

Pressemitteilung

[BoxID 144892, Sicherheit]

Storm Worm blows in with New Year wishes

Storm Worm blows in with New Year wishes

(pressebox) München, 03.01.2008 - Apply caution when you get New Year messages in your mail box! A massive attack of the Storm Worm variant called 'Zhelatin.pt' is underway with a rather simpler modus operandi, say Security Experts at MicroWorld Technologies.

It begins with emails arriving with subject line 'Happy New Year' or 'Message for new year'. The mail body has a web address chosen from a random list that contains URLs like newyearcards2008.com, newyearwithlove.com, hohoho2008.com, hellosanta2008.com, happy2008toyou.com and uhavepostcard.com. (Please don't try to access any of these websites on your computer!)

On these websites, a message is displayed which reads as, "Your download should begin shortly..... Click here to launch the download and press Run. Enjoy!". Clicking the link, a file named happynewyear2008.exe or happy2008.exe, which carries the worm Zhelatin.pt, is downloaded into the computer. Once a victim clicks on

weiterempfehlen

Druckversion

Meldungen als RSS

Trackback

**Firmeninfo****MicroWorld Technologies GmbH**

Leopoldstr. 244

D-80807 München

www.microworld.de [Karte](#) **Pressefach**[Mehr Infos dieser Firma](#)**Weitere Meldungen**

03.01.2008

Storm Worm blows in with New Year wishes

24.10.2007

Kennen Sie die neueste Masche der Spammer?
Sie heißt MP3-Spam!

11.10.2007

MicroWorld releases MailScan 5.3 for various
Mail Servers

the downloaded exe, the Worm drops some files and runs certain services to quickly and silently to make the computer a part of a large spam relaying network or Botnet.

"Taking down the websites used in this Worm attack is quite a challenge as all of them are hosted using a technique called Fast-Flux DNS," says Manoj Mansukhani, Head - Global Marketing, MicroWorld Technologies. "Fast-Fluxing is a method where Virus authors deploy a continuously changing network of botnet computers to act as proxies for hosting harmful websites. To add to it, the Russian domain name provider where these sites are registered to is closed for the first week of January, which gives ample time for the criminals behind the worm to make merry!"

The first Zhelatin variant appeared in January 2007 which spread with the help of mails with a subject line '230 dead as storm batters Europe' and other socio political events, thereby deriving its popular name - Storm Worm. All mails carried exe attachments with randomly chosen names that invariably lured recipients into downloading them.

"Storm Worm is the most successful malware of its kind with an established botnet of around 3 million compromised computers worldwide according to some estimates. This network of zombie PCs relays a significant portion of the spam mail traffic on the Internet today. Unlike most other botnets, this one does not have a central command but operates using peer-to-peer networks which makes it practically impossible to dismantle it," Manoj points out.

Users can protect their computers from Storm Worm by resisting the temptation of clicking on season's greetings or other messages that require them to visit unknown websites and to download files, Manoj says. It is also equally important to keep their AntiVirus and Spam Control systems up-to-date, he adds.

03.08.2007

New kidnapper malware asks for \$300 ransom

19.07.2007

Spam mails in PDF format flood the web

16.07.2007

MicroWorld's free tool now removes Brontok Worm

11.06.2007

MicroWorld's eScan Wins VB100% in Comparative Review

30.05.2007

New Worm Spreads via email, Web, Network Shares and Software Vulnerability!

Schlagworte:

the
microworld
and
with
command

Ansprechpartner:

MicroWorld Technologies GmbH

E-Mail: pooja@mwti.net

Telefon: +49 (89) 20 80 39 - 223

Fax: +49 (89) 20 80 39 - 226

Über MicroWorld Technologies GmbH:

MicroWorld Technologies (www.mwti.net) is the developer of highly advanced AntiVirus, Content Security and Firewall software solutions eScan, MailScan, and eConceal. MicroWorld Winsock Layer (MWL) is the revolutionary technology that powers most of MicroWorld products enabling them to achieve several certifications and awards by some of the most prestigious testing bodies, notable among them being Virus Bulletin, Checkmark, TUCOWS, Red Hat Ready and Novell Ready.

For more information, please visit www.mwti.net

Veröffentlichung honorarfrei.

Bei Veröffentlichung bitte Belegexemplar an

service@pressebox.de

Für die oben stehende Pressemitteilung ist allein der jeweils angegebene Herausgeber (siehe Firmeninfo) verantwortlich. Die Huber Verlag für Neue Medien GmbH übernimmt keine Haftung für die Korrektheit oder Vollständigkeit der dargestellten Meldung. Auch bei Übertragungsfehlern oder anderen Störungen haftet sie nur im Fall von Vorsatz oder grober Fahrlässigkeit.

[AGB](#)|[Kontakt](#)|[Impressum](#)

© Huber Verlag für Neue Medien 2002 - 2008, Alle Rechte vorbehalten.

Partnerportale: [seminarSPIEGEL](#)|[Initiative Mittelstand](#)|[ititpro.com](#)|[www.promago.de](#)|[aktiv-verzeichnis.de](#) |[LifePR.de](#)