MCAFEE
Network Security & Management

White Paper

Current Computer Virus Threats, Countermeasures and Strategic Solutions

McAfee
2710 Walsh Avenue
Santa Clara, CA 95051
Tel: 408-988-3832
Fax: 408-970-9727

http://www.mcafee.com
Internet FTP: ftp. mcafee.com
BBS: 408-988-4004
America Online: MCAFEE
CompuServe: GO MCAFEE

Introduction

Contents:

About This White Paper

This paper presents a comprehensive overview of the current computer virus world, in light of the latest independent research and the most threatening new viruses.

The subject of computer viruses is one that seems to engender a great deal of media hype alternating with backlash periods during which public dialogue may attempt to minimize the virus threat. Yet, complacency about viruses puts all concerned at greater risk.

Therefore, as the leading provider of anti-virus software for desktop PCs and networked environments, McAfee recommends that a balanced and up-to-date understanding of virus realities is a necessary foundation for strategic anti-virus policies and procedures, and ultimately, the overall reduction of virus incidents. To that end, we developed *Current Computer Virus Threats, Countermeasures and Strategic Solutions.*

About the Author and McAfee Associates

Scott Gordon is McAfee Associates' product manager and primary spokesperson for anti-virus solutions. McAfee's anti-virus products claim over 68% market share for DOS, Windows and OS/2 unit sales, worldwide.[1] Founded in 1989, McAfee offers award-winning solutions for network security and management, including asset management, metering, electronic software distribution, storage management, remote access, security, enterprise service desk management and other client/server applications in addition to anti-virus software.

It Could Happen to You
(and probably already has)

Most people are aware that viruses spread via physical media such as diskettes and electronic methods such as e-mail. Unfortunately, many still believe that the circumstances of virus infection will somehow appear "suspicious" and that they will know when it is likely to happen. Here are just a few "real world" infection scenarios that may be all too familiar:

▶ John is working on a project after hours. He had transferred some information from a disk he borrowed from Bob, his co-worker. John turns his computer off and goes home. The next day, he returns to his desk and turns on his computer, forgetting to take Bob's disk out of the drive before starting up. His computer then displays the error message "non-system disk." Bob removes the disk, presses "enter" and his computer apparently continues to start normally.

But later that week, John is unable to access his hard disk drive, and he finds out that the disk borrowed from Bob was infected with a *boot virus*. Since John started his system up with Bob's disk inserted, John's computer is infected, too. The payload of this particular boot virus was to destroy the hard drive's file allocation table.

▶ Mary does a lot of her work on a home computer, which is also used by her daughter, Jill. Mary and Jill both enjoy playing a computer game that Jill had downloaded from the Internet as shareware, and Mary thought her co-workers would like the game, too. After she placed the game in a shared public directory on her company's network and posted a message to all her friends at work, the game became quite popular. Weeks later, complaints about missing files were increasing throughout the company, and the technical support department discovered that Mary's shareware game files were indeed infected by a *file virus*. This virus' payload was random deletion of files after a specified number of file reads.

▶ A coworker sends you an e-mail, attaching a recently modified expense document. You thought she was pretty savvy, but it turns out that this file was infected by a *macro virus*. It spread to your copy of the application the first time you opened the file. Now this application macro, in turn, can infect any document files you create, modify or save.

▶ A college instructor distributes disks to students as part of a class assignment. Unfortunately, the instructor was not vigilant about viruses and several students returned diskettes that carried virus infections from the homes and offices where the students worked on their assignments after hours.

▶ Software purchased from a retailer in shrink wrap is infected because the store re-wrapped returned software without checking the disks for viruses. (Apparently, the original buyer had tried out the software on an infected machine.)

The fact is, viruses are designed to proliferate. Every contact between your system and any other system is an opportunity for infection, including floppy disks and connections via network and modem.

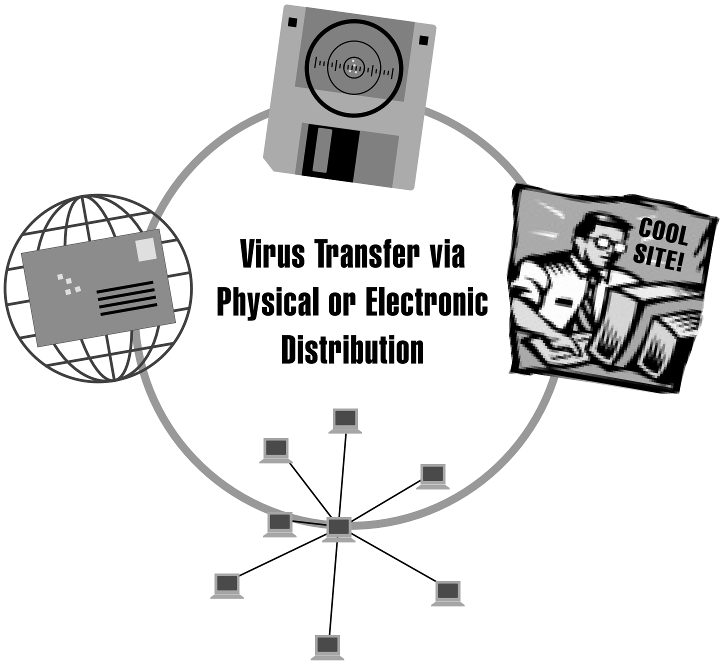
People who frequently use many different systems outside your organization are particularly likely to spread viruses. Three notorious examples are:

- ▶ Field service technicians
- ▶ Salespeople who run demonstration programs on your system
- ▶ Outside auditors who use their disks in your system (or, in some cases, connect their notebook computers directly to your network).

Even if you rarely encounter people of those occupations, you are at a higher-than-normal risk of spreading or encountering virus infections if any of the following descriptions apply to you:

- ▶ *Supervisor* –
  One who has access rights and responsibilities for other peoples' systems and data controls
- ▶ *Super User* –
  Advanced user who doesn't believe he/she is subject to infection…also often consulted by others for advice on or service of their systems
- ▶ *Globetrotter* –
  Nationwide or worldwide traveller who exchanges software and diskettes
- ▶ *Home Worker/Telecommuter* –
  User who shares a computer with other family members
- ▶ *Internet Junkie* –
  One who frequently downloads software from a variety of sites
- ▶ *Exchanger* –
  User who exchanges software with others
- ▶ *Tester* –
  One who tests pre-release versions of new software or updates

Today, of course, many people fit several of these high-risk definitions simultaneously.



Current Trends in Computer Viruses

Any computer, whether in an office, at a service provider, or a home, is susceptible to virus infection. The extensive (and constantly growing) PC networks in large organizations seem to be natural hotbeds of virus activity, and therefore a good subject for study on current and emerging trends.

One of the most ambitious recent studies of computer viruses in that type of setting was performed early in 1996 by the National Computer Security Association (NCSA), co-sponsored by McAfee and other members of the anti-virus community. The study consisted of interviews with key anti-virus system personnel in 2,300 organizations with at least 500 PCs installed. Some key results of the NCSA study follow…

Virus Prevalence

The computer virus problem is large and growing larger.

98% of large North American corporations (and other large organizations) have first-hand experience with virus infection. At the time of the study, about 90% of sites with 500 or more PCs reported going through virus encounters or incidents every month. Using a weighting formula, the NCSA concluded that, in large networked organizations, *the likelihood of experiencing a virus infection is about 1 chance per 100 PCs per month.*

(It should be noted that the term “virus incident” is herein and in the NCSA study defined as an “event in which a minimum of 25 PCs, diskettes or files were infected by the same virus at relatively the same time.”)

Is Perception Reality?

Organizations see little or no improvement to the virus situation in the past year.

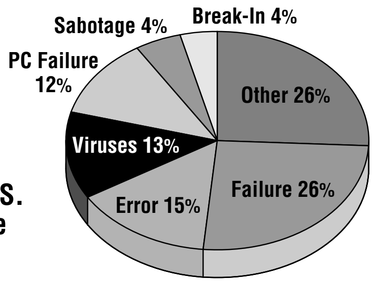
90% of respondents felt that computer virus problems are worse or no better than a year before. Some of the most detrimental virus effects were experienced with alarming frequency by responding organizations during the prior year, as follows:

Lost Productivity	81%
PC Downtime	71%
Damaged Data	59%
Lost Data	39%

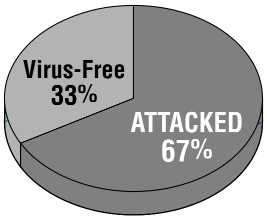
More Survey Highlights

- ▶ 30% of incident sites reported average server downtime of 5.8 hours due to a virus infection
- ▶ Over 70% of infections were traced to diskette distribution
- ▶ Over 46% of incident sites required more than 19 days to completely recover from a virus infection
- ▶ 37% stated incident costs of $1,999 or more
- ▶ Electronic distribution of viruses occurred in over 20% of reported cases
- ▶ Less than 35% of those surveyed use the full-time protection capabilities of their anti-virus software

In December 1995, just prior to this NCSA study, Ernst & Young surveyed 1,293 IT and Security executives. Results included the following statistics:



Virus damage ranks 4th among top IT financial loss issues.



A majority of U.S. companies were attacked in the past year.

Virus Growth

In less than a year, the growth of macro viruses such as "Word.Concept" was the most dramatic trend.

For several years, the most common virus was *Form* (a boot-sector virus). Rather suddenly in Summer 1995, *Word Macro* viruses (such as *Word.Concept,* also known as *Winword.Concept* or *Prank*) appeared, and by Fall Word.Concept had grown faster than any previous virus. By the time of the study in early 1996, Word.Concept was already three to four times more prevalent than *Form*. In the first two months of 1996, it was responsible for 49% of all virus encounters. (In July 1996, it was estimated there were already about 50 variant strains of Word Macro viruses.)

The rapid rise of Macro viruses is especially dramatic because it represents a whole new type of virus. Part of their "success" is that they infect an application's document files instead of executable program files or disk boot sectors. The distribution of documents is a far more common (and previously thought to be safe) practice than the distribution of programs, so macro viruses are more widely distributed. Another danger inherent in macro-based viruses is the ease of creation and modification by non-programmers. Previously, most virus creation was confined to programmers.

Compounding the problem is today's reliance on collaborative applications such as sending documents by e-mail and Lotus Notes. This practice allows file viruses and document-based macro viruses to travel and spread even faster.

The Emergence of Other Macro Viruses

Another entirely new category—still too recent for widespread statistical study—is also spread via document files from popular software.

Discovered in mid-July 1996, the new virus *Laroux* is the first Macro virus capable of infecting Microsoft Excel (versions 5 and 7) spreadsheets. Laroux can occur under Windows 3.x, Windows 95 and Windows NT operating systems, but so far Macintoshes can only act as carriers. The example of Word Macro viruses demonstrates how quickly macro-based viruses can grow, and with Excel's position as the world's most popular spreadsheet (for Macintoshes, as well), it seems only a matter of time before many more encounters are reported for a variety of applications.

Status of Viruses Today...

- ▶ 8,500+ known viruses, increasing by about 200 new viruses per month…yet, less than 200 account for most incidents
- ▶ Widespread growth of virus incidents surrounding collaborative applications, online services and Internet usage by both business and home users
- ▶ Anti-virus vendors report growth in the overall number of suspected virus-infected files received from their clients

Likely Trends of Tomorrow...

Based on observations and analysis by McAfee's Virus Emergency Response Center, the following trends appear very likely to materialize in the coming years:

- ▶ As virus growth has slowed to 40% annually, a prediction of 10,800 total viruses by the end of 1996 seems more realistic than previous estimates (the 50% growth rate of the past would have resulted in 12,300 viruses in that time period)
- ▶ Powerful new Native Windows 95 and Windows NT viruses will emerge in late 1996 or early 1997
- ▶ The Internet will take over as the predominant carrier of viruses by the middle of 1997
- ▶ Globally, more anti-virus laws will be enacted
- ▶ Macro viruses for even more applications, especially suite applications, will appear in 1997
- ▶ Standardized hardware platforms will enhance virus replication and transfer

The Cost of Virus Incidents

Even conservative estimates indicate widespread lost productivity and high costs.

True virus incidents (encounters involving a minimum of 25 PCs, diskettes, or files with the same virus at the same time), happened to 29% of the NCSA survey sites, and respondents were questioned about the effect on their organizations. As shown in previous studies, the most critical problem cited was operational disruption, which directly translates as lost productivity.

Once an organization discovers that it is experiencing a virus incident, it must begin the lengthy process of investigating suspect equipment, eradicating found viruses and then getting everyone back up to speed. (The average virus incident infected 135 PCs, according to NCSA survey results.)

Survey respondents were asked to compare the number of machines originally suspected to be infected with the number later confirmed as infected, with interesting results. *While relatively accurate in their estimates for infected PCs, respondents significantly underestimated the number of infected servers.* In relation to all viruses, the average suspected number of infected servers was 1.6; the number found to be infected was 5.4.

In estimating the cost of virus incidents, respondents were asked to consider a variety of factors, resulting in these facts:

- ▶ Average downtime for servers was 5.8 hours (actual downtimes reported ranged from zero to 320 hours)
- ▶ Recovery time averaged 44.3 hours and a total of an average of 10 person-days
- ▶ When asked to state the monetary cost resulting from the lost productivity, respondents averaged $8,106

Although this monetary estimate seems quite conservative, considering the time-factor responses, it is still clear that virus incidents are very costly.

The following table lists all reported virus incident results in order of response frequency:

Cited Results of Viruses

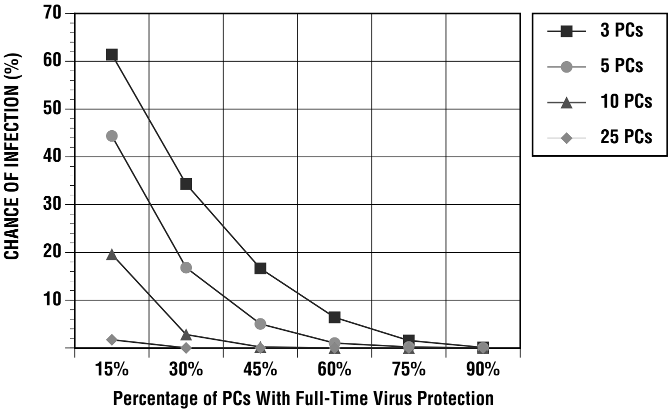
Lost productivity	81%
PCs unavailable	71%
Message lock-up	62%
Corrupted files	59%
Lost data access	49%
Lost data	39%
Unreliable applications	35%
System crash	30%
Loss of confidence	17%
None	4%
Threat of job loss	3%

Can Your Infection Risk Be Predicted?

The following infection risk estimates are from a McAfee co-sponsored virus cost model, extracted from the NCSA's 1996 Virus Prevalence Survey (available from McAfee and the NCSA). By implementing the complete features of reliable anti-virus software, one can dramatically reduce the risk of infection.

Chance of 3, 5, 10 and 25 PC Infections When X% Employ Full-Time, Background Anti-Virus Protection:

% PCs w/ full-time protection	Chance of 3 PC infections	Chance of 5 PC infections	Chance of 10 PC infections	Chance of 25 PC infections
15%	61.41%	44.37%	19.6%	1.72%
30%	34.30%	16.81%	2.8%	0.01%
45%	16.64%	5.03%	0.25%	0.00%
60%	6.40%	1.02%	0.01%	0.00%
75%	1.56%	0.10%	0.00%	0.00%
90%	0.10%	0.00%	0.00%	0.00%



What Is a Virus?

Computer viruses are programs which replicate themselves, attach themselves to other programs, and perform unsolicited and often malicious actions. *Self-replication* is the key trait that distinguishes viruses from other destructive programs. For instance, a *Trojan Horse* is a program which performs unsolicited actions, but it cannot replicate and spread on its own.

Viruses are destructive to productivity as well as data. An example of productivity damage is the *Stoned* virus which simply writes "Your computer is stoned" on the screen. Data damage is exemplified by the *Hare* virus (popularized in Summer 1996), which erases data from hard drives. In any case, viruses always cause some degradation of system resources, and some degree of wasted time for computer users. Since they are unsolicited and concealed, it does not seem accurate to call any virus "benign."

Critical to a virus' "success" is the ability to remain undetected for a long enough period to replicate and spread to new hosts. By the time the virus' presence is revealed, through unusual computer "behavior," damage to data or taunting messages, it usually will have been quite some time since the original infection took place.

This delay in time, between infection and manifestation, obviously makes it more difficult to trace the origin of the virus and/or the route it took to reach one's system. So delays are often made an inherent "feature" within a virus' design. A virus may monitor for a trigger event, which is a computer condition that, when it occurs, will cause the virus' *payload* to be delivered.

Examples of trigger events include dates (such as March 6 for the infamous Michelangelo virus), times, number of file saves or disk accesses, or file sizes. Specific keystroke sequences, in any predictable combination, can also be triggers.

A payload is an action performed by a virus—usually, but not always, the action that reveals the virus' presence. Examples of payloads include:

- "Amusing" or political messages (such as the *Nuclear* macro virus which asks for a ban on French nuclear testing)
- Prevention of access to one's disk drives (the *Monkey* virus)
- A stealth boot virus overwriting data as it attempts to write pre-infected boot information to another part of the disk
- Inconspicuous activity and minute data damage spread out over a long period of time—probably the most lethal type of virus effect (the *Ripper* virus)

Typical Signs that a Virus May Be Present:

- Unusual messages displayed
- Files are missing or have increased in size
- System operates slower
- Sudden lack of disk space
- Cannot access disk

Boot vs File Viruses

Before the inception and rapid proliferation of the Macro category, most IBM-compatible and Macintosh viruses fell into two basic categories: *Boot,* such as "Michelangelo" and *File,* such as "Jerusalem."

Boot viruses activate upon system start-up and are more common. They infect a system's floppy or hard disk and then spread (by replicating and attaching) to any logical disks available. *File* viruses are actually programs which must be executed in order to become active, and include executable files such as .com, .exe and .dll. Once executed, file viruses replicate and attach to other executable files. Since most viruses attach at the beginning or end of processes, their execution goes unnoticed.

Additional Virus Classifications

Other troublesome general virus sub-classes that are active today include *Stealth* (active and passive), *Multipartite, Encrypted, Polymorphic*, and *Macro.*

Stealth viruses (such as "Tequila") are difficult to detect because, as their name implies, they actually disguise their actions. Passive Stealth viruses can increase a file's size, yet present the *appearance* of the original file size, thus evading Integrity Checking—one of the most fundamental detection tactics. Active Stealth viruses may be written so that they actually attack installed anti-virus software (generic or brand-specific), rendering the product's detection tools useless.

Multipartite viruses, such as "Natas," have the characteristics of both boot and file viruses. "Cascade" is a well-known Encrypted virus. The challenge of Encrypted viruses is not primarily one of detection, per se. The encryption engine of this type of virus masks its viral code—making *identification,* as opposed to detection, more difficult.

The Polymorphic category ("SMEG" is an example) has grown considerably, presenting a particular detection challenge. Each polymorphic virus has a built-in mutation engine. This engine creates random changes to the virus' signature on given replications. Therefore, detection and prevention of recurring infections further requires frequent anti-virus component updates from a given vendor.

The New Macro Virus Threat

As discussed in the *Trends* section of this paper, Word Macro viruses have very suddenly become the most widespread category, and new Excel Macro spreadsheet viruses are an emerging threat. A macro virus is a set of macro commands, specific to an application's macro language, which automatically execute in an unsolicited manner and spread to that application's documents.

It is easier to create and modify Macro viruses than other virus types, and documents are more widely shared than programs, especially with instant e-mail distribution. It is also very easy to "catch" just by opening an infected Word document or template. The following factors appear to be key contributors to the alarmingly high growth rate of Macro viruses.

Macro Virus Dependencies:

- ▶ *Application Popularity –*
  The more common and "horizontal" the application, the greater the risk. More specialized or vertical market-specific programs aren't attractive enough to offer a large "breeding ground" for macro viruses.
- ▶ *Macro Language Depth –*
  The extent of the application's macro language affects a virus writer's ability to create a successful macro virus.
- ▶ *Macro Implementation –*
  Not all programs embed macro commands into data files. For instance, AmiPro documents will not necessarily contain "invisible" macro information. The easier it is to transfer and execute the macro from within the application, the faster the spread of the virus.

Major Virus Classifications:	BOOT			FILE			MACRO	
Sub-Classes:	Encrypted	Stealth: Passive or Active		Multipartite		Polymorphic	Application	
Examples:	*Cascade*	*Tequila*	*Michelangelo*	*Natas*	*Jerusalem*	*SMEG*	*Word.Concept*	*Laroux*

Current estimates recognize as many as 8,500 distinct viruses. Rate of growth is estimated at 100 to 200 new viruses each month.

Is It a Virus?

Viruses Are Often Blamed for Non-Virus Problems

As awareness of computer viruses has grown, so has the tendency to blame "some kind of virus" for any and every type of computing problem.

In fact, more cases of "not a virus" are encountered by customer support staff at anti-virus vendors than are actual virus infections, and not only with inexperienced users. Typical symptoms of viral infection such as unusual messages, screen color changes, missing files, slow operation, and disk access or space problems may all be attributable to non-virus problems.

Possible culprits include lost CMOS data due to a faulty system battery, another user's misuse, fragmented hard disks, reboot corruption, or even a practical joke. For instance, some PCs play the Happy Birthday song through their speakers every November 13. Sounds like a virus payload, but it happens only in computers containing BIOS chips from a certain batch that was sabotaged by a former programmer at the BIOS vendor. Switching out the BIOS chip eliminates the annual singing message.

Even deliberately written unwelcome programs are not always viruses...

As stated before, a multitude of hardware and software incompatibilities and/or bugs may cause virus-like symptoms, but there is also the in-between world of destructive, deliberately designed programs which still are not viruses. *Again, it is important to remember that the key distinction of viruses is their ability to replicate and spread without further action by their perpetrators.* Some non-virus programs are more destructive than many actual viruses.

Non-virus threats to user systems include *Worms*, *Trojan Horses* and *Logic Bombs*. In addition to the potential for damage these programs can bring by themselves, all three types can also be used as vehicles for virus program propagation.

Worms

Worms, often confused with viruses, infiltrate legitimate programs and alter or destroy data. Although a worm program cannot replicate itself, its damage can be great. For example, a worm program might instruct a bank's computer to transfer funds to an illicit account. However, once a worm invasion is discovered, recovery is relatively easy, as there is only one copy of the worm to destroy.

Trojan Horses

A Trojan Horse is a destructive program that comes concealed in software that not only appears harmless, but is also particularly attractive to the unsuspecting user (such as a game or graphics application). Named for the ancient myth in which Greek warriors invaded the gated city of Troy by hiding in a huge and beautiful wooden horse figure (which the Trojans took in believing it a peace offering), Trojan Horse computer programs can contain worm and/or virus programs. Trojan Horses are frequently used for embezzlement, and can be programmed to self-destruct, leaving no evidence aside from their damage.

Logic Bombs

Logic Bombs are a favored device for disgruntled employees who wish to harm their company *after* they have left its employ. Triggered by a timing device, logic bombs can be highly destructive. The "timer" might be a specific date (i.e., the logic bomb that uses Michelangelo's birthdate to launch "his" virus embedded within). An event can also be the designed-in trigger (such as after the perpetrator's name is deleted from a company's payroll records).

Anti-Virus Technologies

Without control of the "human element" and proper implementation, anti-virus software alone cannot provide full protection.

However, it is still the critical element in the fight against viruses. As stated before, non-virus problems may appear to be virus related, even to sophisticated users. Without anti-virus software, there is no conclusive way to rule out viruses as the source of such problems and then arrive at solutions.

Effective anti-virus software must be capable of performing three main tasks: *Virus Detection, Virus Removal* (File Cleaning) and *Preventive Protection*. Of course, detection is the primary task and the anti-virus software industry has developed a number of different detection methods, as follows.

Five Major Virus Detection Methods:

- ▶ *Integrity Checking* (aka *Checksumming*)—Based on determining, by comparison, whether virus-attached code modified a program's file characteristics. As it is not dependent on virus signatures, this method does not require software updates at specific intervals.

  Limitations—Does require maintenance of a virus-free Checksum database; Allows the possibility of registering infected files; Unable to detect passive and active stealth viruses; Cannot identify detected viruses by type or name.

- ▶ *Interrupt Monitoring*—Attempts to locate and prevent a virus' "interrupt calls" (function requests through the system's interrupts).

  Limitations—Negative effect on system resource utilization; May flag "legal" system calls and therefore be obtrusive; Limited success facing the gamut of virus types and legal function calls.

- ▶ *Memory Detection*—Depends on recognition of a known virus' location and code while in memory; Generally successful.

  Limitations—As in Interrupt Monitoring, can impose impractical resource requirements; Can interfere with valid operations.

- ▶ *Signature Scanning*—Recognizes a virus' unique "signature," a pre-identified set of hexadecimal code, making it highly successful at virus identification.

  Limitations—Totally dependent on maintaining current signature files (as software updates from vendor) and scanning engine refinements; May make false positive detection in valid file.

- ▶ *Heuristics/Rules-based Scanning*—Faster than traditional scanners, method uses a set of rules to efficiently parse through files and quickly identify suspect code (aka *Expert Systems, Neural Nets,* etc.).

  Limitations—Can be obtrusive; May cause false alarms; Dependent on the currency of the rules set.

All five techniques can usually perform *on-access* or *on-demand* scans, for both network servers and workstations. On-access scanning is analogous to a building's automatic sprinkler system—virus scanning is automatically initiated on file access, such as when a disk is inserted, a file is copied or a program is executed. On-demand scanning is more like a fire extinguisher—requiring user initiation (but may also be set up to continue scanning at regular intervals or at system startup).

Today, all effective products leverage a combination of detection methods because of the large number of virus types and their many tricks for invasion and disguise. Anti-virus software is a constantly evolving field, and as the knowledge base deepens, vendors can further refine these methods and develop even more effective future solutions.

Anti-Virus Policies and Considerations

The best anti-virus software in the world cannot protect you if it is not deployed systematically throughout the enterprise (even if "the enterprise" is a single home-based computer!).

Many people think they can dismiss a disk, shared or e-mailed file because it came from someone they know and trust. What they aren't considering is that their friend, colleague, customer or vendor is working on another system, with its own set of vulnerabilities from different outside conditions.

Computer users must recognize that the virus threat is too pervasive today to be ignored by anyone…the number of users who *never* come into contact with others' files is small and becoming smaller every day, especially with the tremendous growth of online services and Internet usage.

Therefore, McAfee strongly recommends that all computer users review the following as a starting point for effective anti-virus protection.

Basic "Safe Computing" Tips

▶ Use and update anti-virus software regularly.

▶ Scan any newly received disks and files before loading, opening, copying, etc.

▶ Never assume disks and/or files are virus-free.

▶ To help avoid boot viruses, do not leave diskettes in your computer when shutting it down.

▶ Change your computer's CMOS boot sequence to start with the *C* drive first, then the *A* drive.

For offices or homes with one or two computers, following these basic rules faithfully is probably adequate protection. However, in organizations with multiple PCs, especially in networks, a sound anti-virus strategy will necessarily be more complex.

This is because vulnerability to viruses increases in proportion to the number of machines, the extent of their interconnection, and the number of non-technical users who may view anti-virus vigilance as "someone else's job." (In contrast, a solo entrepreneur is likely to take the virus threat seriously because he or she will have to deal with infection results personally or pay an outside consultant.)

All organizations are different in the way they operate and the industries they serve, so no one anti-virus scheme is correct for all enterprises. However, at the very least, a company's program should include ongoing user education and a system for tracking virus activity (suspect and real) in addition to using anti-virus software.

Ultimately, your goal is to provide consistent, effective protection and a "damage control and recovery" plan for virus infections that may occur despite your efforts. In addition, and perhaps most importantly, you want to achieve this while minimizing any negative impact on staff productivity and system/network resources.

Therefore, to formulate a comprehensive anti-virus plan, it is necessary to first analyze the "big picture" of your organization along with its more detailed computing characteristics.

5 Key Factors in Anti-Virus Program Planning

1. The number and density of personal computers

The more PCs you have, or the higher the ratio of computers to people, the more you need a formalized, thoroughly documented anti-virus program.

2. The degree of interconnection between computers

"Interconnection" does not necessarily mean electronically networked. If data is frequently moved from one PC to another via diskettes or other media, those computers are effectively connected, whether they are separated by a few yards or many miles. Again, the frequency of data interchange may be as important as the methods of transfer.

3. How many locations are involved in the anti-virus plan

Assuming that multiple locations are involved because they are linked via data communications, more locations will require more coordination and reporting between the various IT staffs, as well as more user training.

4. The operational pace of the enterprise

Every organization has an inherent pace of operations, mostly dependent on the nature of its business. No matter how "busy" it is, a research laboratory's pace will not be as fast as that of a securities brokerage firm. In general, the faster the pace of operations, the greater the risk of virus infection because of the faster rate at which new data is being generated and distributed.

faster pace = more frequent new data = greater risk!

5. Whether there is a high level of transaction processing

If massive and timely data exchange is typical, the plan must yield the highest possible level of anti-virus security, along with comprehensive backup. Even weekly backups won't be adequate if vital data captured in real-time has been violated by a virus infection since the last backup.

Balance: Implementing Security by Function

Whatever the profile of your organization's computing characteristics and virus vulnerability, it is important to remember that anti-virus measures must be *balanced* in relation to the actual functions of various machines and their users.

Even within a specific location of the enterprise, there may be computers for which you need to sacrifice some level of anti-virus security in order to maintain necessary throughput and/or productivity. Cost is another factor that must be balanced against "ideal" protection levels, for all equipment and personnel in the organization.

Anti-Virus Implementation Questions

▶ Are there any PCs that should *not* be included in the anti-virus program? (For instance, computers that are isolated, diskless or used solely for manual data entry.)

▶ What special procedures should apply to the headquarters network, as opposed to branch offices?

▶ How should user reports of suspected virus activity be handled? What is a realistic (*vs* desired) response time?

▶ In response to an apparent virus infection, what procedures should users be authorized and trained to perform by themselves?

▶ How should suspected and/or actual virus infections, and resulting countermeasures, be recorded and reported? (It is important to log routine anti-virus scans as well as suspicious situations.)

▶ Who is responsible for maintaining these possibly exhaustive records?

▶ What improvements to existing backup procedures might be necessary? (Note that the common practice of rotating backup media might cause clean data to be replaced by infected data.)

▶ An anti-virus policy and procedures manual will need to be created and then maintained…who will take charge?

▶ How will you establish a "baseline" *virus-free environment* for the new anti-virus program to maintain?

▶ How will the schedule for adoption of a new virus control program be established? How will you balance simultaneous needs for speed *and* low cost?

▶ Who will provide the funding for the anti-virus program staff, development and software? Is upper management fully behind the program?

More Virus Prevention Tips

▶ Write-protect any data source diskette before inserting it in the drive, and then use anti-virus software to scan it before doing anything else.

▶ Include in your policy and training that employees who work on computers at home must follow the same anti-virus procedures they use at the office (whether on personal machines or company-supplied portables).

▶ Even with the above policy in place, handle disks brought back from employees' homes as foreign disks, following the write-protect and scanning procedure.

▶ Consider any suspicious computer behavior to be possibly virus-related and follow-up accordingly.

▶ Files that must be received from outside the organization, such as from the Internet, should be downloaded directly to quarantined scanning areas whenever possible.

▶ You may want to consider dedicating an isolated computer (not connected in *any* way to the network) to the task of testing all new files and/or diskettes. Then all files on the control machine can be systematically scanned for viruses before anyone has access to them. (Note that some compressed files may have to be decompressed before scanning.)

Take Advantage of Vendor Expertise

The larger your network, and/or the more sensitive your enterprise's data security position, the more you should seek guidance from industry peers and the anti-virus software industry *before* finalizing your plan.

Representatives from the leading vendors have experience in providing anti-virus solutions for many different kinds of distributed environments, in many different industries. Plus, their training programs and consulting services can be invaluable, helping to prevent both costly virus incidents and ensuring that your program is more cost-effective.

Evaluating Anti-Virus Vendors

Although anti-virus software companies design their products to detect and remove viruses, there is more to making a smart choice than comparing detection rates and/or product prices.

The fact that anti-virus software is necessary for everyone in the enterprise means that it must work alongside a variety of applications, and probably on multiple computing platforms within the location. Therefore, a common anti-virus product that can work "seamlessly" throughout the enterprise is desirable, for both cost-effectiveness and simpler administration.

The software must also be effective against the majority of common and damaging viruses, yet be as unobtrusive to productivity as possible. (Bear in mind that this is as important for user compliance as for the bottom line—if users feel hampered by anti-virus procedures they may "overlook" them in their haste to get work done.)

Another major factor to consider is the burgeoning number of viruses—as many as 200 new ones each month. Anti-virus software that does not include regular updates cannot provide adequate protection for long.

Primary Vendor Criteria

To ensure that you are providing the best possible solution, the anti-virus vendor you ultimately choose should satisfy the following primary criteria:

- *Technological Strength*—Demonstrably superior virus detection rates; leadership, quality assurance and timeliness in releasing new products and updates; Good grasp of technological trends that may impact your organization in the future.
- *Infrastructure*—Company resources in terms of financial health and strategic alliances to provide for ongoing development; Size and experience level of customer support staff; Size and scope of current user base; Ability to handle complex contracts smoothly.
- *Relationships*—Vendors who offer only technological strength, or excellent service with mediocre technology, will be inferior choices for an enterprise-wide anti-virus program. To get the most out of your anti-virus efforts, base them on software from a company that can sustain long-term relationships and provide excellent anti-virus technology.

While investigating anti-virus vendors and products, be sure to also assess these cost of ownership issues:

- Types of licenses available
- Variety of platforms supported
- Cost of updates for virus signatures and product releases
- Emergency services available
- Customer training (on and/or off-site)
- Consulting services available
- Maintenance agreements
- Contract terms and guarantees

In determining what is needed from the vendor, and the best contract arrangements, evaluators should also consider their in-house support and training resources, as well as the organization's growth potential and plans for introducing any new computing platforms.

Information Available from McAfee

For an in-depth study of the evaluation process for anti-virus solutions, including testing methodologies and criteria, see McAfee's white paper entitled *Evaluating Anti-Virus Solutions in Distributed Environments.*

Another tool available from McAfee is the *Virus Cost Model* developed in conjunction with the McAfee co-sponsored NCSA Virus Prevalence Survey. With this model, companies can actually analyze, estimate and calculate their virus risks based on real data. *(See Page 6 of this paper for an example.)*

Also new from McAfee is an interactive *Anti-Virus Tutorial*, developed with ViaGrafix.™ Containing information about the latest virus threats, answers to Frequently Asked Questions, Safe Computing How-to's and more, the tutorial may be purchased from McAfee or ViaGrafix.

Available at all times, and constantly being updated, is McAfee's World Wide Web site: http://www.mcafee.com. Information maintained on the site includes:

- *McAfee's Virus Emergency Response Center*—Maintained by industry-recognized McAfee virus researchers, experienced support staff and McAfee agents in over 65 countries around the world (more resources than any other anti-virus vendor).
- *McAfee's Virus Information Library*—

  VIRUS INFO LIBRARY

  A one-stop resource database that classifies each virus by name and type for quick and easy access. *InfoWorld* recently called it "Excellent." This library contains other virus information such as suggested remedies, new virus alerts, etc.
- *McAfee's Technical Documents*—The latest data sheets for all McAfee products, plus white papers, case studies and more. (For additional information on McAfee's products and services, see page 16 for other online forums.)

Other Resources

As mentioned before, computer users and technical management should also consult the valuable resource represented by peers from other organizations. Ask about their experiences in encountering and combatting viruses. Everyone involved in computing today can benefit from these shared experiences.

The National Computer Security Association (NCSA) serves both users and vendors by providing measurable industry standards in the form of anti-virus software certification. It also conducts periodic research studies on various aspects of viruses and other security issues, and promotes ongoing education of the anti-virus community.

The NCSA's effort to catalog all known viruses is assisted by more than thirty participants from several different countries, including major software vendors and independent researchers. The NCSA can be reached online at *www.ncsa.com.*

A leading independent database and catalog of thousands of viruses is maintained in *Patricia Hoffman's VSUM*. It contains detailed information on virus characteristics, including background of first encounters, how the viruses behave, and more. The VSUM online address is *www.vsum.com.*

Again, the anti-virus software industry can help in a multitude of ways…just ask, and you may be surprised at the wealth of information that is readily available.

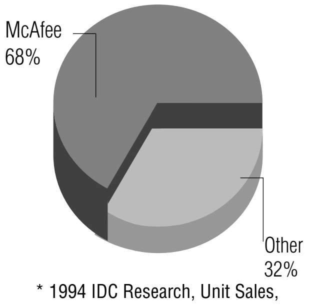
Why More People Trust McAfee

McAfee's huge installed base is more than an indicator of success—it's also a key to continued success in the fight against viruses.

McAfee currently has 68% worldwide unit market share for anti-virus software, according to IDC Research. VirusScan™ alone is used by more than 40,000 organizations. Millions of individual and corporate VirusScan customers and McAfee agents in over 65 countries enable us to analyze more viruses first and meet demands to resolve incidents quickly.

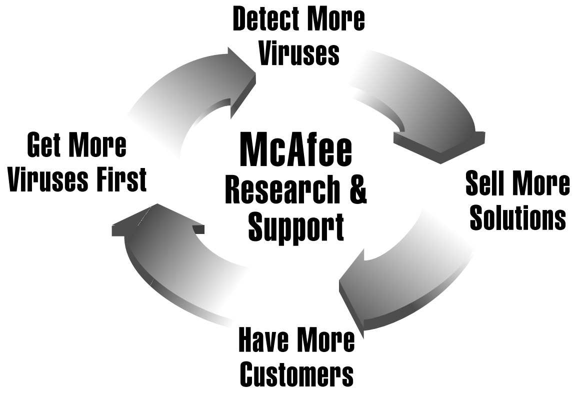
McAfee's tremendous installed user base and exhaustive testing, including NCSA and VSUM virus library certifications, provide our researchers with hundreds of suspect virus files per month and more opportunities to raise quality control and detection standards.

Worldwide Anti-Virus Market Share*

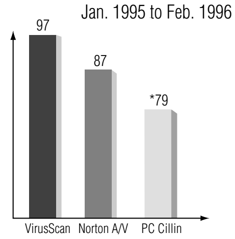


* 1994 IDC Research, Unit Sales, Windows, DOS, OS/2 Market

Success breeds success in the anti-virus fight…



Average Virus Detection Rates[†]



† VSUM DOS scanner published reports.
*PC Cillin results only published in Feb. 1996.

While virus detection rates will vary for all vendors month by month, McAfee's track record for high detection is consistently maintained.

Consistent virus detection and removal requires a sizeable staff of skilled and experienced virus researchers, engineers and support teams. McAfee is constantly expanding its capabilities—staffing with leading virus researchers, streamlining support mechanisms and designing groundbreaking virus extrapolation tools.

This customer-driven effort delivers significant monthly updates and the best reviews in the industry. VirusScan has consistently achieved over 96% VSUM detection rates.

Multiple Point Protection

McAfee's anti-virus solutions fight computer viruses at all points of entry—protecting your entire enterprise against damaged data and lost productivity. Current product offerings include:

- **VirusScan** *Top-Rated Desktop Protection* (Windows, Windows 95, Windows NT, OS/2, DOS, Macintosh, Solaris)
- **WebScan** *Web Browser & E-mail Protection* (Windows, Windows 95, Windows NT)
- **WebShield** *Internet Gateway Protection* (Windows, Windows 95)
- **NetShield** *Network Server Protection* (Windows NT, NetWare)
- **BootShield** *Real-Time Boot Virus Protection* (Windows, DOS)

Test for Yourself

If you have a modem, you have the opportunity to contact McAfee and test-drive McAfee products at any time—seven days a week, 24 hours a day. For an evaluation copy of any McAfee anti-virus product, just:

http://www.mcafee.com
Internet FTP: ftp. mcafee.com
BBS: 408-988-4004
America Online: MCAFEE
CompuServe: GO MCAFEE

Expertise Throughout the Enterprise

In addition to the industry's number-one anti-virus software, McAfee offers award-winning solutions for asset management, metering, electronic software distribution, storage management, remote access, security, enterprise service desk management and other client/server applications.

More than 80% of Fortune 100 companies use McAfee products—25% operating with enterprise-wide site licenses. Worldwide, more than 10 million people and 2 million-plus network nodes have McAfee software.

McAfee also offers an extensive array of professional services, including training programs and consulting. Even the largest, most complex global enterprises can find new ways to make their networks more secure and productive through these extended services from McAfee.

Notes

[1] IDC, 1995. VirusScan, WebScan, WebShield, NetShield, BootShield, Code Trace, Code Matrix and Code Poly are trademarks of McAfee, Inc. Other company and product names may be trademarks and are the property of their respective holders. Printed in the U.S.A. Part #WPAVSCCV0996