©1995-2001 Symantec Corporation.
All rights reserved.

Legal Notices
Privacy Policy

security updates

W32.Malot.int

Discovered on: July 10, 2001
Last Updated on: July 12, 2001 at 11:38:03 AM PDT

Printer-friendly version

This is a mass-mailing worm.

Infection Length: 12,288, 1,291, 416

Virus Definitions: July 10, 2001

Threat Assessment:

Wild:	Damage:	Distribution:
Low	Low	Low

Wild:

- Number of infections: 0 - 49
- Number of sites: 0 - 2
- Geographical distribution: Low
- Threat containment: Easy
- Removal: Easy

Damage:

- Payload Trigger: Tuesdays
- Payload: Changes the window text of the "System Properties" window to "PetiK always is with you :-)"
  - Large scale e-mailing: Emails itself to all persons specified in the mailto: line of .html files located in IE cache folder
  - Modifies files: All .html files in the %windows% directory are appended with a small script

Distribution:

- Subject of email: New Virus Alert !!
- Name of attachment: MSVA.EXE
- Size of attachment: 12,288
- Ports: 25

Technical description:

NOTES:
Throughout this writeup:

- \Windows refers to the folder where Windows is installed, even if the folder has a name other than \Windows.
- \Startup refers to the \Startup folder of the user who was logged on to Windows when the worm was executed.

Arrival

This worm arrives as the following email message:

Subject: New Virus Alert !!
Message:

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

This is a fix against I-Worm.Magistr.
Run the attached file (MSVA.EXE) to detect, repair and protect you against this malicious worm

The email message is designed to appear to be sent by Microsoft, when in fact it has been mailed by the worm.

Insertions

This worm inserts the following files on the computer:

- \Windows\Runw32.exe
- \Windows\System\Msva.exe
- \Startup\VARegistered.htm

Modifications

The worm may add a line to the Win.ini file as follows:

```
[windows]
run=%windir%\runw32.exe
```

Infections

A small script is appnded to files with .htm* extensions that are in the \Windows folder. The script causes the following message to be displayed:

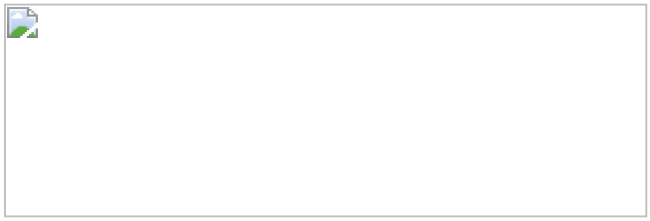
```
This file is infected by my new virus
Written by PetiK (c)2001
HTML/W32.MaLoTeYa.Worm
```

It also changes the Internet Explorer home page to the author's home page.

How the worm works

Activation from locations other than the \Windows folder
When the worm is executed, if it is not located in the \Windows folder, it does the following:

- It inserts itself onto the system
- It modifies the Win.ini file.
- It creates the VARegistered.htm file.
- It displays the following message:



Activation from the \Windows folder
When the worm is executed, if it is located in the \Windows folder, it does the following each time that Windows starts (following the initial infection):

- It infects all .html files in the \Windows folder.
- It sends country information that it finds in the Win.ini file to the author, using a mail server that is located in the United Kingdom.
- It iterates through the cache folder of Internet Explorer, and searches for .htm* files. Each file that is found is searched for lines that contain the **mailto:** command. The **mailto:** commands are used to send each recipient an email message that contains a copy of the worm.

Payload

On Tuesdays the worm changes the title bar text of the System Properties window to **PetiK always is with you :-).**

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.Malot.int, and if necessary, replace them from a clean backup.

Additional information:

Due to bugs, this worm:

- May cause system instability or cause the system to stop responding when the worm is run.
- Repeatedly infects files in the \Windows folder.

Write-up by: Atli Gudmundsson

 *Tell a Friend about this Write-Up*