# Worm:W32/NetSky.H | F-Secure

Archived: 2026-04-05 13:29:00 UTC

## Classification

Aliases:

NetSky.H, W32/NetSky.H@mm, I-Worm.NetSky.h, W32.NetSky.H@mm

## Summary

Yet another NetSky worm variant - NetSky.H was found on 5th of March 2004. This variant is very close to NetSky.G variant. It spreads itself in emails as an executable attachment.This worm contains another, but this time less insulting message for the authors of Bagle and Mydoom. And like its previous variants NetSky.H tries to uninstall Bagle worm variants from an infected computer.

## Removal

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.

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 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.

## Technical Details

Descriptions of all previous NetSky worm variants can be found here:

- W32/NetSky.A@mm
- W32/NetSky.B@mm
- W32/NetSky.C@mm
- W32/NetSky.D@mm
- W32/NetSky.E@mm
- W32/NetSky.F@mm
- W32/NetSky.G@mm

The worm's file is a PE executable file 22528 bytes long, packed with PE-Pack file compressor. The unpacked file's size is over 28 kilobytes.

On March 8th, 2004 the worm constantly beeps with PC speaker from 11:00 to 11:59. Below is the link to the WAV file with the sound that the worm makes: https://www.f-secure.com/virus-info/v-pics/netsky_d.wav

NetSky.H worm doesn't copy its files to shared folders.

### Installation to system

When run, the worm installs itself to system. It copies its file to Windows folder as MAJA.EXE and creates a startup key for this file in System Registry:

```
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] "Antivirus" = "%windir%\maja.exe -antivirus se
```

where %windir% represents Windows directory

The worm creates a mutex named "MI[SkyNet.cz]SystemsMutex" to avoid running more than one instance of itself.

### Spreading in emails

NetSky.H worm has its own SMTP engine that it uses to send emails with infected attachments to all found email addresses. The worm uses different subjects, message body texts and attachment names in its emails.

The worm scans all available drives except CD-ROM drives for emails. It searches for email addresses in files with the following extensions:

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

The subject for infected messages is selected from the following list:

```
Re: Samples Re: Document Re: Approved Re: Here the file Re: Yours Re: Your file Re: Your folder Re:
```

The message body text for infected messages is selected from the following list:

```
Your document is attached. Here is the file. See the attached file for details. Please have a look
```

The attachment name for infected messages is selected from the following list:

```
your_smaples.scr your_document.scr document.scr message_part2.scr your_document.scr document_full.s
```

The worm avoids sending emails to email addresses that contain any of the following substrings:

```
icrosoft antivi ymantec spam avp f-secur itdefender orman cafee aspersky f-pro orton fbi abus messa
```

### Deleting Registry keys and disinfecting Bagle worm

The NetSky.H worm variant of the worm deletes the following Registry keys:

```
[HKCR\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32] [HKCU\Software\Microsoft\Windows
```

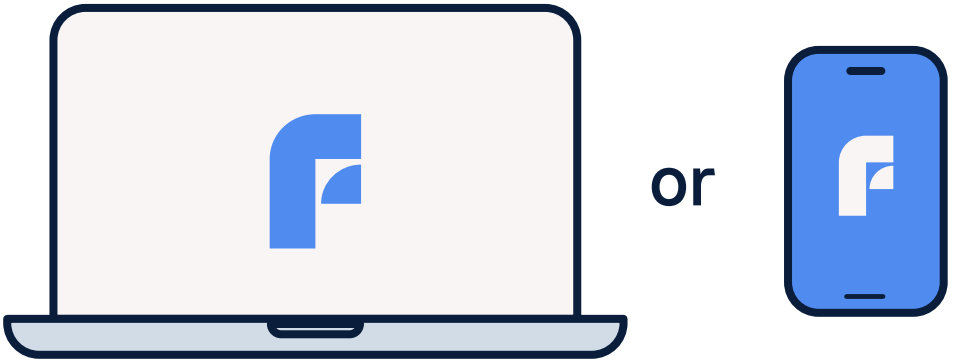
NetSky.H worm removes Registry keys of several Bagle worm variants if it finds them on an infected computer. At least the last 8 keys listed above belong to earlier Bagle variants.

## Protect your devices from malware with F-Secure Total

Protecting your devices from malicious software is essential for maintaining online security. F-Secure Total makes this easy, helping you to secure your devices in a brilliantly simple way.

- Award-winning antivirus and malware protection
- Online browsing, banking, and shopping protection
- 24/7 online identity and data breach monitoring
- Unlimited VPN service to safeguard your privacy
- Password manager with private data protection

Choose how many devices you want to protect to get started.




- Free customer support
- Cancel anytime
- The trial does not obligate you to buy the product

Try Total 30 days for freeAfter 30 days your subscription will renew automatically for one year at €69.99.

- Free customer support
- Cancel anytime
- The trial does not obligate you to buy the product

Try Total 30 days for freeAfter 30 days your subscription will renew automatically for one year at €89.99.

- Free customer support
- Cancel anytime
- The trial does not obligate you to buy the product

Try Total 30 days for freeAfter 30 days your subscription will renew automatically for one year at €99.99.

## More Support

**Contact Support**

Chat with with or call an agent.