Malware Environment

Malware Descriptions
- Network Worms
- Classic Viruses
  - File and Boot Viruses
  - Macro Viruses
  - Script Viruses
- Trojan Programs
- Other Malware

Who Creates Malware

History of Malware

Malware Trends

If Your Computer Is Infected

Malware Description Search

Search

Home / Viruses / Virus Encyclopedia / Malware Descriptions / Classic Viruses / File and Boot Viruses

Virus.VBS.Small.a

Detection added	Dec 25 2006 19:54 GMT
Update released	Dec 25 2006 21:26 GMT
Description added	May 24 2007
Behavior	Virus

Technical details

This malicious program has two components. The first is a file containing a script written in Visual Basic Script. The second is a command interpreter packet file. The components vary in size from 483 to 1368KB.

Payload

Once launched, the packet (virus) file will add to the configuration registry from the registry file "autorun.reg", which is located in the same directory as the virus file.

The virus then exports the contents of "autorun.bin", which is located in the same directory as the virus file, or in the Windows system directory, to "autorun.txt" which is located in the C: root directory:

```
.\autorun.bin
%WinDir%\system32\autorun.bin
c:\autorun.txt
```

If there are no command line parameters in the directory with the virus file, or the Windows system directory, the virus will search for a file called "autorun.vbs". If this file is found and launch, the virus file will cease running.

```
.\autorun.vbs
%WinDir%\system32\autorun.vbs
```

Some modifications of this virus will also create a subdirectory called "system" in the Windows system directory, and copy all "autorun.*" files from the catalogue containing the virus file to this directory:

```
%System%\system.
```

When the second component is launched (the file containing the script written in Visual Basic Script, which will usually be called "autorun.vbs") the current system date will be compared to the date given in the script. If the dates do not match, the component will cease running. If the dates do coincide, a packet file called "autorun.bat" will be launched. The contents of "autorun.txt" in the C: root directory will be read, the file will be decrypted (this file is not zero sized) and the contents of the file will be displayed in a message window.

If the current year is no later than 2030, "autorun.*" files on all local hard and network drives, as well as on all removable storage media (except those with the logical disk names A: and B:) will be copied either direction, either by calling "autorun.bat", the packet file, with a range of parameters.

Removal instructions

If your computer does not have an up-to-date antivirus, or does not have an antivirus solution at all, follow the instructions below to delete the malicious program:

1. Use the Registry Editor to delete registry keys and parameters which were created in the configuration registry from the registry file "autorun.reg".
2. Delete "autorun.txt" from the C: root directory. Delete the following file:

   ```
   c:\autorun.txt
   ```

   Also delete the following files:

   ```
   .\autorun.bin
   .\autorun.vbs
   %WinDir%\system32\autorun.bin
   %WinDir%\system32\autorun.vbs
   ```

3. Update your antivirus databases and perform a full scan of the computer (download a trial version of Kaspersky Anti-Virus).