

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

By Lee Fisher
McAfee Security Strategist

What does the threat do?

W32/Bagle@MM was first discovered on the 18th January 2004, and this (the second) variant was discovered on the 17th February 2004 and was initially classed as a low risk threat. However due to increasing number of samples received by the AVERT™ Labs, this threat was reassessed as a Medium risk later on the same day.

The worm infects Microsoft® Windows® 9x, ME, NT4, 2000 and XP based computers using a single method.

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.

The subject line and message body contain random string texts, but are fairly simple to spot, being constructed as follows:

```
From : (address is spoofed)
Subject : ID (string)... thanks
Body :
Yours ID (string2)
--
Thank
```

Where "string" and "string2" are random.

The attachment name also varies and with this degree of randomisation, and thus blocking/filtering techniques will be thwarted by using the worm's filename.

Upon execution of the worm, the system date is queried, and the worm will stop running if the system date is February 25th, 2004 or later. If the date is prior to this date, then the worm executes the standard Windows sound recorder program (SNDREC32.EXE) while the worm undertakes the following:

The worm copies itself to the Windows System directory (%sysdir%):

```
%SysDir%\AU.EXE
```

The worm then hooks the system registry to ensure future load on system restart, by adding the following keys :

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Run "d3update.exde" = (%SysDir%\AU.EXE
```

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

The worm also creates the following keys in the system registry:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows98 "frn"
HKEY_CURRENT_USER\Software\Microsoft\Windows98 "gid"
```

Target email addresses are then extracted from files on the victim machine by scanning the hard drive. File types with the following extensions are scanned:

```
htm html txt wab
```

The worm then sends messages with infected attachments to the collected addresses. The SMTP engine uses direct Mail eXchange (MX) lookup on the target domain so it does not depend on email settings of the infected computer.

The worm then listens on TCP port 8866 for remote connections, attempting to notify the worm author of an infected system that is waiting for further commands. It undertakes this by calling for a PHP script (named `1.PHP`) which may be located on various remote internet sites:

- `http://www.47df.de`
- `http://www.strato.de`
- `http://intern.games-ring.de`

The worm is attempting to contact the malware author, providing an ID of the infected computer with the backdoor port which has been opened.

Note that the worm also contains a backdoor and at the time this threat brief was published the full extent of its functionality was still under investigation.

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. Details of the worm can be found [here](#).

McAfee Best Practices advise that executable file attachments should not be allowed through the gateway as general security advice.

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.

McAfee Desktop Firewall™ will also prevent the worm from opening TCP port 8866, and from downloading future components.

3. McAfee Enterecept™ will detect the worm attempting to write itself into a system folder (%SystemDir%) in addition to also detecting the worm's attempt 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 as well as its original form W32/Bagle. 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. For customers wishing to identify this worm individually, a new user defined signature has been released. This worm can be blocked by enabling blocking on signature "UDS-SMTP: Worm Bagle.b Detected" in the customer's policy.
5. Like most of the mass mailing threats we see today, W32/Bagle.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 4324 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™ can detect infected clients by performing a network wide port scan of TCP 8866. Any clients found to have that port open may indicate infection. McAfee ThreatScan™ has also been updated for more accurate identification of infection from W32/Bagle.b@MM
- 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)

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 found [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 outbreaks, including W32/Bagle.b@MM. If you are having difficulties, engaging services is a way to provide them a complete and expedient solution to their virus problem. Our emergency outbreak services provide swift detection and cleanup of viruses. Specific to W32/Bagle.b@MM, our services can detect the worm with Sniffer technology and detect and contain with vulnerability assessment, firewalls, and coordination with their security team.

The impact of this virus also highlights the need for Threat Assessment services. This service provides a review of their anti-virus products, 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.