Symantec United States

security updates

global sites

products

purchase

service and

security updates

downloads

about symantec

search

feedback

Legal Notices
Privacy Policy

W32.Update.Worm

Discovered on: May 28, 2001

Last Updated on: May 30, 2001 at 09:22:22 PM PDT

Print Printer-friendly version

W32.Update.Worm is a simple mass-mailing worm that can spread using Microsoft Outlook. The worm is written in a high-level language. However, for the email spreading, the worm creates and executes a VBS script. This worm also can also spread using mIRC.

This worm may also attempt to disable Norton AntiVirus, depending on which version is being used and under which operating system.

NOTE: Virus definitions dated prior to May 28 will detect some components of this worm as Bloodhound.VBS.Worm.

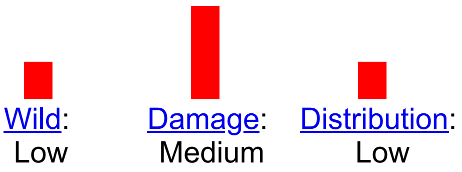
Also Known As: I-Worm.Mustard, W32.Mustard

Category: Worm

Infection Length: 7168 Bytes

Virus Definitions: May 28, 2001

Threat Assessment:



Damage:

- Payload Trigger: Always
- Payload: Attempts to disable NAV

Distribution:

- Subject of email: Antivirus Update
- Name of attachment: AVUpdate.exe
- Size of attachment: 7 Kb

Technical description:

When the worm is first executed, it tries to create an entry in the Windows registry. This appears to be used as a check as to whether the worm has already run on the computer.

The worm creates a copy of itself as \Windows\AVUpdate.exe. It then tries to send the newly created file to everyone in the Microsoft Outlook Address Book. The worm does this by creating the file Send.vbs directly under the root of drive C and executing it.

The worm drops a Script.ini file. If this Script.ini file is used together with the popular Windows IRC chat client mIRC, it sends AVUpdate.exe to other IRC users as they join the channel

Security Updates
Symantec AntiVirus Research Center and SWAT

Download Virus Definitions
Keep your protection up to date

Virus Encyclopedia
Search for Information on Viruses, Worms and Trojan Horses

Virus Hoaxes
Information on Virus Hoaxes

Jokes
Information on Jokes

Newsletter
Email Sent from the Symantec AntiVirus Research Center

Virus Calendar
Monthly Calendar Listing Trigger Dates for Viruses

Reference Area
Learn About Virus Detection Technologies

Submit Virus Samples
Send Suspected Threats for Review

that the infected user is in. The worm can "infect" mIRC only if mIRC is installed in any of the following paths.

- C:\Mirc
- C:\Mirc32
- C:\Program Files\Mirc
- C:\Program Files\Mirc32

NOTE: Norton AntiVirus detects the modified Script.ini file as W32.Update.Worm.

Finally, this worm attempts to disable Norton AntiVirus. However, this happens only under Windows 9x and only with some versions of NAV.

Removal instructions:

1. Run LiveUpdate to make sure that you have the most recent virus definitions.
2. Start Norton AntiVirus (NAV), and run a full system scan, making sure that NAV is set to scan all files.
3. Delete any files detected as W32.Update.Worm.
4. If the worm was executed on your system, reset all Norton AntiVirus settings back to the original settings, or alternatively, reinstall Norton AntiVirus.

Write-up by: Neal Hindocha

Tell a Friend about this Write-Up