



SECURITY News

RSS/XML Feeds::

- [Breaking News](#)
- [Security](#)
- [Entrepreneur's Corner](#)
- [More...](#)

SUBSCRIBE TO OUR eNEWSLETTERS:

[Quick Register](#)

SEARCH PREVIOUS ARTICLES

SPONSORS:



- Home
- About Us
- Contact Us
- The Glance
- Tech Jobs
- Media Kit
- Great Lakes Financial News
- From PR Newswire
- eNewsletter Signup

- Alternative Energy
- Ann Arbor IT Zone
- Breaking News
- Entrepreneur's Corner
- GLIMA/Automation Alley
- Going Global
- Guest Columns
- New Products/Contracts
- Podcast
- Security
- Small Business Association of Michigan



Friday, June 01, 2007

New Worm Spreads Via eMail, Web, Network Shares, Software Vulnerability

SOUTHFIELD – A new email security threat contains the Cheburgen.a worm, which, if activated opens certain ports that connect to IRC channels and takes orders from remote attackers.

The email worm contains the following words:

Here is your documents

Mail Delivery System

Mail Transaction Failed

Re: Thank you for delivery

The Worm is written in VC++ language. The name of the attachment is randomly picked from a list that contains words like Data, Body, Doc and Text. The file extension again is a random choice from bat, cmd, exe, scr, pif and zip. The malware comes with its own SMTP engine and sends copies to email addresses harvested from the Windows Address Book of the compromised computer. It modifies the Windows HOSTS files to stop computers from accessing websites of some security companies. "Cheburgen is also distributed by other Trojans as well as using Drive-by-Download route when someone visits a malicious website," says Manoj Mansukhani, Head – Technology and Marketing, MicroWorld Technologies. "As if that's not trouble enough, it scans other PCs in the network and drops the malware in shared folders. And finally, the Worm is also found to be spreading by exploiting the 'LSASS vulnerability' in Windows."

The Malware displays its Backdoor capabilities when it opens certain ports, connects to IRC channels and takes orders from the remote attacker. The attacker can direct the malware to download and execute files from the Internet by working through this Backdoor component.

"This one has taken the term 'Blended Threat' real far that it adopts something or the other from a variety of malware breeds," points out Govind Rammurthy, CEO of MicroWorld Technologies.

"People behind this malicious program simply believe that the more is merrier and tries to fire on as many cylinders as possible in their attempt to proliferate it. If you want to protect your computers against a threat like this, it is imperative that you rely on a Security Software that checks all the modes of its spreading



Alliance Offices
Shanghai
Beijing

BUTZEL LONG
www.butzel.com



Content Partners:

[Automation Alley](#)
[SBAM](#)

[Detroit Regional Chamber](#)

[MITechNews Podcasts](#)

[GLIMANetwork](#)

[Telematics Update](#)

[Gongwer News](#)

[The Car Connection](#)

[Midwest Tech Leaders](#)

[Ann Arbor IT Zone](#)

[MI-SBTDC](#)

[SBAM](#)

[MI Venture Capital](#)

[Great Lakes Angels](#)

[Michigan Small Tech Assoc.](#)

[Ann Arbor Angels](#)

[GL Entrepreneurs Quest](#)

[Motor City ISSA](#)

[Michigan InfraGard](#)

[CreateDetroit](#)

[EMU CERNS](#)

[MichBio](#)

[MI Manufacturers Assoc](#)

[MISurvives](#)

[Walsh College IAC](#)

[HDI Motor City](#)

Advertisers:



routine," he said.

Author: Staff Writer
Source: MITechNews.Com

[<< Previous Article](#)

[Printer Friendly](#)

[Next Article>>](#)



IN BUSINESS,
IT'S NOT WHO
YOU KNOW.
IT'S WHO, WHO
AND WHO...



[CLICK TO LEARN MORE.](#)



Member FDIC



Interested in
advertising in
this
eNewsletter?

Click here for
more
information



IDENTITY THEFT

Identity Theft Shield

Click **HERE** FOR MORE INFO!

ISERV
technology group

Mergers.
Acquisitions.
Operations.

Seeking quality technology acquisitions.

PIXELBIT



[Home](#) | [About Us](#) | [Contact Us](#) | [Media Kit](#)

Copyright © 2000-2006 MiTechNews.com - All rights reserved. Site Designed by: PIXELBIT New Media