

McAfee® Best Practices advisory for W32/NetSky.b@MM

By Lee Fisher
McAfee Security Strategist

What does the threat do?

W32/NetSky.b@MM is the 2nd variant of a worm which was first discovered on the 16th February 2004. This specific variant was discovered on the 18th February 2004 and, due to the number of samples received by the AVERT™ Labs, was assessed as a Medium risk.

The worm infects Microsoft® Windows® 9x, ME, NT4, 2000 and XP based computers using the following methods:

1. It propagates through generating SMTP email (using its own engine) as an attachment within the email. The worm is capable of spoofing email addresses from the infected machine.

One of the following subject lines is used:

- fake
- for
- hello
- hi
- immediately
- information
- it
- read
- something
- stolen
- unknown
- warning
- you

One of the following message bodies is used:

- about me
- anything ok?
- do you? that's funny
- from the chatter
- greetings
- here
- here is the document.
- here it is
- here, the cheats
- here, the introduction
- here, the serials
- i found this document about you
- I have your password!
- i hope it is not true!
- i wait for a reply!
- i'm waiting ok
- information about you
- is that from you?
- is that true?
- is that your account?
- is that your name?
- kill the writer of this document!
- my hero
- read it immediately!
- read the details.
- reply
- see you
- something about you!
- something is fool
- something is going wrong
- something is going wrong!
- stuff about you?
- take it easy
- that is bad
- thats wrong why?
- what does it mean?
- yes, really?
- you are a bad writer
- you are bad
- you earn money
- you feel the same
- you try to steal
- your name is wrong

The attachment name also varies and with this degree of 'randomisation' choosing one of the following names:

- aboutyou
- attachment
- bill
- concert
- creditcard
- details
- dinner
- disco
- doc
- document
- final
- found
- friend
- jokes
- location
- mail2
- mails
- me
- message
- misc
- msg
- nomoney
- note
- object
- part2
- party
- posting
- product
- ps
- ranking
- release
- shower
- story
- stuff
- swimmingpool
- talk
- textfile
- topseller
- website

Providing one of the following attachment 'type' names:

- .doc
- .htm
- .rtf
- .text

It could be followed by one of the following, performing the 'double extension' trick:

- .com
- .exe
- .pif
- .scr

Finally the worm may also be included within a *.ZIP file.

Due to the degree of randomisation of how the attachment is received, here are a couple of examples:

Friend.doc.pif
Story.rtf.exe

2. The worm propagates through copying itself to mapped network drives.
3. The worm propagates through copying itself to the local systems share or sharing directories.

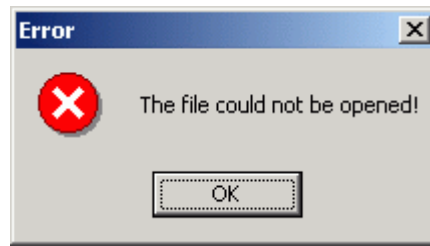
Note that the following filenames are used when propagating via methods 2 and 3:

- aboutyou.zip
- attachment.zip
- bill.zip
- concert.zip
- creditcard.zip
- details.zip
- dinner.zip
- disco.zip
- final.zip
- found.zip
- friend.zip
- jokes.zip
- location.zip
- mail2.zip
- mails.zip
- me.zip
- message.zip
- misc.zip
- msg.zip
- nomoney.zip
- note.zip
- object.zip
- part2.zip
- party.zip
- posting.zip
- product.zip
- ps.zip
- ranking.zip
- release.zip
- shower.zip

4. The worm propagates through the various Peer to Peer applications, including Bearshare, KaZaA and Limewire, under the following filenames:

- angels.pif
- cool screensaver.scr
- dictionary.doc.exe
- dolly_buster.jpg.pif
- doom2.doc.pif
- e.book.doc.exe
- e-book.archive.doc.exe
- eminem - lick my pussy.mp3.pif
- hardcore porn.jpg.exe
- how to hack.doc.exe
- matrix.scr
- max payne 2.crack.exe
- nero.7.exe
- office_crack.exe
- photoshop 9 crack.exe
- porno.scr
- programming basics.doc.exe
- rfc compilation.doc.exe
- serial.txt.exe
- sex sex sex sex.doc.exe
- strippoker.exe
- virii.scr
- win longhorn.doc.exe
- winxp_crack.exe

Upon execution of the worm, the following dialogue box is displayed:



The worm then begins to extract email addresses from the system by scanning the following file types:

```
.adb      .asp  .dbx  .doc  .eml  .htm  .html
.msg      .oft  .php  .pl   .rtf  .sht  .tbb
.txt      .uin  .vbs  .wab
```

The virus sends itself via SMTP, constructing messages using its own SMTP engine. It queries the DNS server for the target domain MX record and connects directly to the MTA of the targeted domain and sends the message.

The worm then copies itself into %windir% folder using the filename SERVICES.EXE.

The worm then hooks the system registry to ensure future load on system restart:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
"service" = %windir%\services.exe -serv
```

Note: %windir% is a variable for the windows directory name. The worm does not use this exact name. It simply uses this to obtain the Windows directory.

Finally the worm virus removes the following registry values to deactivate the W32/Mydoom.a@MM and W32/Mydoom.b@MM worms.

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Taskmon
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Explorer
- HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32

Further details of the worm can be found in the McAfee AVERT [Virus Information Library](#).

What proactive steps can be taken against the threat ?

1. The most likely method for the worm to enter your organisation is via email. It arrives as an attachment with various filenames with the body text detailed above.

The McAfee® gateway appliances and GroupShield™ products offer the ability to block emails based on their attachment type or name, or body text within the mail.

However, you should be aware that the latter method may leave you open to new variants of the worm that use different body text phrases. McAfee Best Practices advise that executable file attachments should not be allowed through the gateway as general security advice. If you would like a copy of the recommended file types to block, please contact your McAfee sales representative.

In any case you should begin to immediately deploy the 4325 virus definition files (DATs) across your organisation to prevent systems from infection.

2. By default McAfee Desktop Firewall™ will block access to SMTP on TCP port 25 if no legitimate applications are defined to make use of those ports. This will prevent infected systems from further propagating the worm. Where using McAfee Desktop Firewall, the default port used by the worm will be blocked.

In addition, the McAfee Desktop Firewall has an application control feature whereby any untrusted (not previously approved) application will not execute. If your clients used this feature, they will not become infected, although the worm will be on the computer's hard drive.

3. McAfee Entercept™ will detect the worm attempting to write itself into a system folder (%windir%) in addition to also detecting that the worm attempting to write entries within the 'RUN' key in the system registry and would therefore prevent infection occurring.
4. McAfee IntruShield® already provides a generic signature to protect against this worm. The generic signature covers all commonly used attachment types for worms. To stop the propagation, the customer can enable blocking for the signature "SMTP: Worm Detected in Attachment" in their policy.
5. Like most of the mass mailing threats we see today, W32/NetSky.b@MM uses its own SMTP mail engine. This email is unlikely to pass through local email servers, (i.e. the local Microsoft® Exchange Server) instead heading straight for your Internet mail gateway. Your Internet mail gateway should be configured to only accept SMTP traffic from specific IP addresses (your email servers) within your environment. This would prevent the worm from further propagating.

What can I do if I have been infected with the threat ?

The first steps with any infection are to gain some level of information as to the scale of the infection and then limit it from progressing further.

- Immediately update your mail/gateway scanners to the 4325 definition files. (DATs)
- If possible, implement a temporary email filter to block executable files within your GroupShield/WebShield® anti-virus scanners. You may wish to add elements of the worm's body text to your content filters on Webshield. (Note you can also use this feature to detect infected users)
- McAfee ThreatScan™ signatures have also been updated for more accurate identification of infection from W32/NetSky.b@MM. ThreatScan can assist in detecting infected clients which may not have AV installed, or be up to date.
- Implement a network wide update of your anti-virus definition files.
- Run an on demand scan task to force anti-virus scanners to detect infections. You can make this less obtrusive by limiting the scan to the clients C:\WINNT or C:\WINDOWS (include subdirectories)
- The forthcoming System Compliance Profiler is an integral component of ePolicy Orchestrator (ePO), enabling security professionals to quickly assess enterprise-wide, system compliance.

With the System Compliance Profiler feature, you can assess which systems may have been infected with this worm – EVEN without a McAfee anti-virus solution being installed on the remote system.

Using the pre-defined templates, it is simple to initiate a comprehensive and accurate scan for system infections, and takes only a few minutes to configure.

The System Compliance Profiler is currently in Beta and is available for download [here](#).

Once you have discovered infected machines they should be quarantined to limit the infection until they are cleaned from infection.

- Where McAfee Desktop Firewall is installed the attempt to send data through any of the compromised ports listed above would result in an alert event being created. Where this is being managed by ePolicy Orchestrator (ePO), this will give you real time data on any instances of PC's infected by the worm.
- A free to use Stinger utility has been made available to clean potentially infected clients. AVERT Stinger can be located [here](#).

If at all possible you should clean infected PC's first, then expand to apply the update all other PC's. Use ePolicy Orchestrator™ (ePO) infection reports to help confirm the removal of the worm. For ePO users the 'wake-up call' or global update feature can help you ensure all PC's get and apply the update immediately. The ePO coverage reports give you visibility, to ensure compliancy.

If you have ThreatScan, we would suggest running a ThreatScan resource scan to give you visibility into all the devices on the network, so you can ensure they are ePO-managed. Rogue PC's are a common source of infection and re-infection.

Expert Services – We can help you

Network Associates Expert Services offers several services to help organization clean up all varieties of Malware outbreaks and assist in security patch management implementations.

If you are having difficulties, engaging services is a way to provide your organisation with a complete and expedient solution to your problem.

McAfee services can assist in vulnerability assessment programmes, patch management system management and work in coordination with your security team.

Our emergency outbreak services also provide swift detection and cleanup of viruses.

The impact of these vulnerabilities also highlights the need for Threat Assessment services. These services provide a review of anti-virus implementations, policies and processes, a vulnerability scan of mission critical servers and a scan of random nodes to determine the organization's exposure to threats, a review of their change management procedures and policies, and incident response planning.

For more information contact your local services representative.