

Continue warning of viruses: W32 / Bereb-B, Troj / Eyeveg-C, W32 / Netsky-M

W32 / Bereb-B is a deep computer cum function of Trojan. W32 / Bereb-B can listen to commands on special IRC channels. W32 / Netsky-M is a deep bomb, capable of self-replicating and spreading according to the addresses collected from infected computers

Virus name

Summary

Detail

W32 / Bereb-B

W32 / Bereb-B is a deep computer cum function of Trojan. W32 / Bereb-B can listen to commands on special IRC channels.

Nickname

Worm.P2P.Astaber, Win32 / Bereb.C, W32.HLLW.Bereb, WORM_BEREB.B

W32 / Bereb-B is a peer-to-peer computer worm, capable of replicating the *shared startup* in the Windows folder under various names, including:

```
007 Crack.exe
007 keygen.exe
007.exe
3D Flash Animator v3.7.exe
3D Magic Pixel 3D Crack.exe
Magic 3D Pixel 3D.exe
Naked 9 girls.exe
ws_ftp.exe
xbox emulator (works !!) exe
xbox.info.exe.exe
xxx.exe
```

- For startup items to be turned into *shared folders* , W32 / Bereb-B will add values ??to the registry at the following address:

```
HKCUSoftwareKazaaLocalContentDir0 =
```

- W32 / Bereb-B will also clone to the Windows directory with the name svckernell.com ;and create registry keys at the following address so that it can be activated when the computer boots:

HKLMSoftwareMicrosoftWindows
CurrentVersionRunsckernell

- W32 / Bereb-B is a type of Trojan backdoor that spreads via IRC channel, and can listen to commands on special IRC.

- W32 / Bereb-B creates library.dat file in WinMx sub-directory, under Program Files folder.This file is not dangerous and can be removed.

Troj / Eyeveg-C

Troj / Eyeveg-C is a Trojan that steals passwords and collects personal information on infected computer systems and sends them to its creators.

- Troj / Eyeveg-C is a password-stealing Trojan that works in a Windows environment.

- To be able to run automatically every time Windows starts, Troj / Eyeveg-C replicates to a file with random names in the system directory (Windows) and adds registry keys related to this file.

- Troj / Eyeveg-C will also clone to the Windows startup directory.

- Troj / Eyeveg-C collects system and password information and sends it to a web site online.

W32 / Netsky-M

W32 / Netsky-M is a "deep bomb", capable of self-replicating and spreading according to the addresses collected from infected computers

- W32 / Netsky-M is a "deep bomb" that replicates and spreads according to the addresses collected from infected computers.

- W32 / Netsky-M copied itself into the Windows folder under the name AVPROTECT9X.EXE ;and to ensure that worms can be activated when the computer starts, W32 / Netsky-M will add values ??to the registry at the following address:

HKLMSoftwareMicrosoftWindows
CurrentVersionRun9XHtProtect =
AVprotect9x.exe

- W32 / Netsky-M collects e-mail addresses from the following extension files:

PL, HTM, HTML, EML, TXT, PHP, VBS, RTF, UIN, ADB, TBB, DBX, ASP, WAB, DOC, SHT, OFT, MSG, JSP, WSH, XML, SHTM, CGI, DHTM

E-mail infected with W32 / Netsky-M carries the following characteristics :

Headline :

Re: Requested file
Re: My file
Re: My document
Re: My information
Re: My details
Re: Information
Re: Improved
Re: Requested document
Re: Document
Re: Details
Re: Your document
Re: Your details
Re: Approved

Message line :

Chi ti?t cho.
Document.
I ?ã nh?n tài li?u c?a b?n. The improved document is attached.
I have attached document.
Your document is attached to this mail.
Authentication for c?n thi?t.
Requested file.
Xem t?p tin.
Hã y ??c các thông báo quan tr?ng msg_.
Please confirm the document.
is attached.
Your file is attached.
Hã y ??c t?p tin.
Your document is attached.
Hã y ??c t?p tin attached.
Hã y xem t?p tin k?t n?i cho chi ti?t.

Attachment (with extension ". PIF") :

improved_
message_
detailed_
your_document_
word_doc_
doc_
artichel_
picture_

file_
your_file_
details_
document_

You finished reading the article "**Continue warning of viruses: W32 / Bereb-B, Troj / Eyeveg-C, W32 / Netsky-M**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.