



Achilles' Shield™

A New Internet Security System for Protecting Networks and Computer Systems Against Viruses and Malicious Code

A Technology White Paper
From INDEFENSE, INC.
June 2000

TODAY'S COMPUTING WORLD:	3
THE GROWING SECURITY PROBLEM	3
HOW MALICIOUS PROGRAMS WORK	3
MORE ON VIRUSES	4
<i>Boot Sector Infection</i>	5
<i>Macro Infection</i>	5
<i>Executable File Infection</i>	6
WHY TRADITIONAL ANTI-VIRUS SCANNER TECHNOLOGY IS INEFFECTIVE	7
VIRUS SCANNERS	7
HEURISTIC SCANNERS	7
HOW ACHILLES'SHIELD WORKS	8
ACHILLES'SHIELD ARCHITECTURE.....	8
<i>First Barrier of Defense – Activity Monitoring and Damage Prevention</i>	8
File Viruses	8
Boot Viruses	9
Macro Viruses.....	9
Trojans and Worms.....	9
<i>Second Barrier of Defense - Detection</i>	10
File Viruses	10
Boot Viruses	10
Macro Viruses.....	10
<i>Third Barrier of Defense - Restoring</i>	10
File Viruses	10
Boot Viruses	10
Macro Viruses.....	10
ACHILLES'SHIELD COMPONENTS	11
<i>Active Components</i>	11
Real-Time Monitor	11
Outlook/Exchange Email Client	11
Avcheck/AvBlock/NTCheck	12
<i>Manual Components</i>	12
Task Manager	12
Rescue Disk	12
<i>Detector and Supporting Components</i>	12
Integrity Checker/Vaccinator.....	13
MacroDetect.....	13
Zip Manager.....	13
ACHILLES'SHIELD MACRO VIRUS SOLUTION	13
MACROS VIRUSES.....	13
<i>What is a Macro?</i>	13
<i>What is a Non-Automatic Macro?</i>	13
<i>What is an Automatic Macro?</i>	14
<i>What is a Macro Virus?</i>	14
ACHILLES'SHIELD MACRODETECT	15
<i>Achilles'Shield MacroPass</i>	16
<i>Achilles'Shield Macro Analyzer</i>	15
ACHILLES'SHIELD – AN ADMINISTRATION SECURITY TOOL	16
DISTRIBUTION	17
ADMINISTRATION	17
REPORTING.....	17

TODAY'S COMPUTING WORLD: Always-On means Always-Vulnerable

Today's computing environment is faster and more inter-connected than ever before. Businesses of every type are leveraging the capabilities of the Internet and corporate Intranets to streamline internal business processes and build closer connections with customers and suppliers. On a daily basis, these networks carry billions of transactions around the world, enabling users to conduct business, access information, and communicate in a fraction of the time these activities formerly required. And, while the growth of inter-networking has increased the resources available to individuals and enabled businesses to operate more effectively, it has also *exponentially* increased exposure and vulnerability to attacks from viruses, Trojans, worms and other malicious programs (malware).

The Growing Security Problem

Experts agree that the number of viruses and malicious programs is growing rapidly — from a few viruses a decade ago to more than 35,000+ cataloged viruses today — and more are being created daily (one estimate is that three to five new viruses are created every day). The most prolific type of virus — the macro virus — can be created easily even by non-experts. With the capabilities of the Internet and Intranets, macro viruses and worms can travel more widely and infect systems at an unprecedented rate. Many new types of viruses and worms are being spread through electronic mail, which can distribute them around the world within hours and days, rather than weeks and months.

As the threat of virus infection grows, so does the potential for virus damage. With networks providing the lifeblood of commerce today, disruptions affect more than a single user or installation. As businesses rely on the capabilities of the Internet to reach customers and business partners, systems become even more critical for business operations. For every business today, the potential cost of a prolonged system outage is high. Even if a virus does not actively disrupt operations, it occupies system memory and disk space, slowing system response and throughput and reducing productivity.

Recognizing the risk from malware, most MIS departments have implemented anti-virus software throughout their organizations. These solutions are typically anti-virus scanner programs that look for the signatures of viruses they know. Unfortunately, in today's online, always-on inter-networked environment, this anti-virus technology no longer delivers effective protection.

The evolution of computing and operating systems has produced an evolution in the creation and threat of malware. The threats have evolved from attacking only executables and boot sectors, to attacking macros in documents and data (with the introduction of the macro function in Word in 1995), to the hybrid malicious code (Melissa: part worm, part virus), to Trojans that enable Distributed Denial of Service (DDoS) attacks and create "backdoor" security holes. With new viruses spreading at Internet speed, this window of vulnerability between updates is the "Achilles' heel" of traditional scanners. Enter Achilles'Shield™ from InDefense, Inc.

How Malicious Programs Work¹

Although there are technical distinctions among malicious programs, the term "virus" is used to refer to malicious programs and includes viruses, Trojans and worms. The following section gives an overview of how each type works to infect a PC.

A **virus**, as distinct from a worm, is a computer program that makes copies of itself by using a host (much like a flea that needs a dog to survive, replicate, and transfer from place to place). A graphical example to explain how a virus parasitically attaches itself to a program is illustrated below.

¹ From, Ken Dunham, antivirus.guide@about.com, 6/17/99



The red area is where the virus attaches its code to the program during infection. The infected program now contains instructions for the normal program code and the virus code (red). When the infected program is executed, it activates normal program code as well as the virus code - normally resulting in more infections and spreading of the virus through the infected system. Some viruses, coined TSR, terminate and stay resident in memory - infecting other programs while you work.

A worm does not require a host; it is a program unto itself. The worm makes and distributes complete copies of itself once it infects a system, normally replicating at very high rates compared to viruses. Worms utilize network and internetwork infrastructures to spread. They either attach to and send email copies of the malicious code or utilize the file transfer capabilities of internetworking utilities. Contrasted to a parasitic virus-host type relationship, a worm program contains only the worm's own code as shown in the illustration below.



In conclusion, worms and viruses are very similar to one another but are technically different in the way that they replicate and spread through a system.

A Trojan horse is a program in which dangerous or harmful code is contained inside what is presented as a normal, useful program. Social engineering tricks the user into executing the program. Once executed, the program can install itself on the system and either gain control or grant access to external programs. Some Trojans cause system damage, such as ruining the file allocation table on your hard disk. Trojan horse programs don't replicate or reproduce themselves, as do viruses. However, in today's Internet world, rapid redistribution of a Trojan makes it considered a virus by the general population. (FYI: The term Trojan Horse comes from Homer's *Iliad*. In the Trojan War, the Greeks presented the citizens of Troy with a large wooden horse in which they had secretly hidden their warriors. During the night, the warriors emerged from the wooden horse and overran the city.)

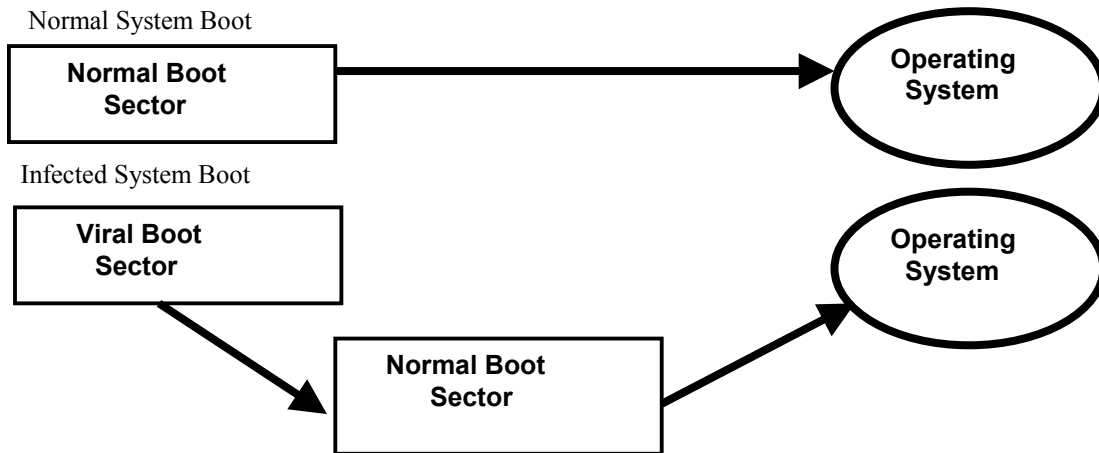
More on Viruses

There are three basic types or families of viruses: boot sector, executable file and macro. By definition, viruses are programs that replicate and attach to other programs. If a program does not fulfill these criteria, it is not a virus. To work, at all, viruses must be executed by some means. Thus, they can infect only executable code, such as the computer's boot sector, executable files, and macros. Viruses cannot be activated from pure data files. Viruses consist of two parts: the replication capability and the payload.

Because all viruses act in fundamentally the same way, it is possible to distinguish between normal modifications to executable files and viral modifications or behavior.

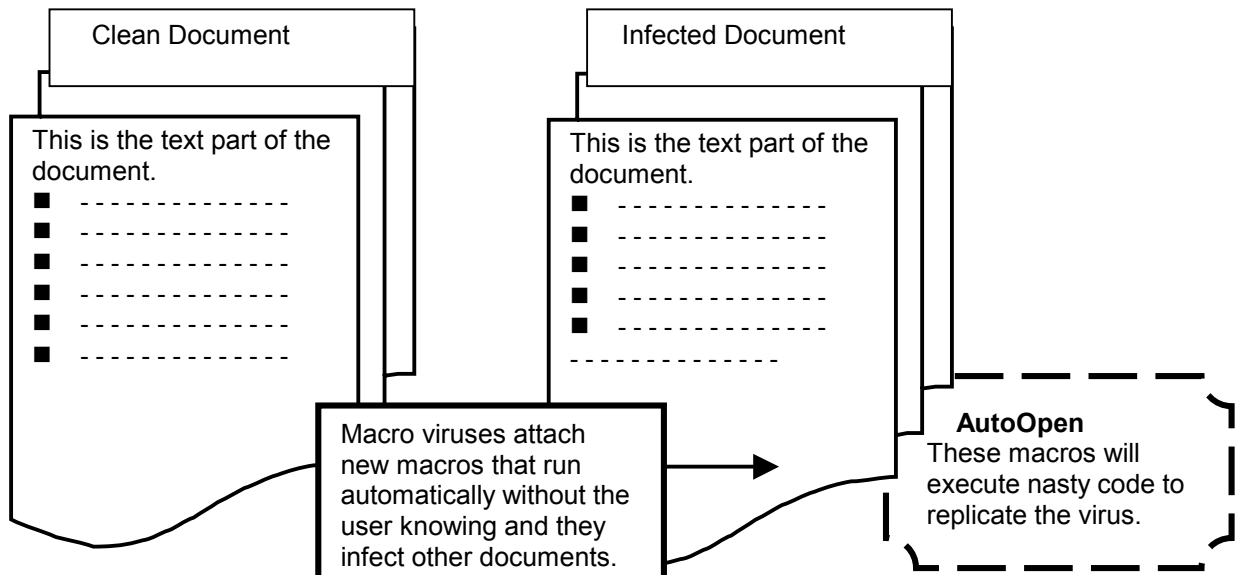
Boot Sector Infection

Boot sector infections typically work by executing the viral code when the system first boots then redirecting the boot up process to the normal boot sector to continue booting normally.



Macro Infection

An infected document has automatic macros added to it that are triggered by certain user-related events such as a File SaveAs or Document Close.



Executable File Infection

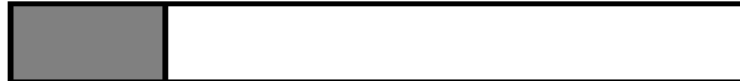
Consider the following clean executable file:



A normal modification (upgrade of an executable file) would look like this:



The same clean file would look like this if it were infected by a virus (viral modifications are marked in gray):



Why Traditional Anti-Virus Scanner Technology Is Ineffective

Anti-virus technology was developed for the computer environment of the mid-1980s. At that time, few viruses existed, and the Internet, far from the universal medium that it is today, was limited to government and academic institutions. Corporations used closed, proprietary networks, if they had any networking capabilities at all. The number of viruses was low and there were limited opportunities for passing them on.

Two common methods used in anti-virus programs are virus scanning and the heuristic scanner approach. Virus scanners characterize viruses by their “signatures,” which are stored in a database. Every file on the system is scanned for the presence of these signatures and if one is found, the virus is eradicated if possible. The heuristic scanner looks in program code for suspicious instructions, which are typical to viruses. Each of these methods has serious drawbacks.

Virus Scanners

The most obvious disadvantage of virus scanning is that it can only look for viruses that it “knows” or has the signature for — it cannot detect unknown viruses with any level of effectiveness. Coded and polymorphic viruses further reduce the effectiveness of scanning. Coded viruses are encrypted to disguise their signatures, while polymorphic viruses change their structure to avoid detection.

Suppliers of virus scanner software address this problem by continuously issuing anti-virus signature updates. As viruses spread at Internet speed, users relying on scanning technology are encouraged to update more frequently. However, updates — by definition — always lag behind the development of new viruses, limiting the usefulness of scanners in an inter-networked environment. In the case of the DDoS attacks that brought down Yahoo, EBAY, and other e-commerce sites early in 2000, the Trojans were used only once, so having the code in the database would offer little protection from the next DDoS attack.

Scanners are also costly to users, both in terms of the cost of anti-virus signature updates and the time required for their distribution. For large organizations, extensive effort is required to keep the anti-virus scanner up-to-date on every desktop. And, inevitably, as the number of identifiable viruses increases, so does the time required to scan files and the space required to store the scanner’s signature database. For instance, the signature database of the most common anti-virus scanner has increased in size more than fifteen times in the past two years.

Heuristic Scanners

Heuristic software extends the capabilities of scanners because it is not limited to a specific number of viruses it “knows”. However, this method doesn’t find all extant viruses nor does it eradicate them. Heuristic scanners can only detect suspicious instructions. They do not have enough information about the virus or enough information about the infected files to remove the virus or clean the file. The chief drawback of the heuristic anti-virus is that it gives many false alarms. The heuristic scanner can only affirm that a file “looks suspicious,” but not whether it is infected or not. Consequently, it generally takes some time, and the intervention of an expert, before it transpires that the alarm was false. This wastes a lot of time and leads to frustration on the part of the user. Typically, after a few false alarms users will disengage their anti-virus completely, thereby risking infection, rather than put up with the whole false alarm routine.

How Achilles'Shield Works

Achilles'Shield is the first commercially available Internet security solution that effectively defends against viruses and malicious code without requiring anti-virus signature file updates. Achilles'Shield's advanced behavior blocking technology detects malicious code by its behavior, and activity, not by its individual signature file. Achilles'Shield technology monitors and stops malicious activity at several system levels, including the boot record, CMOS, system registry, etc.

The Achilles'Shield approach is distinct from traditional anti-virus scanners in two key ways:

- (1) It is pro-active and preventative, rather than reactive, and
- (2) It has no database of virus definition files of "known" viruses that requires updating.

Achilles'Shield is both dynamic and intelligent in the way it acts, as it:

- Detects viral activity—the "dynamism" of viruses— rather than scanning or looking for static signature strings or suspicious instructions
- Adapts to the resident PC and its installed software rather than indiscriminately downloading a static library (database) of viruses.
- Deploys, in real-time, barriers or layers of defense appropriate to detect and stop the particular viral activity that is being exhibited.

To detect and eradicate malicious activity, Achilles'Shield simultaneously provides these features:

- "Smart" memory resident monitor
- Integrity checker
- Activity checker
- Macro detector module
- Advanced macro analyzer
- Rescue disk
- Multi-level password protections for network installations

Achilles'Shield Architecture

The Achilles'Shield components work together to provide three barriers of defense against viruses and malicious code.

First Barrier of Defense – Activity Monitoring and Damage Prevention

Achilles'Shield's first line of protection is a real-time activity-monitoring module that prevents viruses or malicious code from modifying the system or application program files. The Achilles'Shield Real-Time Monitor provides this protection. Because there is no signature database to search and very few associated I/O operations, the Real-Time Monitor occupies a very small segment of memory and has a negligible effect on response time and performance.

File Viruses

The memory resident module monitors the system for specifically viral behavior in executable files. Viral behavior includes:

- Modifying the code of an executable file
- Attaching additional code to an executable file
- Executing the attached code.

These three activities are initiated simultaneously when a virus activates.

Smart memory-resident monitoring is active whenever the computer is running and operates in the background. When file modification activity is detected, Achilles'Shield detects the modification and stops it, displaying an alert to the user. If the user chooses to deny the operation, the offending process is killed and the user is prompted and must decide whether or not to remove the offending program. If the user decides to allow the modification, the process is allowed to continue and the event is logged. If Achilles'Shield detects an operation that modifies a non-critical area of an executable file—and nothing else—it takes no action because the activity does not meet the criteria for being viral.

Malicious code can also be detected and prevented from entering the system by the Achilles'Shield email client add-in for Microsoft Outlook. Whenever an email attachment contains executable code, such as an executable program, VB script, or macro, an alert is issued and the user can remove the program or code.

Boot Viruses

When a user inserts and accesses a diskette that contains a boot sector virus into the floppy disk drive, Achilles'Shield checks the floppy, detects the infection and issues an alert.

The main cause of boot sector infection is rebooting to an infected floppy diskette. Achilles'Shield protects against this by checking for the presence of a diskette in the default floppy drive whenever the system is shutdown or restarted. If a diskette is detected, Achilles'Shield warns that there is a diskette in the drive and cautions the user to remove it.

Macro Viruses

Achilles'Shield provides active protection from macro viruses by examining each MS Office file accessed by the user for macros. The memory-resident module prevents any file operation from completing if the file contains uncertified macros. The user gets alerted to the "suspicious" macros and must either remove, certify, or ignore the macros before the file operation will complete.

The Achilles'Shield email client add-in for Microsoft Outlook also detects suspicious macros on the fly by detecting when Microsoft Office files are attached to emails. The add-in creates a quarantine area where the file can be examined by the Achilles'Shield MacroDetect component. Suspicious macros cause an alert and enable the user to analyze and remove the macro if necessary.

Trojans and Worms

Trojan and worm programs typically install themselves onto the system by copying code to the hard drive and altering system startup parameters so the malicious program starts when the system boots. Many malicious programs simultaneously access the system email component and attempt to send off copies of itself to addresses in the user's address book.

The Achilles'Shield Real-Time Monitor detects when certain startup parameters are altered, alerting the user and effectively stopping the process. The user can then decide to allow or deny the change based on the user's activity when the alert was issued. If the change is denied, the startup parameter is not changed and the program attempting the change is killed. The user is then prompted and given the opportunity to delete the offending program.

If a Trojan or worm accesses the system email component and uses Microsoft Outlook to send off multiple copies of the malicious code, Achilles'Shield email client add-in detects the executable code in the attachment and alerts the user giving them a choice to allow the attachment to be sent or to delete it. The user sees that an email is being sent that he did not create and can immediately delete the attachment.

Second Barrier of Defense - Detection

The second level of protection is provided by the Achilles' Shield detector components: the Integrity Checker/Vaccinator and MacroDetect.

File Viruses

The Integrity Checker/Vaccinator can be scheduled to examine executable and system files during system start-up or run manually by the user. The program compares system files with integrity information stored in vaccination files and detects any file modifications. The system's built-in intelligence distinguishes between the way viruses alter files and other normal file modifications. When a suspicious file modification is identified, the user is alerted and can choose to re-vaccinate the file, delete it, or bypass any action so the file can be replaced by a clean copy.

Boot Viruses

Boot sector modifications are detected when the system boots or when checked manually by the user. A DOS program, AVCHECK.EXE, compares the existing boot sector with an image of the original boot sector stored on the hard drive. Any changes to the boot sector are detected. Boot sector changes can be the result of viral modifications, hard drive failure or corruption, system upgrades, or BIOS modifications. The user sees an alert and is required to accept the changes or restore the system to its previous state.

Macro Viruses

The Achilles' Shield Task Manager's can be used to create and configured tasks that will check the hard drive(s) for Microsoft Office files that contain macros. These tasks can be configured to run when the system boots or at any desired interval or can be run manually. Documents that contain macros will be compared to a database of pre-certified macros and the list of macros certified by the user. If the document is in neither database, it is considered suspicious and the user is alerted. The user then has the option of removing the macros, certifying them or ignoring them.

Third Barrier of Defense - Restoring

Achilles' Shield's third or "safety-net" barrier consists of the Achilles' Shield MacroDetect, Integrity Checker/Vaccinator and the Rescue Diskette.

File Viruses

The Achilles' Shield Integrity Checker cannot restore files modified by viruses. Users are alerted and must be careful not to delete critical system files. Files modified in a suspicious way can be replaced manually by locating a clean copy of the file and copying it over the modified file. In some cases, an anti-virus scanning program can be used to attempt to clean the file.

Boot Viruses

An image of the clean state of the boot sector is stored on the active partition of the hard drive and on the Achilles' Shield Rescue Diskette. This location, outside of the computer, holds a faithful backup of the pristine system snapshot. It permits restoring the infected or corrupted boot sector and recovering from other types of mistakes or damage, thus permitting the unbootable system to boot.

Macro Viruses

Microsoft Office files infected by macro viruses will be restored to their clean state when the user instructs MacroDetect to remove the macros.

Achilles' Shield Components

The components that provide the multiple levels of protection can be divided into three classes:

- Active components
 - Real-Time Monitor
 - Outlook/Exchange Email client
 - AvCheck Boot-up program
 - AVBlock DOS TSR
- Manual components
 - Task Manager
 - Rescue Diskette
- Detector and supporting components
 - MacroDetect
 - Integrity Checker/Vaccinator
 - Zip Manager

Active Components

The Real-Time monitor and the Outlook/Exchange Email client stay active when the system is running and the components are enabled. AvCheck runs once each time the system boots to check for changes to the boot sector. AVBlock is loaded when the system boots and stays resident in memory to protect the system from low-level 16-bit DOS viruses. On Windows NT/2000 system, the 32-bit program, NTCheck.exe, provides the functionality provided by AvCheck in Windows 95/98 systems.

Real-Time Monitor

The Achilles' Shield Real-Time monitor is the cornerstone of the Achilles' Shield virus and malicious code protection system. Malicious activity occurs in the computer's memory whenever a viral or malicious program is executed. Preventing infection or damage is the best way of maintaining the system in a clean state. By monitoring activity in memory, the Real-Time monitor can:

- detect and prevent viral programs from modifying other executable or system files
- detect and prevent malicious programs from changing startup parameters
- detect and prevent malicious programs from creating new malicious executables on the hard drive
- detect and alert when suspicious macros are found in MS Office files during an active file operation
- detect when an infected floppy diskette is accessed and clean it
- detect and alert when the user attempts to shut down or restart the system with a floppy in the default floppy drive

The Real-Time monitor will allow viral or malicious programs to exist on the system in an inactive state but, when activated, will not allow them to replicate, install onto the system, damage the system, or spread to other systems via email.

Outlook/Exchange Email Client

The Achilles' Shield Outlook/Exchange Email Client is an add-in module for the Microsoft Outlook email client application. It enables the checking of email attachments for executable code, including standard DOS or Windows executables, Visual Basic (VB) scripts or suspicious macros, when sending or receiving email. The email client module intercepts all incoming and outgoing mail, checks each message to see if a

file is attached, and checks attached files to see if they contain executable code or if they are MS Office type files. If the attached file is a Microsoft Office file, the email client add-in creates and copies the file to a temporary directory where the MacroDetect then examines the files. MacroDetect alerts if a suspicious macro is found (see section below for a full description of MacroDetect and “suspicious” macros). If the attached file is any type of executable, the email client issues an alert. The user can answer “yes” to allow the attachment to be sent/received or “no” to delete it.

Avcheck/AvBlock/NTCheck

AvCheck is a detector module that runs from the AUTOEXEC.BAT file when Windows 95/98 systems first boot. The first time the module runs it takes a snap-shot of the system’s boot sector and stores the information in a file in the root of the active partition. On subsequent boots, when AvCheck runs, it compares the current boot sector with the stored snap-shot. If any modifications are detected, the user is alerted and can accept the changes or restore the boot sector to its original state.

AvBlock is a DOS TSR that also loads from the AUTOEXEC.BAT file on Windows 95/98 systems. The TSR stays active in memory and protects the system from infections caused by older 16-bit executable file viruses.

On Windows NT/2000 systems, NTCheck provides the same functionality as AvCheck, but runs after the system boots up and Windows loads. Viral file types that are targeted by AvBlock are not effective on Windows NT systems.

Manual Components

Manual components are designed for the detection and recovery of file and system modifications in case the Real-Time monitor is intentionally disabled.

Task Manager

The Achilles’Shield Task Manager allows the user to create and schedule customized tasks for checking the local system’s hard drives or mapped network drives for file modifications and suspicious macros. Some suggested tasks are created during installation. These can be modified and scheduled to run at startup or at any daily interval desired. Customized tasks can be created to check any combination of drives, files or folders using any of the following tools:

- MacroDetect
- Integrity Checker/Vaccinator
- Zip Manager

Rescue Disk

The Rescue Disk is used to recover from a modified or corrupted boot-sector that prevents the system from booting up. The Rescue Disk is either created during installation or manually and stores the boot-sector snap-shot created by AvCheck as well as the AvCheck program and system boot-up files. If the system becomes unbootable due to boot sector infection or corruption, the user places the Rescue Disk into the default floppy drive and boots to the floppy. AvCheck runs automatically and detects the modified boot-sector and prompts the user to repair it.

Detector and Supporting Components

The detector components are the Integrity Checker/Vaccinator and MacroDetect. These components are called from the Real-Time monitor when file activity is monitored in memory or by the Task Manager when scheduled or manual tasks are run. The Zip Manager is a supporting utility that enables the detector components to check files contained in compressed or archive files.

Integrity Checker/Vaccinator

During installation, the Integrity Checker/Vaccinator takes a snap-shot of all system and executable file types and stores the information in a small data file in each of the directories where those file types are found. The vaccination files average around 100 bytes per file vaccinated. When an executable is accessed or run, before closing the file, the Real-Time monitor checks the active file information against the information for that file stored in the vaccination file. If a modification is detected in a section of the file where viruses tend to infect, a backup of the unmodified state is made and the user is alerted and prompted to accept or deny the change. If the user denies the change, the file reverts back to its original state.

The Task Manager also accesses the Integrity Checker/Vaccinator when a task is run that is configured to use it. The user configures the Task Manager to check certain file types or all file types and the Integrity Checker/Vaccinator checks executable or system file types for viral modification.

MacroDetect

Please see the extensive section below on Achilles' Shield Macro Solution.

Zip Manager

The Zip Manager is a tool available to the Task Manager and the Outlook/Exchange email client add-in for checking files compressed into zip and other compressed file archives. When a zip file is checked, the Zip Manager creates a temporary directory and extracts files from zip and self-extracting zip files. The files are then sent back to the Task Manager or Outlook/Exchange client for file-type identification and checking by the appropriate detection module.

Achilles' Shield Macro Virus Solution

Because macro viruses are by far the most prevalent viruses found in the wild, this extended section addresses what a macro is, describes macro viruses and concludes with an outline of the Achilles' Shield solution to the macro risk.

Macros Viruses

What is a Macro?

A macro is a program written in an application's own language to automate the using of the application. Microsoft macros are written in Word Basic or Visual Basic for Applications (VBA) in Microsoft Office applications like Word and Excel. Macros are created to automate tasks and save time.

Users can create macros in MS Office applications either using a process called **recording a macro** or by manually editing VBA code. Recording a macro involves turning on the macro recorder (using the Tools/Macro feature) and performing the steps to be recorded. Either process can be used to create automated macros, which execute when a specific action is performed in the application.

What is a Non-Automatic Macro?

A non-automatic macro is a macro written in VBA that must be run manually. They are usually written for company or institutional tasks, which must be accomplished by groups or large numbers of users regularly or for specific projects.

What is an Automatic Macro?

(i.e., AUTOOPEN, FILESAVE, etc.)

An automatic macro is a macro that executes automatically on certain events, without the user needing to give a command to actively run or execute it. The specific event is indicated by the macro name – e.g., a macro called “FileSave” will execute automatically every time the user does a file save.

Note: There is a significant distinction between manually run and automatic macros. This distinction is the key to understanding the potential danger of macro viruses.

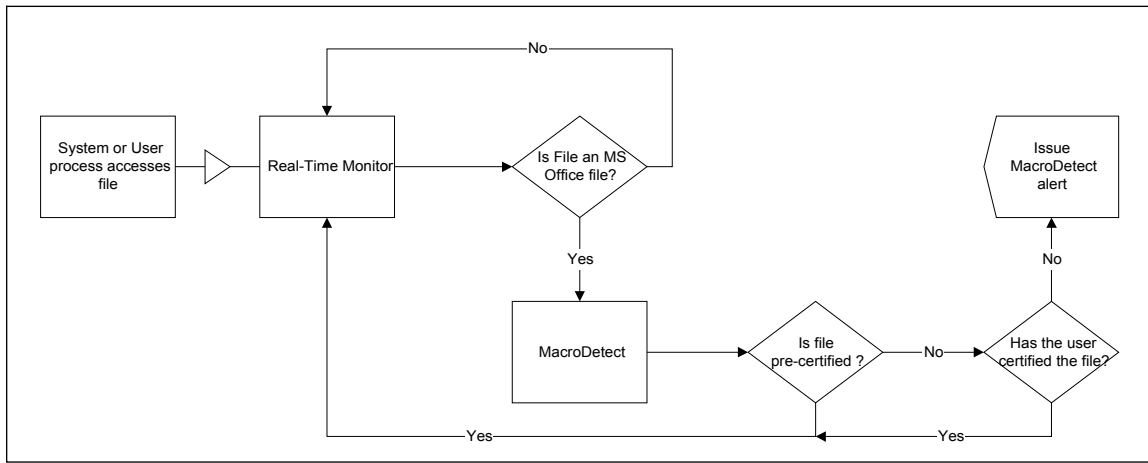
What is a Macro Virus?

A macro virus is a piece of macro code that is self-replicating. These programs or pieces of code are written in the application’s macro language (VBA in the case of MS Word and MS Excel). Macro viruses typically write or copy automatic macros to the default template in MS Word or create a default spreadsheet in MS Excel. The macros are then designed to infect any document or spreadsheet opened or created. In some cases they will remove existing macros and insert their own automatic macros. Macro viruses that cause damage contain a “jump start” or “trigger” that activates a “payload” or “damage routine” that can be annoying or possibly destructive. The “jump start” is a cause (remember, these are automatic macros) that the virus writer has programmed the virus to look for, such as a date or time elapsed, etc.

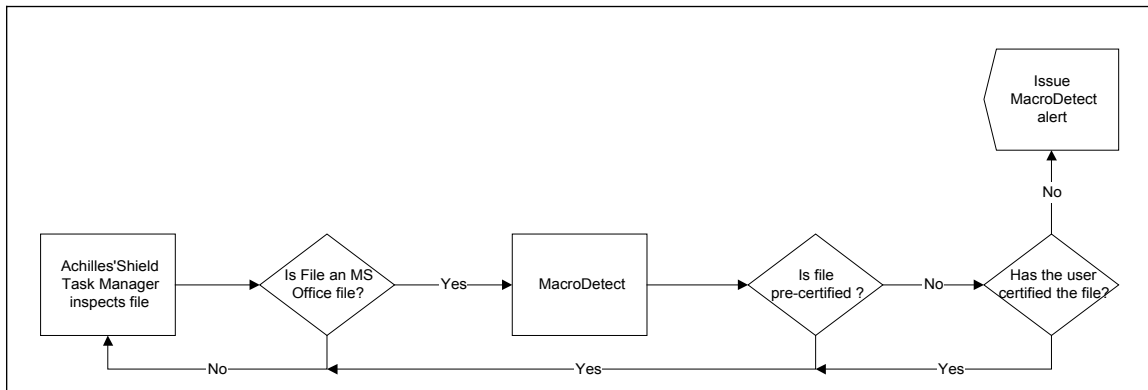
Achilles'Shield MacroDetect

Achilles'Shield MacroDetect is a detector component specifically designed to detect macros contained in Microsoft Office file types. The MacroDetect component is called either from the Achilles'Shield memory resident module or from the Achilles'Shield Task Manager.

The memory-resident module detects and sends any MS Office file types to MacroDetect whenever they are accessed. MacroDetect checks to see if the file is in the pre-certified or certified databases. If the file is not certified, then MacroDetect issues an alert. If the user chooses to certify the file, a CRC of the file is taken and the file name and CRC information are added to the certified database. The same file with the same name will not be alerted when the file is accessed again regardless of where the file is located on the system.



When a task using the MacroDetect tool is run from the Achilles'Shield Task Manager, as folders are accessed, the Task Manager examines each file to determine if it's a MS Office file. If it is a MS Office file, it gets sent to MacroDetect and follows the same sequence as described above.



Achilles'Shield Macro Analyzer

Often users don't use macros or even know what they are. At first look, it can be difficult for the average user to determine if a macro causing an Achilles'Shield alert should be removed or certified. To help the users out, InDefense developed the Macro Analyzer. This module examines the macro code contained in suspicious macros and generates a report indicating what actions the macros will take if executed. This

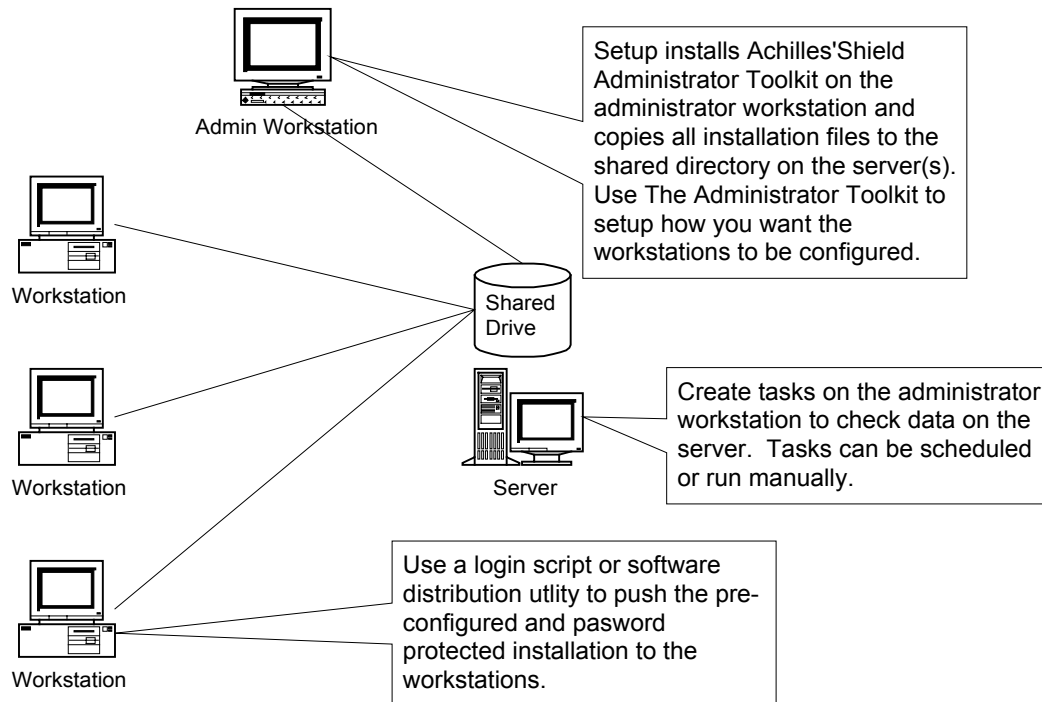
makes it very easy for even a beginning computer user to see whether or not suspicious macros are viral in nature so he or she can eliminate them.

Achilles'Shield MacroPass™

In order to minimize the alerts issued by MacroDetect on safe macros distributed by well-known application vendors (including Microsoft), InDefense distributes a database of files containing macros deemed safe. Individual users can use the Achilles'Shield MacroPass utility to add new macros or their own macros to the pre-certified database. MacroPass takes a Cyclic Redundancy Check (CRC) of the macro code contained in files being added and stores that information. Whenever MacroDetect examines a file, it first checks to see if the CRC of the active file matches any of those contained in the pre-certified database. If a match is made, no alert is issued and control is passed back to the active process. The user can add macros to MacroPass for distribution to other computers. MacroPass is an important component of the Achilles'Shield Administrator's Toolkit, which is used for configuring and distributing Achilles'Shield throughout a business network.

Achilles'Shield – An Administration Security Tool

The Achilles'Shield approach to protecting a business network is to automatically distribute Achilles'Shield to network-attached workstations and then provide administrators with a tool for defining how they want the client software configured and how much user access will be allowed to the program. The administration tool allows system administrators to define the network's policy for automatic macros and allows them to be in control of the company documents' integrity, thus ensuring total protection against macro viruses. Centralized reporting allows administrators to easily view and monitor suspicious activity throughout the network.



Distribution

The figure above shows the distribution and configuration process suggested for network installations. The process can be broken up into 3 steps:

1. Install Achilles'Shield and the Administrator's Toolkit on the administrator's workstation.
2. Use the Administrator's Toolkit to setup the workstation installation and configuration parameters and to configure the amount of control of the program to be granted to users. Create groups of users and configure each group accordingly. Create a path for centralized reporting to enable simple monitoring of suspicious network activity. Also, pre-certify all internally acceptable macros not already contained in the pre-certified database using MacroPass. Distribute the installation files and workstation parameters to shared network folders on one or more servers.
3. Distribute the software to the workstations either manually or automatically using a login script or a software distribution utility.

Administration

The Achilles'Shield Administrator's Toolkit is constantly available on the administrator's workstation for making changes to workstation setup parameters, centralized report path, control settings and the administrator password or message. Changes are distributed to network-attached workstations each time Achilles'Shield loads on the workstation, provided the login is successful .

Reporting

The Toolkit also provides the ability to create and access a centralized report. Any alerts or errors generated on the workstations will be logged into the central report. Centralized reporting is a useful administrative tool for monitoring malicious code activity on the network.

About InDefense, Inc.

Headquartered in the Silicon Valley, with offices in Santa Cruz, California and Toronto, Ontario Canada. InDefense, Inc. is an expert software development firm specializing in Internet security solutions, including virus protection and data security. The company's flagship product, Achilles'Shield™, is the follow-on to InDefense Virus Protection System™, a uniquely designed Windows-based software program that defends networked and stand-alone PC's from viruses carried by the Internet, e-mail, LANs, and diskettes. The critically acclaimed InDefense was the only non-scanner-based product of its kind to be certified under West Coast Labs' demanding Checkmark Level I independent testing methodology for virus and malicious code protection solutions.

Copyright Information: © 2000 InDefense, Inc. InDefense and Achilles'Shield are trademarks of InDefense, Inc. Microsoft Word and Microsoft Excel are U.S. registered trademarks of Microsoft Corporation. Windows, Windows 95, 98, 2000 and Windows NT are trademarks of Microsoft Corporation.