Alcarys

CLASSIFICATION

Category:	Malware
Type:	-
Platform:	-
Aliases:	Alcarys, I-Worm.Alcaul, W32/Alcarys@mm, W32.Alcarys@mm, Alcaul

SUMMARY
Alcarys is an email worm written in Visual Basic. The worm's executable file is compressed by UPX file compressor. The worm was first discovered in February 2002.

Automatic action

Based on the settings of your F-Secure security product, it will either move the file to the **quarantine** where it cannot spread or cause harm, or **remove** it.

Suspect a file is incorrectly detected (a False Positive)?

A False Positive is when a file is incorrectly detected as harmful, usually because its code or behavior resembles known harmful programs. A False Positive will usually be fixed in a subsequent database update without any action needed on your part. If you wish, you may also:

- **Check for the latest database updates**

  First check if your F-Secure security program is using the latest detection database updates, then try scanning the file again.

- **Submit a sample**

  After checking, if you still believe the file is incorrectly detected, you can submit a sample of it for re-analysis.

  NOTE If the file was moved to **quarantine**, you need to collect the file from quarantine before you can submit it.

- **Exclude a file from further scanning**

  If you are certain that the file is safe and want to continue using it, you can exclude it from further scanning by the F-Secure security product.

  NOTE You need administrative rights to change the settings.

FOR MORE SUPPORT

Community
Find the latest advice in our Community.

User Guide
See the user guide for your product on the Help Center.

Contact Support
Chat with or call an expert for help.

Submit a sample
Submit a file or URL for further analysis.

TECHNICAL DETAILS

Variant:Alcarys.A

The worm puts a shortcut on the desktop with the 'free XXX Passwords.lnk' name and points the link to 'c:\xxxpasswords.doc' file. Also the worm creates another shortcut on the desktop with the name 'mailme.url' and when this shortcut is clicked, an email client opens a new messages to 'alcopaul@cannabismail.com' which is the worm's author email address.

The worm attempts to download and run the 'update.exe' file from an account at www.tripod.com free web hosting service. To do this the worm creates the 'c:\v.vbs' file with appropriate commands and starts it.

The worm creates 'c:\dnserror1.html' file that has the text 'Hello... Click here to start...'. The 'here' word is a link to 'c:\windows\system\inet.exe' file that is one of worm's copies. This file has author's credits: '--by alcopaul.ph--'.

The worm will create copies of itself in a system with the following names:

```
c:\windows\system\inet.exe
c:\windows\cmd.com
c:\syra.scr
c:\windows\system\tmp.tmp
c:\SexSound.exe
c:\windows\opme.co_
c:\autorun.com  a:\moans.exe
c:\www.EcstasyRUs.com
f:\pussy.scr
```

The worm creates 'c:\readme.txt' file with the following text:

```
A Collection Of Haiku
-----------------
Dried marijuana...
And my grandfather's old pipe...
Tears in my red eyes...
-----------------
Condoms in the bag...
A lustful stare from your eyes...
In the girl's rest room...
-----------------
```

The worm looks for windows with the following text and attempts to close them:

```
PC-cillin 2000 : Virus Alert
JavaScan
DAPDownloadManager
Real-time Scan
Pop3trap
AVP Monitor
IOMON98
NAI_VS_STAT
```

The worm creates and imports 'c:\v.reg' file to modify Microsoft Word security settings, to create the startup key for its files in the Registry:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\*inet]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce\*cmd]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\*autorun]
```

Also the worm changes Windows registration information to:

```
RegisteredOwner = 'alcopaul.ph'
ProductName = 'syra, the worm'
```

If mIRC client is found on an infected system the worm creates 'script.ini' file in 'c:\mirc\' folder. This script file contains commands that will send the 'c:\windows\opme.co_' file to all people joining and leaving an infected channel. Together with itself the worm will send one of the following text messages:

```
Hello..
Do you wanna be an operator of this channel? Here's a software from mIRCx..
First, you'll have to convert it to a .com file then run it and become a channel operator instantly...
Be a channel operator using this software from mIRCx...
First, you'll have to convert it to a .com file then run it and become a channel operator instantly...
```

To spread itself the worm opens Outlook Address Book and sends itself to all email addresses it can find there. Infected messages look like this:

```
Subject:        sounds of sex and other stuffs"

Body:           ....Hear me and my girlfriend moan...We spent yesterday's night having sex...
I've also included a list of haiku, a cool talking screensaver and a link to a site
offering cheap ecstasy pills.. enjoy..

Attachment:
sexsounds.wav (which is 'sexsound.exe' file)
haiku for you (which is 'readme.txt' file)
http://www.EcstasyRUs.com (which is 'www.EcstasyRUs.com' file)
the cool talking screensaver (which is 'syra.scr' file).
```

After spreading the worm will create the 'c:\alcopaul.html' file with the text 'Infected by Syra' and show a messagebox:

```
w32.hllp.syra.b by alcopaul
you've been hit by, you've been struck by the smooth criminal, AW!
```

The worm has a dangerous payload. It overwrites all HTM and HTML files in can find on a system with the contents of 'c:\dnserror1.html' file (see above). Also the worm overwrites all COM and SCR files (except COMMAND.COM and WIN.COM) with its copy. Also the worm creates 'satellite' files for every WAV and MP3 file it can find on an infected system. The worm copies itself with the name of a found MP3 or WAV file and adds EXE extension. Also the worm tries to overwrite the following files:

```
avpm.exe
_avpm.exe
avp32.exe
_avp32.exe
vshwin32.exe
```

F-Secure Anti-Virus detects this worm with the updates published on 25th of February, 2002.

Variant:Alcarys.B

This variant is not in the wild. F-Secure is currently analysing this worm variant.