WHITE PAPER

MARCH 1, 2002

TREND MICRO, INC.
10101 N. DE ANZA BLVD.
CUPERTINO, CA 95014
T 800.228.5651 / 408.257.1500
F 408.257.2003
WWW.TRENDMICRO.COM

The Real Cost of a Virus Outbreak

Why Is Antivirus Needed?

WHY IS ANTIVIRUS NEEDED?

A computer virus is a piece of executable code with the unique ability to replicate. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. They can attach themselves to just about any type of file and are spread as files are copied and sent from individual to individual.

Some computer viruses have a damage routine that can deliver a payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other kinds of damage. If the virus doesn't contain a damage routine, it can still cause trouble by taking up storage space and memory, and downgrading the overall performance of your computer or system network

Several years ago most viruses spread primarily via floppy disk, but the Internet has introduced new virus distribution mechanisms. With email now used as an important business communication tool, viruses are spreading faster than ever. Viruses attached to email messages can infect an entire enterprise in a matter of minutes, costing companies millions of dollars annually in productivity loss and cleanup expenses. Antivirus has become a necessity in the changing communication environment.

PREVALENCE OF INTERNET SECURITY BREACHES

% Reported	Threat
94	computer viruses
91	employee abuse of Internet access
48	attacks from outside
38	denial of service attacks

The Computer Security Institute conducted a survey of 538 computer security practitioners in corporations, government agencies, financial institutions, medical institutions, and universities in the United States. Their results[1] revealed that 85 percent of respondents had detected computer security breaches within a twelve-month period. The 35 percent[2] who listed a financial impact reported $377,828,700 in financial losses. Of these, many cited their Internet connection as the point of attack for hackers.

JUST HOW REAL IS THE CYBER-THREAT OF DESTRUCTIVE COMPUTER VIRUSES?

Viruses won't go away anytime soon. More than ten thousand have been identified and 500 new ones are created every month, according to the International Computer Security Association (ICSA). With numbers like those, it's safe to say that most organizations deal regularly with virus outbreaks. No one who uses computers is immune from viruses. With the growth of the Internet and email as the main communication tools, viruses and malicious code are undoubtedly a major concern for many businesses. A single email attachment or execution of a virus from the Internet or email can lead to widespread infection in a matter of hours and result in costly downtime.

[1] "2001 Computer Crime and Security Survey." Computer Security Institute (www.gosci.com).

[2] Ibid, 186 respondents out of 538.

WHAT RISK IS YOUR NETWORK FACING RIGHT NOW?

Hackers, with track records of developing sophisticated automated hacking tools, are hard at work creating new types of malware to confound IT administrators. Of 70,000 corporate networks surveyed in January 2001,[3] hackers made 6,000 attempts each month to gain access to corporations. This is three times the number of attempts made in the previous month. And IT managers have reported a sharp increase in the number of denial-of-service attacks[4] which can freeze an e-business web site, resulting in a loss of revenue.

Trend Micro offers a free Virus Risk Assessment service to provide an estimate of a network's vulnerability to virus attacks at http://www.antivirus.com/free_tools/edoctor/. The service is available in two levels of detail: Quick Assessment, which provides a fast and simple assessment of the system, and Advanced Assessment, which provides a thorough check of the entire corporate network.

TYPICAL VIRUS OUTBREAK SCENARIO

More than 87% of all viruses enter the enterprise via email.[5] Email has evolved beyond communication to become a business critical application. If email goes down, vital links to customers and vendors go down with it, and business grinds to a halt.

In this scenario, the entry point is an infected spreadsheet attached to an email sent via the Internet to 100 recipients at both Company A and Company B. It is assumed that 100% of computers are infected.

Investing in email virus protection can save an enterprise $22,000 per incident or, calculating the assumed average number of times a hacker will attempt to crack a network, $528,000 per year.

[3] The survey was conducted by Alameda, CA, based Pilot Network Services which closed in May of 2001.

[4] "Suspicious Server Probes Multiply." Computerworld, February 19, 2001 (www.computerworld.com)

[5] ICSA Labs Sixth Annual Computer Virus Prevalence Survey 2000 (www.ICSA.net).

TYPICAL COSTS INVOLVED WITH DETECTING, CLEANING AND RECOVERING FROM A VIRUS ATTACK

Action	Cost
Cost for an IT manager to be informed of and take action on one virus incident	$500
Cost for one workstation to be stopped, scanned, and cleaned of virus	$1,000
Cost for one workstation to detect and clean a virus infection locally	$100
Average number of times hackers will attempt to crack a network per month	2

COMPARATIVE COSTS OF A TYPICAL VIRUS OUTBREAK

COMPANY A
(no email protection)

Action	Cost
20% of users protected, but still call IT for help	$10,000
5% of users unprotected, require IT to scan and clean	$5,000
75% of users detect and clean infection themselves	$7,500
Total Cost of Incident	**$22,500**

COMPANY B
(email virus protection)

Action	Cost
IT Manager alerted and takes appropriate action	$500
Total Cost of Incident	**$500**

COMPARATIVE COSTS OF VIRUS OUTBREAKS OVER TIME

		COMPANY A (no email protection)	COMPANY B (with email virus protection)
Time Period	Virus Incidents	Total Cost	Total Cost
1 year	24	$540,000	$12,000
5 years	120	$2,700,000	$60,000
10 years	240	$5,400,000	$120,000

At one time the corporate safe was hidden behind a picture in the CEO's office — today the most precious assets are information. The concern here is with the loss of confidential or proprietary information due to an uncontrolled virus attack. There is no way to measure the actual value of information rendered unrecoverable by a malware program, but the cost can be high.

According to the ICSA,[6] 36 percent of 300 organizations surveyed reported their servers were down for 1 hour or less, with the median downtime being 21 hours. A few respondents experienced longer recovery times up to 1,000 hours. More than 80 percent of those reporting a virus outbreak required 20 person-days or less to recover. The average cost was between $10,000 (median) and $120,000 (average) in estimated direct costs.

The sooner an infection is detected, the lower the cost of eradicating it and the lower the residual costs due to damage and data loss. Stopping viruses at the server, rather than removing infections from numbers of files on hundreds of workstations, will save thousands of dollars per incident. To calculate the cost of a virus outbreak to your organization, visit the Trend Micro Cost Analysis web site at: http://www.antivirus.com/products/smex/costanalysis.htm.

[6] ICSA Labs Sixth Annual Computer Virus Prevalence Survey 2000 (www.ICSA.net).