



News:

Search for:

in

[Full TargetSearch with Google](#)

No Cone of silence for this malcode

By Edward Hurley
25 Mar 2004 | [SearchSecurity.com](#)

SITE SPONSOR

EXPLORE THIS AREA: RICH MEDIA ADVERTISEMENT

Peer-to-peer networks have been a boon for people who like free music and software. But swappers may find themselves downloading a worm or virus instead of the latest version of some video game.

So far, there have been few pure peer-to-peer worms. More commonly, mass mailing worms also have a peer-to-peer component. Often, the worm spreads more via e-mail, thus obscuring the fact that it can also spread via peer-to-peer networks.

Cone-E, which surfaced this week, is such a worm. It spreads primarily via e-mail but when it infects systems the worm creates copies of itself with different file names. Those files, with names such as "401 guitar tabs.chm," "adult check passwords.chm" or "Credit card numbers.chm," can be accessed by users of the Kazaa peer-to-peer network.

Or earlier this month, mass mailer Bagle-Q looked for folders with "shar" in the name and then copied itself to it using a variety of enticing names. For example, it could appear as "Adobe Photoshop 9 full.exe," "Matrix 3 Revolution English Subtitles.exe" or "Windows Sourcecode update.doc.exe."

Convincing social engineering is needed for worms to spread via peer-to-peer networks because there are no known exploits that would allow the worm to execute automatically, said Patrick Hinojosa, chief technology officer at Panda Software. "The social engineering is needed to exploit the human vulnerability."

Protecting against peer-to-peer works isn't that difficult. Blocking the software in the first place is the surest bet. A properly configured firewall that only allows specifically approved services in and out would do the trick, Hinojosa said.

If a company wants or has to allow peer-to-peer exchanges, then memory-resident antivirus software should be installed on desktops. Such protection would mean any downloaded file is scanned before it's executed.

The danger posed by peer-to-peer sharing highlights the need for multiple layers of protection. For example, many companies have gateway scanners, which are helpful because they stop worms before they hit the network and therefore save bandwidth, said Carole Theriault, security consultant at Sophos. However, such scanners don't protect against worms that spread via peer-to-peer networks.

"Antivirus protection at the desktop is paramount," Theriault said. "Worms can travel by so many ways including instant messages, peer-to-peer networks and even downloads from Web sites."



RELEVANT SPONSORED LINKS

[Join the Kazaa Revolution](#)

Think P2P technology can change the world of entertainment? Act now!

www.kazaa.com/revolution/

[Free Music Downloads](#)

9 Billion Songs, No Download Fees!

All Favorite Artists, All Legal aff

www.mp3advance.com

[K-Lite 2004 - No Spyware](#)

80 Million Songs, Movies & Videos!

The Safe & Legal Version. aff

<http://klitetk.com/index.asp>

[Legal Music -30 Million](#)

Members legal aff, One time fee

No Download Fee No Monthly Fee

www.mp3advance.com

[Share Music Legally](#)

Upload files. Stream them to the world. Get your free trial today.

live365.com/broadcast/



EMAIL A FRIEND

[Send the article you've just read to a friend](#)

LATEST HEADLINES

- >> [Bug hunters go open source](#) (The Register)
- >> [Speech and security dominate in Gates' appearances](#) (SearchWin2000.com)
- >> [Hacker insurance may drop](#) (vnunet.com)
- >> [NIST publishes security drafts for mapping, encryption](#) (Federal Computer Weekly)
- >> [Computer virus damage shatters records](#) (The Globe and Mail)



WHAT'S NEW

on SearchSecurity

1. [Security Decisions in 3 weeks](#)
2. [Best of SearchSecurity.com - March 2004](#)
3. [Subscribe to Info Security Magazine](#)
4. [Attend Data Center Decisions June 2-4](#)

TechTarget
Security Media



[View this month's
issue and subscribe
today.](#)



[Apply online for free
conference admission.](#)



SECURITY MARKETPLACE

GET YOUR PRODUCT OR SERVICE LISTED HERE

Partner Links

[Get FREE Security Management Tools at microsoft.com/security/IT Training - Notifications - Guidance Kit - Tools](#)

[Join Mike Nash, Microsoft s VP of Security, for a live monthly Security Webcast. http://go.microsoft.com/fwlink/?LinkId=25281](#)

[Register now for a FREE Microsoft\(R\) Security Training Event near you](#)

[Make your big ideas even bigger. Download your FREE ASP.NET Resource Kit now. Visit: http://msdn.microsoft.com/asp.net/asprk/](#)

[Microsoft\(R\) Visual Studio\(R\) .NET makes our big ideas even bigger. Get your FREE Visual Basic .NET Resource Kit today.](#)

GET YOUR PRODUCT OR SERVICE LISTED HERE

SearchSecurity.com is part of the TechTarget network of industry-specific IT Web sites

APPLICATIONS

[SearchCRM.com](#)

[SearchSAP.com](#)

DEVELOPMENT

[SearchVB.com](#)

ENTERPRISE IT MANAGEMENT

[SearchCIO.com](#)

CORE TECHNOLOGIES

[SearchDatabase.com](#)

[SearchMobileComputing.com](#)

[SearchNetworking.com](#)

[SearchOracle.com](#)

[SearchSecurity.com](#)

[SearchStorage.com](#)

[SearchWebServices.com](#)

[WhatIs.com](#)

PLATFORMS

[Search390.com](#)

[Search400.com](#)

[SearchDomino.com](#)

[SearchEnterpriseLinux.com](#)

[SearchExchange.com](#)

[SearchWin2000.com](#)



[TechTarget Enterprise IT Conferences](#) | [TechTarget Corporate Web Site](#) | [Media Kit](#)

Explore [SearchTechTarget.com](#), the guide to the TechTarget network of industry-specific IT Web sites.

All Rights Reserved, [Copyright 2000 - 2004, TechTarget](#)

[Read our Privacy Statement](#)