

Re: W32/Delbot-AK

Source: <http://newsgroups.derkeiler.com/Archive/Alt/alt.comp.anti-virus/2007-04/msg00226.html>

- *From:* foghollow <dave@xxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 18 Apr 2007 12:51:11 +0100
-

In article <1176894469.489878.283310@b75g2000hsg.googlegroups.com>, paulcarr@xxxxxxxxxxxxxxxxxx says...

Has anybody experience a virus referenced as W32/Delbot-AK by sopho's.

We have attempted to clear using sophos across servers.

We think the following files have some thing to do with infection.
cnen.exe & ntoepad.exe.

Does anyone have experience of this and recommendations to removal.

<http://www.sophos.com/virusinfo/analyses/w32delbotak.html> says this:

W32/Delbot-AK is a worm with backdoor functionality for the Windows platform.

W32/Delbot-AK spreads to other network computers by:

- Scanning network shares for weak passwords
- Exploiting common buffer overflow vulnerabilities
- Symantec (SYM06-010)
- Microsoft Security Advisory (935964): Vulnerability in RPC on Windows DNS Server Could Allow Remote Code Execution.

When first run W32/Delbot-AK copies itself to <System>\ntoepad.exe and attempts to download and execute a file from a remote location to <Root>\radi.exe. At the time of writing, this file was unavailable for download

The following registry entry is created to run ntoepad.exe on startup:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Notepad
<System>\ntoepad.exe
```

So it looks simple enough to clean.

Re: W32/Delbot-AK

Boot to Safe Mode, delete that file and registry entry – or just scan with Sophos.
Password all usernames, including Guest even if it shows as disabled.

Re-boot.

Password any shares

Get up to date with MS patches.

—

If you don't want the whelks don't muck 'em about

If you don't want them someone else may

.