Kaspersky Threats — Nyxem

Archived: 2026-04-05 12:49:09 UTC

Parent class: VirWare

Viruses and worms are malicious programs that self-replicate on computers or via computer networks without the user being aware; each subsequent copy of such malicious programs is also able to self-replicate. Malicious programs which spread via networks or infect remote machines when commanded to do so by the "owner" (e.g. Backdoors) or programs that create multiple copies that are unable to self-replicate are not part of the Viruses and Worms subclass. The main characteristic used to determine whether or not a program is classified as a separate behaviour within the Viruses and Worms subclass is how the program propagates (i.e. how the malicious program spreads copies of itself via local or network resources.) Most known worms are spread as files sent as email attachments, via a link to a web or FTP resource, via a link sent in an ICQ or IRC message, via P2P file sharing networks etc. Some worms spread as network packets; these directly penetrate the computer memory, and the worm code is then activated. Worms use the following techniques to penetrate remote computers and launch copies of themselves: social engineering (for example, an email message suggesting the user opens an attached file), exploiting network configuration errors (such as copying to a fully accessible disk), and exploiting loopholes in operating system and application security. Viruses can be divided in accordance with the method used to infect a computer:

- file viruses
- boot sector viruses
- macro viruses
- script viruses

Any program within this subclass can have additional Trojan functions. It should also be noted that many worms use more than one method in order to spread copies via networks.

Class: Email-Worm

Email-Worms spread via email. The worm sends a copy of itself as an attachment to an email message or a link to its file on a network resource (e.g. a URL to an infected file on a compromised website or a hacker-owned website). In the first case, the worm code activates when the infected attachment is opened (launched). In the second case, the code is activated when the link to the infected file is opened. In both case, the result is the same: the worm code is activated. Email-Worms use a range of methods to send infected emails. The most common are: using a direct connection to a SMTP server using the email directory built into the worm's code using MS Outlook services using Windows MAPI functions. Email-Worms use a number of different sources to find email addresses to which infected emails will be sent: the address book in MS Outlook a WAB address database .txt files stored on the hard drive: the worm can identify which strings in text files are email addresses emails in the inbox (some Email-Worms even "reply" to emails found in the inbox) Many Email-Worms use more than one of the sources

listed above. There are also other sources of email addresses, such as address books associated with web-based email services.

Read more

Platform: Win32

Win32 is an API on Windows NT-based operating systems (Windows XP, Windows 7, etc.) that supports execution of 32-bit applications. One of the most widespread programming platforms in the world.

Description

1. Reboot your computer in Safe Mode - press and hold F8 while the machine is rebooting and choose Safe Mode from the menu when it appears.
2. In Task Manager, terminate any process with one of the following names:

```
rundll16.exe


scanregw.exe


Update.exe


Winzip.exe


WINZIP_TMP.EXE


New WinZip File.exe


WinZip Quick Pick.exe
```

3. Manually delete the following files from the Windows root and system directories, and the system registry:

```
%Windir%rundll16.exe
```

```
%System%scanregw.exe

%System%Update.exe

%System%Winzip.exe

%System%WINZIP_TMP.EXE

%System%New WinZip File.exe

%User Profile%Start MenuProgramsStartupWinZip Quick Pick.exe
```

4. Delete the following value from the system registry:

```
[HKLMSoftwareMicrosoftWindowsCurrentVersionRun]

"ScanRegistry" = "scanregw.exe /scan"
```

5. Reboot your computer and check you have deleted all infected messages from all mail folders.
6. If any applications have been damanged (in most cases this will be antivirus solutions and firewall programs) you will need to re-install them.
7. Perform a full scan of your computer (download a trial version of Kaspersky Anti-Virus here

Read more

Find out the statistics of the vulnerabilities spreading in your region on statistics.securelist.com

Found an inaccuracy in the description of this vulnerability? Let us know!
