

# McAfee® Best Practices advisory for W32/Sobig.f@MM

By Lee Fisher  
Solutions Architect

## What does the threat do?

W32/Sobig.f@MM is the 6th variation of a threat that was first discovered on the 9th January 2003. This specific variant was discovered on the 18<sup>th</sup> August 2003, and was initially classed as a low risk. However due to the increasing number of samples sent into the AVERT™ labs, this threat was reassessed as a medium risk for corporate and a high risk for home users later on the 18th August 2003.

The worm infects Microsoft® Windows® 9x/ME, NT4, 2000 and XP based computers using two 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.

The worm pads the file with garbage data at the end of the file, therefore the size and checksum of the attachment varies. The attachment is either a \*.PIF file or a \*.SCR file.

Target email addresses are extracted from files on the victim machine with the following extensions:

```
DBX EML HLP HTM HTML MHT TXT WAB
```

Initial copies of the worm always appear to have the following body text:

```
"see the attached file for details"
```

2. It propagates through accessible network shares, writing itself if possible to the %windir% directory on the target computer system. Depending on the OS, this will typically mean that C:\WINNT or C:\WINDOWS will have the following files copied :

```
"winppr32.exe" (a copy of itself) and "winstt32.dat" (configuration file)
```

The following Registry keys are added to hook system startup:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run  
"TrayX" = %windir%\winppr32.exe /sinc
```

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run  
"TrayX" = %windir%\winppr32.exe /sinc
```

Once a machine has become infected the worm attempts to contact a list of IP addresses for remote NTP servers, to which it sends NTP packets (destination port 123).

Like earlier versions of the W32/Sobig family, the worm has a date triggered self-termination routine. If the date is September 10th 2003 or later, the worm will no longer propagate.

## 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 either a \*.PIF or \*.SCR extension 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 at :

[http://vil.nai.com/vil/content/v\\_100561.htm](http://vil.nai.com/vil/content/v_100561.htm)

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™ would block access to SMTP on TCP port 25 and NTP on TCP 137 if no legitimate applications were defined to make use of those ports. This would prevent infected systems from further propagating the worm. Where using McAfee Desktop Firewall, the default port used by the various should be blocked unless you specifically have an application that makes use of those ports.
3. McAfee Enterecept™ would 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 would prevent infection occurring.
4. ThreatScan™ is able to scan your network for the vulnerabilities which W32/Sobg.f exploits. This information provides you with a clear understanding on how much of a risk your network is facing from this ( and many other ) worm.
5. Like most of the mass mailing threats we see today, W32/Sobig.f 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 4287 definition files. (DATs)
- If possible, implement a temporary email filter to block \*.PIF or \*.SCR files within your GroupShield/WebShield™ anti-virus scanners.
- 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 )
- ThreatScan™ has been updated to allow you to remotely scan for W32/Sobig.f infections across your network. This is a powerful, fast mechanism to detect infected clients, allowing you to quarantine them quickly to prevent further propagation.

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

- ThreatScan™ can tell you which network shares the infected PC's had access to, as due to the nature of the worm it is likely these shares may also be infected.
- 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 ePO infection reports to help confirm the removal of the worm. For ePO users the 'wake-up call' 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/Sobig.f@MM. If your customer seems to be struggling, 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/Sobig.f@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.