HERE

ZIFF DAVIS
CIO INSIGHT

@ Ziff Davis CIO Insight

Click Here

ZIFF DAVIS FEATURED SITES: [IT Reseller News & Resources](#)

▶▶▶ IN PRINT



SAVE UP TO 77%

SUBSCRIBE NOW & RECEIVE A FREE 3-VOLUME SOFTWARE SUPERPAC!

Name

Email (e.g. user@jsp.com)

Address

City

State Postal Code

FREE BONUS

Get our 3-Volume Software SuperPac loaded with utilities software, desktop customizers, games and more!

SUBSCRIPTION SERVICES

+ [Get Help with your Subscription](#)

- + [Renew - Give a Gift](#)
- + [Our New Digital Format](#)

Click "Continue"
to proceed to our
secure server.

newsletters

Get PCMag.com's **FREE** email newsletters delivered to your inbox.

It's easy, just follow the steps.

Want more? Check out our other newsletters [here](#).

Manage your newsletter subscriptions [here](#).

1. Make your selections:

- Inside PCMag.com
- Internet Business Technology
- Productwire: First Looks Update
- Tip of the Day
- PC Magazine's TrendWatch
- Utility Library Update
- Security Watch
- Shareware Update

2. Select email format:

3. Enter email address:



FREE ONLINE SEMINARS FOR EXECUTIVES AND IT PROFESSIONALS

- [2/03 - Special Edition Sun Net Talk Secure and Affordable: Sun's Java™ Desktop System in Action](#) with Michael Krieger. *Sponsored by Sun Microsystems, Inc.*
- [2/05 - Beyond Voice Mail: Reducing Business Costs With Latest Generation of Unified Communications Applications](#) with Frank Derfler. *Sponsored by AVST.*
- [2/18 - Instant Messaging: The Gateway to the Real-Time Enterprise](#) with Jim Louderback. *Sponsored by Yahoo.*

FREE Online Seminars
presented by [Intel](#)

- [PC Refresh: Your Strategy for Success!](#)
- [Server Consolidation-Expand Your Options](#)
- [Wireless LAN: One Size Doesn't Fit All](#)
- [PC Fleet Management: Tools & Strategies](#)

[view more eSeminars >>](#)

SHAREWARE.PCMAG.COM - HOT FILES

Download the best in free trial software from the [PCMag.com Shareware Library](#). Recent hot files:

- [SeeknClean](#) Cleans junk off your hard disk super fast!
- [Girder](#) Great tool for automating Windows.
- [DiskSpace Explorer Home Edition](#) Manage your hard disk space, find and delete useless items.
- [My Stuff](#) Home and personal inventory manager.
- [CyberScrub](#) CyberScrub removes all traces of online activity.

More [files at the Shareware Library >>](#)

NEW FROM ZIFF DAVIS E-LEARNING

Gain new IT and programming skills, prepare for accreditation, and more with online courses from [Ziff Davis eLearning](#).

- **New! Microsoft® Office® Skill Builders:** [Office XP](#), [Access](#), [Powerpoint](#), [Excel](#), [Word](#)
- **Development and IT:** [Java](#), [Adobe](#), [E-Business](#), [Linux](#), [Macromedia](#), [Macromedia Web Professional](#), [Oracle 8i](#), [Project Management](#), [SQL Server](#), [Visual Basic](#)
- **Certification Prep:** [A+](#), [Certified Novell Engineer](#), [iNET+](#), [MCSA](#), [MCSE](#), [Network+](#), [Security](#), [Server+](#)

See [all courses at Ziff Davis eLearning](#)

[>>](#)

ADVERTISEMENT marketplace

▶ [FREE CDRW Upgrade at Dell!](#)

Free CD-Burner Upgrade with purchase of select new Dell Home System. Offer ends 2/25. Click for details.

▶ [Does your company copy software illegally?](#)

Illegal copying is software piracy and it's against the law. Report Software Piracy Today.

▶ [Support Customers Remotely with Secure CRM Tool](#)

GoToAssist (formerly DesktopStreaming) is a secure e-support solution that enables you to deliver help desk support to your remote customers or employees via shared screen, mouse and keyboard control. Access their desktop in just seconds - even over dial-up!

▶ [All-in-one Enterprise Firewall Software ? Free Trial](#)

Astaro Security Linux, six applications in one software package including firewall, IPSec-based VPN, WiFi security, spam protection, surf control and virus control is available for a free 30-day trial.

▶ [RemotelyAnywhere 5.2: Reseller Opportunities](#)

RemotelyAnywhere 5.2 is the secure remote network admin solution for IT professionals. If your company sells and/or recommends Windows-based network products, click above to begin offering your clients RemotelyAnywhere's powerful network admin tools.

[Get your product or service listed here.](#)

ADVERTISEMENT intel showcase

▶ [Shop Now! - Dell Home Solutions Center](#)

▶ [Build your custom desktop or notebook now at MPC!](#)

sponsors

▶ [FREE Double Memory on Select Systems!](#)

▶ [Get Free Shipping on all products at FujitsuPC.com](#)

▶ [Spend \\$200 at Best Buy & get \\$20 off your next purchase](#)

▶ [Save 25% on Kingston Memory for Dell and Gateway PCs! Plus Free Shipping! Shop.kingston.com](#)

▶ [BestBuy.com, free shipping on everything.](#)

▶ [Automate disk maintenance with NEW Diskeeper 8.0 - free trial](#)

▶ [Configure an Award-Winning ABS PC or Notebook For Less](#)

▶ [Go wireless and find your freedom at Best Buy.](#)

PC MAGAZINE

[Issue Index](#) | [Contact Us](#) | [About](#) | [Advertise](#) | [Ad Index](#) | [Magazine Customer Service](#)

ZIFF DAVIS MEDIA

[Home](#) | [Contact Us](#) | [Advertise](#) | [Magazine Subscriptions](#) | [Newsletters](#) | [RSS Feeds](#) | [Tech Shop](#)
[White Papers](#) | [Tech Courses Online](#) | [Headlines for Your Site](#) | [Custom Utilities](#)

[1UP](#) | [Baseline](#) | [Business 4Site](#) | [CIO Insight](#) | [Computer Gaming World](#) | [DigitalLife](#) | [Electronic Gaming Monthly](#)
[eSeminars](#) | [eWEEK](#) | [ExtremeTech](#) | [Gaming Industry News](#) | [GMR](#) | [Microsoft Watch](#)
[Official US PlayStation Magazine](#) | [PC Magazine](#) | [Small Business Center](#) | [Ziff Davis Channel Zone](#)

Use of this site is governed by our [Terms of Use](#) and [Privacy Policy](#)

Copyright © 1996-2004 [Ziff Davis Media Inc.](#) All Rights Reserved. PC Magazine is a registered trademark of Ziff Davis Publishing Holdings Inc. Reproduction in whole or in part in any form or medium without express written permission of Ziff Davis Media Inc. is prohibited. For reprint information: [click here](#).

[Home](#) > [News and Analysis](#) > [Special Reports](#) > [Security Watch](#) > [SW Newsletter](#) > **Dumaru.Y—Very New and Very Dangerous**

Dumaru.Y—Very New and Very Dangerous

 Print  Email  Save  Discuss  Subscribe

Top Threat: W32/Dumaru.Y-mm

Unlike last week's hot pistol, Bagle.A, which made a lot of noise, but was shooting blanks, this week's top threat, W32/Dumaru.Y-mm is the real McCoy. The virus was discovered on January 23rd and 24th (depending on source), and according to MessageLabs tracking, is most active in the US, Canada and the UK. Dumaru.Y is a mass mailing worm/virus that installs a keylogger, harvests e-mail addresses from a victim's machine, and e-mails personal information out along with keystroke and clipboard data. It is also known as Dumaru.Y ([Panda](#)), I-worm.dumaru.J ([Kaspersky](#)), and W32/dumaru.Y@mm ([Symantec](#), [McAfee](#)).

RELATED LINKS

[Breaking Virus News: MyDoom Hobbles Internet E-mail](#)

According to analysis by Symantec, Panda and McAfee, Dumaru.Y spreads via an infected email attachment from "Elene" F***ENSUICIDE@HOTMAIL.COM , with a subject line "Important information for you. Read it immediately !". The attachment is a zip file called myphoto.zip, that contains the executable virus in a file called

"myphoto.jpg.exe"

. Note that there are 56 spaces between the JPG and the .EXE, to mask its true file type. When the file is viewed in WinZip or another archive program, only myphoto.jpg is visible, unless the user scrolls to the end of the line. When the user tries to open the file, the virus infects the machine. When Dumaru.Y is executed, it makes copies of itself in the %windir% and %system% folders (where %windir% is "C:\Windows" or "C:\Winnt", and %system% is C:\windows\system, C:\windows\system32, or C:\winnt\system32, depending on OS). The files created are:

table of contents

- [Introduction](#)
- **Top Threat**
- [Security Tip](#)
- [Top 10 E-Mail Viruses](#)
- [Top 5 Vulnerabilities](#)
- [Microsoft Security Updates](#)
- [Jargon Buster](#)
- [Security Watch Story Feed](#)

- news
- [MyDoom.F-mm Starting Slow, But Has Scary Potential](#)
 - [This Worm Only Wants to Heal](#)
 - [A Front Row Seat to a Major Attack](#)
 - [MyDoom.A: Fastest Spreading Virus in History](#)
 - [Dumaru.Y—Very New and Very Dangerous](#)
- [View All >](#)

new white papers

ADVERTISEMENT



BRING OUR LESSONS TO YOUR BUSINESS

CHECK OUT BASELINE TOOLS:

TUTORIALS
PLANNERS
QUIZZES
CALCULATORS
PRIMERS
AND MORE!

%WinDir%\RUNDLLX.SYS
%SysDir%\L32X.EXE
%SysDir%\VXD32V.EXE

According to McAfee, Dumar.Y also creates a copy in the windows Startup folder:

c:\Documents and Settings\user\Start Menu\Programs\Startup\dlxw.exe

McAfee also notes that the following registry entries are created or modified to automatically start the virus when the victim's system is started:

For Windows 9x and NT, the following is created:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Run "load32" = %SysDir%\L32X.EXE

For Windows NT and 2000 systems, the following value is modified:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Winlogon "Shell"
from:
Explorer.exe
to:
explorer.exe %SysDir%\VXD32V.EXE

Dumar.Y also modifies the Win.INI and System.INI files

The WIN.INI key:
[windows]
"run" = %WinDir%\RUNDLLX.SYS

The SYSTEM.INI key:

[boot]
"shell" = Explorer.exe is modified to: "shell" = explorer.exe %SysDir%\VXD32V.EXE

According to Symantec, Dumar.Y may also create the registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\SARS

Once Dumar.Y is running, it will harvest e-mail addresses from the victim's Windows address book (WAB), HTML, HTM, dbx, tbb, and abd files. The antivirus vendors were still analyzing the worm at press time, but it appears to create a copy of itself in the file %windir%\TEMP\zip.tmp. Dumar.Y then uses its own SMTP engine to send the zip file to the harvested addresses.

While a full analysis is not completed, Dumar.Y will attempt to terminate antivirus and firewall processes, and may open a backdoor server on TCP port 10000. It also may e-mail personal information that

 [Want to Let Customers Know Your Website is Safe?](#)

 [Looking for mission-critical server security?](#)

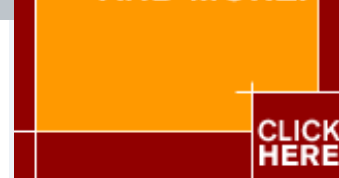
 [Protect Your Network from Corporate E-mail Threats](#)

[All White Papers >](#)

ADVERTISEMENT

Partner Services:

- ▶ [Dell Business Systems](#)
- ▶ [Dell Home Systems](#)
- ▶ [MPC \(MicronPC\)](#)



CLICK HERE

FREE CD-Burner Upgrade with purchase of select new Dell Home Systems.
Offer expires 2/25.

DELL ▶ **CLICK HERE**

FREE SUBSCRIPTION

eWEEK
THE ENTERPRISE NEWSWEEKLY

CLICK HERE ▶ APPLY

PROD BY
CIO INSIGHT

@ Ziff Davis CIO Insight

Click Here

includes the logged keystrokes and clipboard data to an internally stored source.

Fact File

Virus name: W32/Dumaru.Y-mm, W32/Dumaru.J@mm, W32/Dumaru.Y@mm, I-Worm.Dumaru.Y, W32/Dumaru.Y

Type: Windows 32bit virus/worm

Systems affected: Windows 9x, NT, 2000, XP, 2003

Systems not affected: DOS, Windows 3.x, ME, Linux, Mac

Infection vector: Infected attachment via email

From Field: "Elene" F***ENSUICIDE@HOTMAIL.COM

Subject: Important information for you. Read it immediately !

Message:

Hi !

Here is my photo, that you asked for yesterday.

Attachment: myphoto.zip (contains a file myphoto.jpg.exe with 56 spaces between the jpg and the.exe)

Removing W32/Dumaru.Y-mm

The easiest way to remove Dumaru is to update your antivirus program, if the process has not been stopped. As of 1/24, most vendors have added at least beta detection and deletion to their pattern definition updates. By our publication time, most should have finished updates. If your antivirus software has been disabled, or you don't have one, you may try McAfee's [FreeScan](#) , or TrendMicro's [Housecall](#).

Manually removing W32/Dumaru.Y-mm

Manually removing Dumaru.Y requires editing the registry and INI file as outlined in the following steps.

Step 1. Disable System Restore if you're using Windows Me/XP. When you make changes to your system, Windows does a restoration checkpoint. If it does this while the system is infected, it may come back to re-infect later. For [Windows XP](#) or [Windows ME](#).

Step 2. Restart the computer in Safe Mode (or VGA mode on Windows NT). Since Dumaru creates running processes, and Windows doesn't allow you to delete files connected with running processes, restarting is necessary. Using Safe mode prevents Windows from loading drivers and autorun entries so your system boots relatively clean.

Step 3. Run a full system scan with an updated Antivirus scanner. If your scanner does not remove everything, follow the next few steps.

Step 4. Your antivirus software should, during detection, produce a list of files associated with the W32.Dumaru.Y virus. Delete all these files. The files will typically be the ones mentioned in the description above.

Step 5. Make a backup of the registry before you edit. (Windows 95/98/ME [here](#) , Windows XP/2000/2003 go [here](#). Delete the entries associated with Dumar.Y from the registry as listed above. Delete any entries flagged by your antivirus program.

Step 6. If the system is running Windows 95/98, you need to delete the entries from the System.INI files. You can do this either by going to Start/Run and typing msconfig and pressing enter, or typing "edit c:\windows\system.ini. Msconfig will have a tab for each file, click on system.ini. In the editor, look for the [boot] entry, and find the line:
shell = Explorer.exe C:\WINDOWS\SYSTEM\vx32v.exe
If the line exists, delete everything to the right of Explorer.exe, so when you're done, it looks like "shell = Explorer.exe"

Step 7. Re-enable System Restore (Windows ME, XP), reboot machine.

[< back](#)

[next >](#)

ZIFF DAVIS FEATURED SITES: [IT Reseller News & Resources](#)

▶▶▶ IN PRINT



FREE BONUS

Get our 3-Volume Software SuperPac loaded with utilities software, desktop customizers, games and more!

SUBSCRIPTION SERVICES

- + [Get Help with your Subscription](#)
- + [Renew - Give a Gift](#)
- + [Our New Digital Format](#)

SUBSCRIBE NOW & RECEIVE A **FREE** 3-VOLUME SOFTWARE SUPERPAC!

Name

Email (e.g. user@jsp.com)

Address

City

State

Postal Code

Click "Continue" to proceed to our secure server.

newsletters

Get PCMag.com's **FREE** email newsletters delivered to your inbox.

Its easy, just follow the steps.

Want more? Check out our other newsletters [here](#).

Manage your newsletter subscriptions [here](#).

1. Make your selections:

Inside PCMag.com

Internet Business Technology

Productwire: First Looks Update

Tip of the Day

PC Magazine's TrendWatch

Utility Library Update

Security Watch

Shareware Update

2. Select email format:

3. Enter email address:



FREE ONLINE SEMINARS FOR EXECUTIVES AND IT PROFESSIONALS

- [2/03 - Special Edition Sun Net Talk Secure and Affordable: Sun's Java™ Desktop System in Action](#) with Michael Krieger. *Sponsored by Sun Microsystems, Inc.*
- [2/05 - Beyond Voice Mail: Reducing Business Costs With Latest Generation of Unified Communications Applications](#) with Frank Derfler. *Sponsored by AVST.*
- [2/18 - Instant Messaging: The Gateway to the Real-Time Enterprise](#) with Jim Louderback. *Sponsored by Yahoo.*

FREE Online Seminars presented by **Intel**

- [PC Refresh: Your Strategy for Success!](#)
- [Server Consolidation-Expand Your Options](#)
- [Wireless LAN: One Size Doesn't Fit All](#)
- [PC Fleet Management: Tools & Strategies](#)

[view more eSeminars >>](#)

SHAREWARE.PCMAG.COM - HOT FILES

Download the best in free trial software from the [PCMag.com Shareware Library](#). Recent hot files:

- [SeeknClean](#) Cleans junk off your hard disk super fast!
- [Girder](#) Great tool for automating Windows.
- [DiskSpace Explorer Home Edition](#) Manage your hard disk space, find and delete useless items.
- [My Stuff](#) Home and personal inventory manager.
- [CyberScrub](#) CyberScrub removes all traces of online activity.

More [files at the Shareware Library >>](#)

NEW FROM ZIFF DAVIS E-LEARNING

Gain new IT and programming skills, prepare for accreditation, and more with online courses from [Ziff Davis eLearning](#).

- **New! Microsoft® Office® Skill Builders:** [Office XP](#), [Access](#), [Powerpoint](#), [Excel](#), [Word](#)
- **Development and IT:** [Java](#), [Adobe](#), [E-Business](#), [Linux](#), [Macromedia](#), [Macromedia Web Professional](#), [Oracle 8i](#), [Project Management](#), [SQL Server](#), [Visual Basic](#)
- **Certification Prep:** [A+](#), [Certified Novell Engineer](#), [iNET+](#), [MCSA](#), [MCSE](#), [Network+](#), [Security](#), [Server+](#)

See [all courses at Ziff Davis eLearning >>](#)

ADVERTISEMENT marketplace

▶ [FREE CDRW Upgrade at Dell!](#)

Free CD-Burner Upgrade with purchase of select new Dell Home System. Offer ends 2/25. Click for details.

▶ [Does your company copy software illegally?](#)

Illegal copying is software piracy and it's against the law. Report Software Piracy Today.

▶ [Support Customers Remotely with Secure CRM Tool](#)

GoToAssist (formerly DesktopStreaming) is a secure e-support solution that enables you to deliver help desk support to your remote customers or employees via shared screen, mouse and keyboard control. Access their desktop in just seconds - even over dial-up!

▶ [All-in-one Enterprise Firewall Software ? Free Trial](#)

Astaro Security Linux, six applications in one software package including firewall, IPSec-based VPN, WiFi security, spam protection, surf control and virus control is available for a free 30-day trial.

▶ [RemotelyAnywhere 5.2: Reseller Opportunities](#)

RemotelyAnywhere 5.2 is the secure remote network admin solution for IT professionals. If your company sells and/or recommends Windows-based network products, click above to begin offering your clients RemotelyAnywhere's powerful network admin tools.

[Get your product or service listed here.](#)

ADVERTISEMENT intel showcase

▶ [Shop Now! - Dell Home Solutions Center](#)

▶ [Build your custom desktop or notebook now at MPC!](#)

sponsors

▶ [FREE Double Memory on Select Systems!](#)

▶ [Get Free Shipping on all products at Fujitsupc.com](#)

▶ [Spend \\$200 at Best Buy & get \\$20 off your next purchase](#)

▶ [Save 25% on Kingston Memory for Dell and Gateway PCs! Plus Free Shipping! Shop.kingston.com](#)

▶ [BestBuy.com, free shipping on everything.](#)

▶ [Automate disk maintenance with NEW Diskeeper 8.0 - free trial](#)

▶ [Configure an Award-Winning ABS PC or Notebook For Less](#)

▶ [Go wireless and find your freedom at Best Buy.](#)

ZIFF DAVIS MEDIA [Home](#) | [Contact Us](#) | [Advertise](#) | [Magazine Subscriptions](#) | [Newsletters](#) | [RSS Feeds](#) | [Tech Shop](#)
[White Papers](#) | [Tech Courses Online](#) | [Headlines for Your Site](#) | [Custom Utilities](#)

[1UP](#) | [Baseline](#) | [Business 4Site](#) | [CIO Insight](#) | [Computer Gaming World](#) | [DigitalLife](#) | [Electronic Gaming Monthly](#)
[eSeminars](#) | [eWEEK](#) | [ExtremeTech](#) | [Gaming Industry News](#) | [GMR](#) | [Microsoft Watch](#)
[Official US PlayStation Magazine](#) | [PC Magazine](#) | [Small Business Center](#) | [Ziff Davis Channel Zone](#)

Use of this site is governed by our [Terms of Use](#) and [Privacy Policy](#)

Copyright © 1996-2004 **Ziff Davis Media Inc.** All Rights Reserved. PC Magazine is a registered trademark of Ziff Davis Publishing Holdings Inc. Reproduction in whole or in part in any form or medium without express written permission of Ziff Davis Media Inc. is prohibited. For reprint information: [click here](#).



ADVERTISEMENT

Easy as **DELL**

Up to \$800 total savings including a FREE CD-Burner Upgrade with online purchase of select new Dell Home PCs. Offers expire 2/25.

▶ [Click for Details](#)

[Home](#) > [News and Analysis](#) > [Special Reports](#) > [Security Watch](#) > [SW Newsletter](#) > **Dumaru.Y—Very New and Very Dangerous**

Dumaru.Y—Very New and Very Dangerous

Print Email Save Discuss Subscribe

Security Tip: Playing it safe on eBay and other auctions

Millions of users log on to eBay every day to buy and sell. It's fun, it's exciting, and it's rife with fraud. Knowing how to buy and sell carefully can save you money and aggravation.

RELATED LINKS

- ▶ [Breaking Virus News: MyDoom Hobbles Internet E-mail](#)

For buyers, check the seller's feedback and location. Do they have any negative feedback? This isn't always bad, since things happen, but see what they were selling at the time, and where. A vendor could have 1,000 positive feedback points for selling \$2 knick knacks, but a couple

\$500 stereo systems they sold never arrived. Be wary of a new seller. Everyone has to start somewhere, but someone with 0 feedback points selling a 1955 double struck penny for half its value may not be the most reliable source.

Never send cash, or wire money with Western Union, as they are basically untraceable. Many sellers ask for Money orders only, which are difficult to trace or get refunds. If your seller is reputable, there is no problem. Be very careful dealing with international sales and escrow services. An escrow service is supposedly a middleman for a transaction. You sent them the money, they tell the seller the money's there, and to ship the item. You then tell the escrow service you got the item, and they release the money to seller. Simple, safe? Not necessarily. A current scam is where the seller sets up a bogus escrow service and asks you wire the money using Western Union, or another service. They then take the money and skip. By the time you realize there's a problem, they're long gone. The scams are usually on big-ticket items that would commonly be escrowed.

[< back](#)[next >](#)

table of contents

- [Introduction](#)
- [Top Threat](#)
- [Security Tip](#)
- [Top 10 E-Mail Viruses](#)
- [Top 5 Vulnerabilities](#)
- [Microsoft Security Updates](#)
- [Jargon Buster](#)
- [Security Watch Story Feed](#)

news

- [MyDoom.F-mm Starting Slow, But Has Scary Potential](#)
- [This Worm Only Wants to Heal](#)
- [A Front Row Seat to a Major Attack](#)
- [MyDoom.A: Fastest Spreading Virus in History](#)
- [Dumaru.Y—Very New and Very Dangerous](#)

[View All >](#)

new white papers

- [Want to Let Customers Know Your Website is Safe?](#)
 - [Looking for mission-critical server security?](#)
 - [Protect Your Network from Corporate E-mail Threats](#)
- [All White Papers >](#)

ADVERTISEMENT

Baseline
THE PROJECT MANAGEMENT CENTER**COMPUTER NETWORKS SECURITY XML DATABASES AND MORE****CHECK OUT****PRIMERS @ BASELINE****CLICK HERE**

FREE CD-Burner Upgrade with purchase of select new Dell Home Systems.

Offer expires 2/25.

DELL▶ [CLICK HERE](#)

ADVERTISEMENT

Partner Services:

ZIFF DAVIS FEATURED SITES: [IT Reseller News & Resources](#)

▶▶▶ IN PRINT



SAVE
UP TO
77%

SUBSCRIBE NOW & RECEIVE A **FREE**
3-VOLUME SOFTWARE SUPERPAC!

Name

Email (e.g. user@jsp.com)

Address

City

State

Postal Code

FREE BONUS

Get our 3-Volume Software SuperPac loaded with utilities software, desktop customizers, games and more!

SUBSCRIPTION SERVICES

- + [Get Help with your Subscription](#)
- + [Renew - Give a Gift](#)
- + [Our New Digital Format](#)

Click "Continue"
to proceed to our
secure server.

newsletters

Get PCMag.com's **FREE** email newsletters delivered to your inbox.

It's easy, just follow the steps.

Want more? Check out our other newsletters [here](#).

Manage your newsletter subscriptions [here](#).

1. Make your selections: 2. Select email format:

- Inside PCMag.com
- Internet Business Technology
- Productwire: First Looks Update
- Tip of the Day
- PC Magazine's TrendWatch
- Utility Library Update
- Security Watch
- Shareware Update

3. Enter email address:



FREE ONLINE SEMINARS FOR EXECUTIVES AND IT PROFESSIONALS

- [2/03 - Special Edition Sun Net Talk Secure and Affordable: Sun's Java™ Desktop System in Action](#) with Michael Krieger. *Sponsored by Sun Microsystems, Inc.*
- [2/05 - Beyond Voice Mail: Reducing Business Costs With Latest Generation of Unified Communications Applications](#) with Frank Derfler. *Sponsored by AVST.*
- [2/18 - Instant Messaging: The Gateway to the Real-Time Enterprise](#) with Jim Louderback. *Sponsored by Yahoo.*

FREE Online Seminars
presented by **Intel**

- [PC Refresh: Your Strategy for Success!](#)
- [Server Consolidation-Expand Your Options](#)
- [Wireless LAN: One Size Doesn't Fit All](#)
- [PC Fleet Management: Tools & Strategies](#)

[view more eSeminars >>](#)

- ▶ [Dell Business Systems](#)
- ▶ [Dell Home Systems](#)
- ▶ [MPC \(MicronPC\)](#)

Baseline
THE PROJECT MANAGEMENT CENTER

@ BASELINE
CLICK
HERE

2WEEK APPLY NOW
**GET A FREE
SUBSCRIPTION**

SHAREWARE.PCMAG.COM - HOT FILES

Download the best in free trial software from the [PCMag.com Shareware Library](#). Recent hot files:

- [SeeknClean](#) Cleans junk off your hard disk super fast!
- [Girder](#) Great tool for automating Windows.
- [DiskSpace Explorer Home Edition](#) Manage your hard disk space, find and delete useless items.
- [My Stuff](#) Home and personal inventory manager.
- [CyberScrub](#) CyberScrub removes all traces of online activity.

More [files at the Shareware Library >>](#)

NEW FROM ZIFF DAVIS E-LEARNING

Gain new IT and programming skills, prepare for accreditation, and more with online courses from [Ziff Davis eLearning](#).

- **New! Microsoft® Office® Skill Builders:** [Office XP](#), [Access](#), [Powerpoint](#), [Excel](#), [Word](#)
- **Development and IT:** [Java](#), [Adobe](#), [E-Business](#), [Linux](#), [Macromedia](#), [Macromedia Web Professional](#), [Oracle 8i](#), [Project Management](#), [SQL Server](#), [Visual Basic](#)
- **Certification Prep:** [A+](#), [Certified Novell Engineer](#), [iNET+](#), [MCSA](#), [MCSE](#), [Network+](#), [Security](#), [Server+](#)

See [all courses at Ziff Davis eLearning >>](#)

ADVERTISEMENT marketplace

▶ [FREE CDRW Upgrade at Dell!](#)

Free CD-Burner Upgrade with purchase of select new Dell Home System. Offer ends 2/25. Click for details.

▶ [Does your company copy software illegally?](#)

Illegal copying is software piracy and it's against the law. Report Software Piracy Today.

▶ [Support Customers Remotely with Secure CRM Tool](#)

GoToAssist (formerly DesktopStreaming) is a secure e-support solution that enables you to deliver help desk support to your remote customers or employees via shared screen, mouse and keyboard control. Access their desktop in just seconds - even over dial-up!

▶ [All-in-one Enterprise Firewall Software ? Free Trial](#)

Astaro Security Linux, six applications in one software package including firewall, IPSec-based VPN, WiFi security, spam protection, surf control and virus control is available for a free 30-day trial.

▶ [RemotelyAnywhere 5.2: Reseller Opportunities](#)

RemotelyAnywhere 5.2 is the secure remote network admin solution for IT professionals. If your company sells and/or recommends Windows-based network products, click above to begin offering your clients RemotelyAnywhere's powerful network admin tools.

[Get your product or service listed here.](#)

ADVERTISEMENT intel showcase

▶ [Shop Now! - Dell Home Solutions Center](#)

▶ [Build your custom desktop or notebook now at MPC!](#)

sponsors

- ▶ [FREE Double Memory on Select Systems!](#)
- ▶ [Get Free Shipping on all products at Fujitsupc.com](#)
- ▶ [Spend \\$200 at Best Buy & get \\$20 off your next purchase](#)
- ▶ [Save 25% on Kingston Memory for Dell and Gateway PCs! Plus Free Shipping! Shop.kingston.com](#)
- ▶ [BestBuy.com, free shipping on everything.](#)
- ▶ [Automate disk maintenance with NEW Diskeeper 8.0 - free trial](#)
- ▶ [Configure an Award-Winning ABS PC or Notebook For Less](#)
- ▶ [Go wireless and find your freedom at Best Buy.](#)

PC MAGAZINE

[Issue Index](#) | [Contact Us](#) | [About](#) | [Advertise](#) | [Ad Index](#) | [Magazine Customer Service](#)

ZIFF DAVIS MEDIA

[Home](#) | [Contact Us](#) | [Advertise](#) | [Magazine Subscriptions](#) | [Newsletters](#) | [RSS Feeds](#) | [Tech Shop](#)
[White Papers](#) | [Tech Courses Online](#) | [Headlines for Your Site](#) | [Custom Utilities](#)

[1UP](#) | [Baseline](#) | [Business 4Site](#) | [CIO Insight](#) | [Computer Gaming World](#) | [DigitalLife](#) | [Electronic Gaming Monthly](#)
[eSeminars](#) | [eWEEK](#) | [ExtremeTech](#) | [Gaming Industry News](#) | [GMR](#) | [Microsoft Watch](#)
[Official US PlayStation Magazine](#) | [PC Magazine](#) | [Small Business Center](#) | [Ziff Davis Channel Zone](#)

Use of this site is governed by our [Terms of Use](#) and [Privacy Policy](#)

Copyright © 1996-2004 **Ziff Davis Media Inc.** All Rights Reserved. PC Magazine is a registered trademark of Ziff Davis Publishing Holdings Inc. Reproduction in whole or in part in any form or medium without express written permission of Ziff Davis Media Inc. is prohibited. For reprint information: [click here](#).

ADVERTISEMENT

Easy as **DELL**

FREE Memory Upgrade with purchase of select new Dell Home Systems.
Offer expires 2/25.

► [Click for Details](#)



[Home](#) > [News and Analysis](#) > [Special Reports](#) > [Security Watch](#) > [SW Newsletter](#) > **Dumaru.Y—Very New and Very Dangerous**

Dumaru.Y—Very New and Very Dangerous

 Print  Email  Save  Discuss  Subscribe

Top 10 E-Mail Viruses as Reported by [MessageLabs](#)

These are the latest threats as of Monday January 26, 2004 as listed by MessageLabs:

1. [W32 / Dumaru.A-mm](#)
2. [W32 / Sobig.F-mm](#)
3. [W32 / Sober.C-mm](#)
4. [W32 / Swen.A-mm](#)
5. [W32 / Klez.H-mm](#)
6. [W32 / Mmail.J-mm](#)
7. [W32 / Dumaru.Y-mm](#)
8. [W32 / Mmail.A-mm](#)
9. [W32 / Yaha.P-mm](#)
10. [W32 / Mmail.I-mm](#)

► RELATED LINKS

- [Breaking Virus News:](#)
- [MyDoom Hobbles](#)
- [Internet E-mail](#)

For MessageLabs's complete list of email viruses, [click here](#).

[< back](#)

[next >](#)

table of contents

- [Introduction](#)
- [Top Threat](#)
- [Security Tip](#)
- **Top 10 E-Mail Viruses**
- [Top 5 Vulnerabilities](#)
- [Microsoft Security Updates](#)
- [Jargon Buster](#)
- [Security Watch Story Feed](#)

news

[MyDoom.F-mm Starting Slow, But Has Scary Potential](#)

[This Worm Only Wants to Heal](#)

[A Front Row Seat to a Major Attack](#)

[MyDoom.A: Fastest Spreading Virus in History](#)

[Dumaru.Y—Very New and Very Dangerous](#)

[View All >](#)

new white papers

-  [Want to Let Customers Know Your Website is Safe?](#)
 -  [Looking for mission-critical server security?](#)
 -  [Protect Your Network from Corporate E-mail Threats](#)
- [All White Papers >](#)

ADVERTISEMENT

Baseline
THE PROJECT MANAGEMENT CENTER

BRING OUR LESSONS TO YOUR BUSINESS

CHECK OUT BASELINE TOOLS:

TUTORIALS
PLANNERS
QUIZZES
CALCULATORS
PRIMERS
AND MORE!

CLICK HERE

FREE CD-Burner Upgrade with purchase of select new Dell Home Systems.
Offer expires 2/25.

DELL

► [CLICK HERE](#)

ADVERTISEMENT
Partner Services:

ZIFF DAVIS FEATURED SITES: [IT Reseller News & Resources](#)

▶▶▶ IN PRINT



SAVE
UP TO
77%

SUBSCRIBE NOW & RECEIVE A **FREE** 3-VOLUME SOFTWARE SUPERPAC!

Name

Email (e.g. user@jsp.com)

Address

City

State

Postal Code

FREE BONUS

Get our 3-Volume Software SuperPac loaded with utilities software, desktop customizers, games and more!

SUBSCRIPTION SERVICES

- + [Get Help with your Subscription](#)
- + [Renew - Give a Gift](#)
- + [Our New Digital Format](#)

Click "Continue"
to proceed to our
secure server.

newsletters

Get PCMag.com's **FREE** email newsletters delivered to your inbox.

It's easy, just follow the steps.

Want more? Check out our other newsletters [here](#).

Manage your newsletter subscriptions [here](#).

1. Make your selections: 2. Select email format:

- Inside PCMag.com
- Internet Business Technology
- Productwire: First Looks Update
- Tip of the Day
- PC Magazine's TrendWatch
- Utility Library Update
- Security Watch
- Shareware Update

3. Enter email address:



FREE ONLINE SEMINARS FOR EXECUTIVES AND IT PROFESSIONALS

- **2/18 - Instant Messaging: The Gateway to the Real-Time Enterprise** with Jim Louderback. *Sponsored by Yahoo! Business Messenger.*
- **2/24 - Integrating People, Processes and Technology for Service Management Success** with Frank Derfler. *Sponsored by FrontRange Solutions.*
- **2/25 - I Want My Linux Desktop-- Right Now!** with Jim Louderback. *Sponsored by Wyse Technology.*

FREE Online Seminars
presented by **Intel**

- [PC Refresh: Your Strategy for Success!](#)
- [Server Consolidation-Expand Your Options](#)
- [Wireless LAN: One Size Doesn't Fit All](#)
- [PC Fleet Management: Tools & Strategies](#)

[view more eSeminars >>](#)

- ▶ [Dell Business Systems](#)
- ▶ [Dell Home Systems](#)
- ▶ [MPC \(MicronPC\)](#)

WEEK **APPLY NOW**
**GET A FREE
SUBSCRIPTION**

Baseline
THE PROJECT MANAGEMENT CENTER
@ BASELINE **CLICK
HERE**

SHAREWARE.PCMAG.COM - HOT FILES

Download the best in free trial software from the [PCMag.com Shareware Library](#). Recent hot files:

- [SeeknClean](#) Cleans junk off your hard disk super fast!
- [Girder](#) Great tool for automating Windows.
- [DiskSpace Explorer Home Edition](#) Manage your hard disk space, find and delete useless items.
- [My Stuff](#) Home and personal inventory manager.
- [CyberScrub](#) CyberScrub removes all traces of online activity.

More [files at the Shareware Library >>](#)

NEW FROM ZIFF DAVIS E-LEARNING

Gain new IT and programming skills, prepare for accreditation, and more with online courses from [Ziff Davis eLearning](#).

- **New! Microsoft® Office® Skill Builders:** [Office XP](#), [Access](#), [Powerpoint](#), [Excel](#), [Word](#)
- **Development and IT:** [Java](#), [Adobe](#), [E-Business](#), [Linux](#), [Macromedia](#), [Macromedia Web Professional](#), [Oracle 8i](#), [Project Management](#), [SQL Server](#), [Visual Basic](#)
- **Certification Prep:** [A+](#), [Certified Novell Engineer](#), [iNET+](#), [MCSA](#), [MCSE](#), [Network+](#), [Security](#), [Server+](#)

See [all courses at Ziff Davis eLearning >>](#)

ADVERTISEMENT marketplace

▶ [FREE CDRW Upgrade at Dell!](#)

Free CD-Burner Upgrade with purchase of select new Dell Home System. Offer ends 2/25. Click for details.

▶ [Does your company copy software illegally?](#)

Illegal copying is software piracy and it's against the law. Report Software Piracy Today.

▶ [Support Customers Remotely with Secure CRM Tool](#)

GoToAssist (formerly DesktopStreaming) is a secure e-support solution that enables you to deliver help desk support to your remote customers or employees via shared screen, mouse and keyboard control. Access their desktop in just seconds - even over dial-up!

▶ [All-in-one Enterprise Firewall Software ? Free Trial](#)

Astaro Security Linux, six applications in one software package including firewall, IPSec-based VPN, WiFi security, spam protection, surf control and virus control is available for a free 30-day trial.

▶ [RemotelyAnywhere 5.2: Reseller Opportunities](#)

RemotelyAnywhere 5.2 is the secure remote network admin solution for IT professionals. If your company sells and/or recommends Windows-based network products, click above to begin offering your clients RemotelyAnywhere's powerful network admin tools.

[Get your product or service listed here.](#)

ADVERTISEMENT intel showcase

▶ [Shop Now! - Dell Home Solutions Center](#)

▶ [Build your custom desktop or notebook now at MPC!](#)

sponsors

- ▶ [Free 3-5 day Shipping w/ Dell Home PCs. Details.](#)
- ▶ [FREE Double Memory on Select Systems!](#)
- ▶ [Get Free Shipping on all products at Fujitsupc.com](#)
- ▶ [Spend \\$200 at Best Buy & get \\$20 off your next purchase](#)
- ▶ [Save 25% on Kingston Memory for Dell and Gateway PCs! Plus Free Shipping! Shop.kingston.com](#)
- ▶ [BestBuy.com, free shipping on everything.](#)
- ▶ [Automate disk maintenance with NEW Diskeeper 8.0 - free trial](#)
- ▶ [Configure an Award-Winning ABS PC or Notebook For Less](#)
- ▶ [Go wireless and find your freedom at Best Buy.](#)
- ▶ [New Microsoft® Office System Eval Kit](#)
- ▶ [Go wireless with the HP Business Notebook nc6000.](#)

PC MAGAZINE

[Issue Index](#) | [Contact Us](#) | [About](#) | [Advertise](#) | [Ad Index](#) | [Magazine Customer Service](#)

ZIFF DAVIS MEDIA

[Home](#) | [Contact Us](#) | [Advertise](#) | [Magazine Subscriptions](#) | [Newsletters](#) | [RSS Feeds](#) | [Tech Shop](#)
[White Papers](#) | [Tech Courses Online](#) | [Headlines for Your Site](#) | [Custom Utilities](#)

[1UP](#) | [Baseline](#) | [Business 4Site](#) | [CIO Insight](#) | [Computer Gaming World](#) | [DigitalLife](#) | [Electronic Gaming Monthly](#)
[eSeminars](#) | [eWEEK](#) | [ExtremeTech](#) | [Gaming Industry News](#) | [GMR](#) | [Microsoft Watch](#)
[Official US PlayStation Magazine](#) | [PC Magazine](#) | [Small Business Center](#) | [Ziff Davis Channel Zone](#)

Use of this site is governed by our [Terms of Use](#) and [Privacy Policy](#)

Copyright © 1996-2004 **Ziff Davis Media Inc.** All Rights Reserved. PC Magazine is a registered trademark of Ziff Davis Publishing Holdings Inc. Reproduction in whole or in part in any form or medium without express written permission of Ziff Davis Media Inc. is prohibited. For reprint information: [click here](#).