April 26 could be repeated on July 14! The 'Smash' virus will try to destroy your hard drive!

Submitted by: Marylebone Media Relations
Wednesday, 26 April 2000

Orwell House

Cowley Road

Cambridge CB4 0PP

United Kingdom

Tel.: +44 1223 576001 Fax: +44 1223 470072

WWW: http://www.kasperskylabs.com

Cambridge, UK, April 26, 2000 - Kaspersky Lab, a fast-growing international anti-virus software development company, announces the discovery of a new extremely dangerous Windows virus, Win95.Smash. The virus originated from Russia and has been reported by a user there, to be in the wild.

Detection and disinfection routines for Win95.Smash virus have been included in the emergency update for AntiViral Toolkit Pro (AVP). The update is available free of charge on Kaspersky Lab's Web site on www.kasperskylabs.com.

Technical Details

General Characteristics

This is a memory resident parasitic Windows 9x virus about 10Kin size. The virus uses Win9x specific functions (VxD calls) and is not able to spread under Windows NT.

The virus affects PE EXE files by writing to the end of the file. The virus pays no attention to file name extensions, and as a result it can infect any Windows PE file - executable files, DLL libraries, SCR screen-savers, etc.

Payload

The virus has a very dangerous payload routine that is activated on July 14th - the virus overwrites the C:IO.SYS file with a trojan code and displays the message:

Virus Warning!

Your computer has been infected by virus.

Virus name is 'SMASH', project D version 0x0A.

Created and compiled by Domitor.

Seems like your bad dream comes true...

The virus then reboots the computer. While rebooting the affected IO.SYS file is loaded and executed, the trojan code takes control, displays the text "Formatting hard disk..." and then erases data on the first hard drive.

Infection

To make detection and disinfecting of infected files more difficult the virus uses a polymorphic engine that hides the virus code by using a mutating decryption loop.

The virus also uses a "block-mixing" structure (similar method was used in DOS virus "Badboy"). The virus code and data are divided into about 60 blocks (installation, infection, payload routines, etc.). When the virus infects the next file, it mixes these blocks in random order and links them with a special table. As a result the virus structure is different in each file infected.

When the virus code is prepared for writing to a victim file (blocks are mixed, encrypted and "covered" by a polymorphic "envelope"), the virus creates a new section at the end of the file, to which it writes its code and changes necessary fields in the PE header (including program's startup address field - to get control at the moment infected file is executed). The name of virus section in the file is randomly generated.

Memory residence and stealth functions

The virus installs itself into Windows memory and stays resident until the Windows session ends. To do this the virus uses a programming trick to switch its process from application to kernel mode (Ring3 -> Ring0). It Then allocates a block of kernel memory, hooks into the file search, accesses Windows kernel functions (IFS API) and stays in Windows memory as VxD driver.

When disk files are being searched or opened the virus' hooker takes control and runs its infection and stealth routines. The stealth routines make it very difficult to detect a virus when it is active.

About Kaspersky Lab

Kaspersky Lab Ltd. is a fast growing international privately owned anti-virus software development company with offices in Moscow (Russia), Cambridge (UK) and Johannesburg (South Africa). Founded in 1997 the company concentrates its efforts on the development of world-leading anti-virus technologies and software. Kaspersky Lab also provides free online security related internet information services. The company markets, distributes and supports its software and services in more than 40 countries worldwide.

Media Contacts

Denis Zenkin

Kaspersky Lab, Ltd.

Phone: +7 (095) 797 87 00

E-mail: denis@avp.ru

WWW: http://www.kasperskylabs.com

Sara Claridge

Marylebone Media Relations

Phone +44 118 975 5188

E-mail sara@marylebone.co.uk