



# Agency Guide to Information Security Incident Response



When a security incident is confirmed by the Security Operations Center (SOC) at the South Carolina Information Sharing and Analysis Center (SC-ISAC), SOC will send an e-mail notification to the affected agency's "securityalerts@agencydomain" e-mail distribution list. This distribution list is maintained by the agency and may include multiple recipients, but must *always* include the agency IT Director and Security Officer. The notification includes preliminary response measures recommended by SOC, which are assigned based on an initial assessment of the incident's severity. The response measures are classified by a tier system numbered 1-5. Below is an explanation of each tier and its recommended response.

1. A Tier-5 response recommendation indicates that malicious code or software has been detected on an agency machine, but it is not fully compromised and there is no risk of sensitive information loss.
  - 1.1. **Scenario:** An employee has picked up spyware or adware through routine Internet browsing.
  - 1.2. **SOC Procedure:** SOC observes the event and determines the adware has no capability to steal data. SOC classifies the incident as Tier 5 and sends notification of the incident to the Security Alerts distribution list for the affected user's agency.
  - 1.3. **Recommended response for a Tier-5 incident:** Agency IT personnel will use tools to attempt to clean the machine, place the machine back in service, and document the updated IP address. Agency IT will provide the IP address to the SOC so the SOC can keep the IP address on a watch list for 48 hours to monitor any further malicious activity.
2. A Tier-4 response recommendation indicates that the affected machine is fully compromised; meaning that a malicious user has obtained unauthorized administrative control over the machine, but there is no immediate risk of sensitive information loss.
  - 2.1. **Scenario:** An employee who works in the agency Public Affairs department has received an e-mail from a friend that appears to be legitimate. She opens the e-mail and clicks the link, which contains malware that installs modules on her computer. The installed modules allow a remote user to obtain administrative access to the machine. Once administrative access has been obtained, the user has access equivalent to that of the employee's and is able to use the employee's fully compromised machine to send out more e-mails containing the malicious code, which may reach and affect other agency computers.
  - 2.2. **SOC Procedure:** SOC observes the event and determines the machine is fully compromised by the malware. Since SOC is familiar with this agency's network, the analyst knows the affected user works in Public Affairs and has no access to sensitive information. He classifies the incident as a Tier 4 and sends immediate e-mail notification to the Security Alerts distribution list for the affected user's agency.

- 2.3. **Recommended response for a Tier-4 incident:** Agency IT personnel will wipe the hard drive and re-image in accordance with agency incident response procedures. Agency IT should not attempt to clean the machine. Any passwords used on this machine must be changed. After following these steps, agency IT personnel should re-establish contact with SOC to confirm the issue has been resolved.
3. A Tier-3 response recommendation is both an incident notification and a request for agency assistance. The Tier-3 designation indicates that a machine is fully compromised and there is a possibility that sensitive information could have been accessed or lost. Further investigation by the agency is required to determine if the affected user had access to sensitive information. **An incident should never stay classified as a Tier 3; it will either be escalated to a Tier-2 if the agency reports sensitive information was definitely or potentially involved, or downgraded to a Tier-4 if the agency reports no sensitive information was involved.**
- 3.1. **Scenario:** While browsing the Internet, an employee sees a pop-up that tells them malware has been found on their computer and if they click the pop-up, they can install a program to remove it. (This is a common example of a Trojan horse—a malicious program disguised as something legitimate.) The employee becomes concerned and clicks the link in the pop-up, which downloads the malicious program, and the program begins to search for vulnerabilities in the employee's computer. When it finds one, it downloads more malicious code that will allow a remote user to exploit the vulnerability in order to obtain administrative access to the machine. Once administrative access has been obtained, the user has access equivalent to that of the employee's and is able to download agency data and send it to another location.
- 3.2. **SOC Procedure:** SOC observes the event and determines the machine is fully compromised by the Trojan/Multi-stage dropper and information could have been lost. He classifies the incident as a Tier-3 and sends immediate e-mail notification to the Security Alerts distribution list for the affected user's agency.
- 3.3. **DSIT Help Desk Procedure:** For Tier-3 incidents, the DSIT Help Desk will assist SOC in making sure the agency provides the needed information within the appropriate time frames. Agencies that do not respond within to the initial notification within 60 minutes will receive phone and e-mail communication from the Help Desk operator to ensure the agency is in contact with SOC and taking the appropriate remediation measures. If an agency does not communicate with SOC regarding escalation or downgrading of the incident within 24 hours, the Help Desk will contact the DSIT Director to notify him of the agency's inactivity.
- 3.4. **Recommended response for a Tier-3 incident:** Agency IT personnel will locate the affected machine, interrupt the user, and determine if there is any access to sensitive information from the affected system. If the affected user has access or potential access to sensitive information, agency IT will contact SOC within 24 hours of receipt of the initial ticket to escalate the incident

to a Tier-2. If escalated, agency IT will not proceed to forensic/mitigation activities without authorization and direction from appropriate parties. If the affected user does NOT have access to sensitive information, agency IT will contact SOC within 24 hours of receipt of the initial notification to downgrade the incident to a Tier-4 and follow the appropriate remediation procedures.

4. A Tier-2 response recommendation indicates that the affected machine is fully compromised and network traffic suggests that information has been lost. A Tier-2 designation is made when the information lost is potentially or definitively sensitive in nature.
  - 4.1. **Scenario:** Return to the scenario from the Tier-3. The employee whose computer was compromised by the Trojan/Multi-stage dropper works in the Human Resources department. This particular employee has access to HR databases and SCEIS roles that allow access to the personal information of all agency employees.
  - 4.2. **SOC Procedure:** If SOC observes the event and can determine without agency assistance that a compromised machine has access or potential access to sensitive information, the analyst will classify the incident as a Tier-2 and send immediate e-mail notification to the Security Alerts distribution list for the affected user's agency. If the incident is a Tier-3 that was escalated to a Tier-2 based on agency confirmation of the user's access to sensitive information, the analyst will update the ticket and advise the agency to follow the recommended response for a Tier-2 incident.
  - 4.3. **DSIT Help Desk Procedure:** For Tier-2 incidents, the DSIT Help Desk will assist SOC in making sure the agency provides the needed information within the appropriate time frame. Agencies that do not respond within to the initial notification within 60 minutes will receive phone and e-mail communication from the Help Desk operator to ensure the agency is in contact with SOC and taking the appropriate remediation measures. Due to the potentially serious nature of Tier-2 incidents, the Help Desk operator may assist SOC by periodically contacting the agency for status updates regarding unresolved Tier-2 incidents.
  - 4.4. **Recommended response for a Tier-2 incident:** Agency IT should respond immediately to SOC to acknowledge receipt of the notification and begin forensic/mitigation activities. Agency IT personnel will locate the affected machine and interrupt the user. The user will not be allowed to close anything or have any more interaction with the workstation. Agencies not covered by the MIR device will run the supplied SOC volatile memory preservation script/utility while machine is still on the network. Then unplug the machine, remove the hard drive, and initiate chain of custody procedures. Agency security officer or designee will bring the hard drive and chain of custody form to SC-ISAC for analysis when requested or seek forensic analysis services from local law enforcement.

- 
5. A Tier-1 response recommendation indicates a very serious incident of a criminal nature, usually brought to the attention of SOC through law enforcement agencies (SLED, FBI, Secret Service, etc.) Due to the extremely sensitive and often confidential nature of Tier 1 incidents, agencies will never receive a Tier 1 incident notification from SOC through e-mail. An incident of this magnitude is out of the purview of SOC and agency IT and will be handled by the appropriate authorities, which may include federal, state, or local law enforcement.
    - 5.1. **Scenario:** SLED has discovered that a state agency machine has been compromised and used by a third party to commit criminal activity, such as the theft and sale of personal information.
    - 5.2. **SOC Procedure:** SLED will notify SOC of the finding and coordinate with SOC to perform all necessary forensic investigation of the incident.
    - 5.3. **Recommended response for a Tier-1 incident:** All response procedures will be handled by the appropriate law enforcement agency with SOC assistance. The agency should be ready to provide any information requested by SOC and law enforcement personnel.

## GLOSSARY OF TERMS

Below is a glossary of common terms encountered when reading about or discussing information security.

### A

#### **ActiveX**

ActiveX controls are software modules based on the Microsoft® Component Object Model (COM) architecture. They add functionality to software applications by seamlessly incorporating pre-made modules with the basic software package. Modules can be interchanged but still appear as parts of the original software.

On the Internet, ActiveX controls can be linked to web pages and downloaded by an ActiveX-compliant browser. ActiveX controls turn web pages into software pages that perform like any other program launched from a server. ActiveX controls can have full system access. In most instances this access is legitimate, but one should be cautious of malicious ActiveX applications.

#### **Adware**

Adware is a legitimate, non-replicating program designed to display ads to the end user, often based on monitoring of browsing habits, and often in exchange for the right to use a program without paying for it (a take on the shareware concept).

#### **Algorithm**

An algorithm is a sequence of steps needed to solve logical or mathematical problems. Certain cryptographic algorithms are used to encrypt or decrypt data files and messages and to sign documents digitally.

#### **Anti-antivirus virus**

Anti-antivirus viruses attack, disable, or infect specific anti-virus software. Also see: retrovirus.

#### **Anti-virus software**

Anti-virus software scans a computer's memory and disk drives for viruses. If it finds a virus, the application informs the user and may clean, delete, or quarantine any files, directories, or disks affected by the malicious code. Also see: anti-virus scanner.

#### **Anti-virus virus**

Anti-virus viruses specifically look for and remove other viruses.

#### **Applet**

An applet is any miniature application transported over the Internet, especially as an enhancement to a web page. Authors often embed applets within the HTML page as a foreign program type.

Java applets are usually only allowed to access certain areas of the user's system. Computer programmers often refer to this area as the sandbox.

## Armored virus

An armored virus tries to prevent analysts from examining its code. The virus may use various methods to make tracing, disassembling, and reverse engineering its code more difficult.

## ASCII

ASCII stands for American Standard Code for Information Interchange. Usually, it refers to a coding system that assigns numerical values to characters such as letters, numbers, punctuation, and other symbols.

Basic ASCII allows only 7 bits per character (for a total of 128 characters). The first 32 characters are "unprintable" (line feed, form feed, etc.). Extended ASCII adds an additional 128 characters that vary between computers, programs and fonts. Computers use these extra characters for accented letters, graphical characters or other special symbols.

## ASCII files

ASCII files are usually text files consisting of only ASCII characters. With effort, it is possible to write program files consisting only of printable characters. Windows® batch (BAT) files and Visual Basic Script (See: Batch Files, VBS) files are also typically pure text, and program files.

Because of the danger macro viruses can pose, using ASCII files in email communications may be less risky. While it is possible for ASCII files to contain program code, and thus to contain viruses, ASCII files let you control both content and layout exactly, ensuring your email is legible by the most email programs.

## Attack

An attack is an attempt to subvert or bypass a system's security. Attacks may be passive or active. Active attacks attempt to alter or destroy data. Passive attacks try to intercept or read data without changing it. Also see: brute-force attack, Denial of Service, hijacking, password attacks, password sniffing.

## Attributes

Attributes are characteristics assigned to all files and directories. Attributes include: read-only, archive, hidden, or system.

## B

### Back door

A back door is a feature programmers often build into programs to allow special privileges normally denied to users of the program. Often programmers build back doors so they can fix bugs. If hackers or others learn about a back door, the feature may pose a security risk. This is also called a trap door.

### Background scanning

Background scanning is a feature in some anti-virus software to automatically scan files and documents as they are created, opened, closed, or executed.

### Background task

A background task is a task executed by the system that generally remains invisible to the user. The system usually assigns background tasks a lower priority than foreground tasks. Some malicious software

is executed by a system as a background task so the user does not realize unwanted actions are occurring.

## **Backup**

n. A backup is a duplicate copy of data made for archiving purposes or for protection against damage and loss.

v. A backup is also the process of creating duplicate data. Some programs back up data files while maintaining both the current version and the preceding version on disk. However, a backup is not considered secure unless it is stored in a location separate from the original.

## **Batch files**

Batch files are text files containing one MS-DOS command on each line of the file. When run, each line executes in sequential order. The batch file AUTOEXEC.BAT is executed when the computer is booted, and it loads a series of controls and programs. This file type has the extension BAT.

## **Bayesian filter**

A Bayesian filter is a program that uses Bayesian logic (also called Bayesian analysis) to evaluate the header and content of an incoming email message to determine the probability that it constitutes spam.

## **Bimodal virus**

A bimodal virus infects both boot records and files. It is also called a bipartite virus. Also see: boot-sector infector, file virus, multipartite.

## **BIOS**

BIOS stands for Basic Input/Output System. It is the part of the operating system that identifies the set of programs used to boot the computer before it locates the system disk. The BIOS is located in the ROM (Read-Only Memory) area of system and is usually stored permanently.

## **Boot**

To boot a computer is to start (a cold boot) or reset (warm boot) the system so it is ready to run programs for the user. Booting the computer executes various programs to check and prepare the computer for use. Also see: cold boot, warm boot.

## **Boot record**

The boot record is the program recorded in the boot sector. This record contains information on the characteristics and contents of the disk and information needed to boot the computer. If a user boots a PC with a floppy disk, the system reads the boot record from that disk. Also see: boot sector.

## **Boot sector**

The boot-sector is an area located on the first track of floppy disks and logical disks that contains the boot record. Boot sector usually refers to this specific sector of a floppy disk, whereas the term master boot sector usually refers to the same section of a hard disk. Also see: master boot record.

## **Boot sector infector (BSI)**

A boot-sector infector virus places its starting code in the boot sector. When the computer tries to read and execute the program in the boot sector, the virus goes into memory where it can gain control over basic computer operations. From memory, a boot-sector infector can spread to other drives (floppy,

network, etc.) on the system. Once the virus is running, it usually executes the normal boot program, which it stores elsewhere on the disk. It is also called a boot virus, boot-sector virus, or BSI.

## **Bot network (Botnet)**

A bot network is a network of hijacked zombie computers controlled remotely by a hacker. The hacker uses the network to send spam and launch Denial of Service attacks, and may rent the network out to other cyber criminals. Also see: zombie.

## **Browser hijacker**

A browser hijacker is a type of spyware that allows the hacker to spy on the infected PC's browsing activity, to deliver pop-up ads, to reset the browser homepage, and to redirect the browser to other unexpected sites. Also see: spyware.

## **Brute-force attack**

A brute-force attack is an attack in which each possible key or password is attempted until the correct one is found. Also see: attack.

## **Bug**

A bug is an unintentional fault in a program that causes actions that neither the user nor the program author intended.

## **C**

### **Cavity virus**

A cavity virus overwrites a part of its host file without increasing the length of the file while also preserving the host's functionality.

### **Checksum**

A checksum is an identifying number calculated from file characteristics. The slightest change in a file changes its checksum.

### **Clean**

adj. A computer, file, or disk that is free of viruses is considered clean.

v. To clean is to remove a virus or other malicious software from a computer, file, or disk. Also see: disinfection.

### **Cluster virus**

Cluster viruses modify the directory table entries so the virus starts before any other program. The virus code only exists in one location, but running any program runs the virus as well. Because they modify the directory, cluster viruses may appear to infect every program on a disk. They are also called file system viruses.

### **Cold boot**

To cold boot is to start the computer by cycling the power. A cold boot using a rescue disk (a clean floppy disk with boot instructions and virus scanning capabilities) is often necessary to clean or remove boot-sector infectors. Also see: boot, warm boot.

## **COM file**

A COM file is a type of executable file limited to 64 kb. These simple files are often used for utility programs and small routines. Because COM files are executable, viruses can infect them. This file type has the extension COM.

## **Companion virus**

Companion viruses use a feature of DOS that allows software programs with the same name, but with different extensions, to operate with different priorities. Most companion viruses create a COM file which has a higher priority than an EXE file with the same name.

Thus, a virus may see a system contains the file PROGRAM.EXE and create a file called PROGRAM.COM. When the computer executes PROGRAM from the command line, the virus (PROGRAM.COM) runs before the actual PROGRAM.EXE. Often the virus will execute the original program afterwards so the system appears normal.

## **Compromise**

To compromise a system is to access or disclose information without authorization.

## **Cookie**

Cookies are blocks of text placed in a file on your computer's hard disk. Web sites use cookies to identify users who revisit their site.

Cookies might contain login or registration information, "shopping cart" information or user preferences. When a server receives a browser request that includes a cookie, the server can use the information stored in the cookie to customize the web site for the user. Cookies can be used to gather more information about a user than would be possible without them.

## **Crimeware**

Crimeware is malicious software such as viruses, Trojan horses, spyware, deceptive scripts, and other programs used to commit crimes on the Internet including identity theft and fraud. Also see: malware.

## **Cyber criminals**

Cyber criminals are hackers, crackers, and other malicious users that use the Internet to commit crimes such as identity theft, PC hijacking, illegal spamming, phishing and pharming, and other types of fraud. Also see: cyber gangs.

## **Cyber gangs**

Cyber gangs are groups of hackers, crackers, and other cyber criminals that pool their resources to commit crimes on the Internet. Organized crime is often involved in cyber gang activity. Also see: cyber criminals.

## **D**

### **Default password**

A default password is the password on a system when it is first delivered or installed.

## **Denial of service (DoS)**

A Denial of Service (DoS) attack is an attack specifically designed to prevent the normal functioning of a system and thereby to prevent lawful access to the system by authorized users. Hackers can cause Denial of Service attacks by destroying or modifying data or by overloading the system's servers until service to authorized users is delayed or prevented. Also see: attack.

## **Dialer**

Dialers are programs that use a system, without your permission or knowledge, to dial out through the Internet to a 900 number or FTP site, typically to accrue charges.

## **Direct action virus**

A direct-action virus works immediately to load itself into memory, infect other files, and then to unload itself.

## **Disinfection**

Most anti-virus software carries out disinfection after reporting the presence of a virus to the user. During disinfection, the virus may be removed from the system and, whenever possible, any affected data is recovered.

## **DNS**

DNS stands for Domain Name System or Domain Name Server. A DNS server helps users find their way around the Internet by translating each web site's IP address, which is a string of numbers, into its easy-to-remember domain name.

## **DOC file**

A DOC file is a Microsoft Word Document File. In the past, these files contained only document data, but with many newer versions of Microsoft Word, DOC files also include small programs called macros. Many virus authors use the macro programming language to associate macros with DOC files. This file type has the extension DOC.

## **DOS**

DOS stands for Disk Operating System. This is generally any computer operating system, though the term is often used as shorthand for MS-DOS—the operating system used by Microsoft before Windows was developed.

## **Dropper**

A dropper is a carrier file that installs a virus on a computer system. Virus authors often use droppers to shield their viruses from anti-virus software. The term injector often refers to a dropper that installs a virus only in memory.

## **E**

## **Encrypted virus**

An encrypted virus's code begins with a decryption algorithm and continues with scrambled or encrypted code for the remainder of the virus. Each time it infects, it automatically encodes itself differently, so its code is never the same. Through this method, the virus tries to avoid detection by anti-virus software.

## Encryption

Encryption is the scrambling of data so that it becomes difficult to unscramble and interpret.

## EXE file

An EXE is an executable file. Usually, it is executed by double-clicking its icon or a shortcut on the desktop, or by entering the name of the program at a command prompt. Executable files can also be executed from other programs, batch files, or various script files. The vast majority of known viruses infect executable files. This is also called a program file.

## F

### False negative

A false negative error occurs when anti-virus software fails to indicate that an infected file is truly infected. False negatives are more serious than false positives, although both are undesirable. False negatives are more common with anti-virus software because they may miss a new or a heavily modified virus. Also see: false positive.

### False positive

A false positive error occurs when anti-virus software wrongly claims that a virus is infecting a clean file. False positives usually occur when the string chosen for a given virus signature is also present in another program. Also see: false negative.

### Fast infector

Fast infector viruses, when active in memory, infect not only executed programs, but also other programs that are open at the same time. Thus, running an application, such as anti-virus software, which opens many programs but does not execute them, can result in all programs becoming infected. Also see: slow infector.

### FAT

An FAT is a File Allocation Table. Under MS-DOS, Windows 3.x, 9x, and NT (in some cases), the FAT is located in the boot sector of the disk and stores the addresses of all the files contained on a disk. Viruses and other malicious programs, as well as normal use and extended wear and tear, can damage the FAT. If the FAT is damaged or corrupted, the operating system may be unable to locate files on the disk.

### FDISK/MBR

If you have MS-DOS version 5.0 or later, the command FDISK/MBR can remove viruses that infect the master boot sector but do not encrypt it. Using this command can produce unexpected results and cause unrecoverable damage.

### File viruses

File viruses usually replace or attach themselves to COM and EXE files. They can also infect files with the extensions SYS, DRV, BIN, OVL, and OVY.

File viruses may be resident or non-resident, the most common being resident or TSR (terminate-and-stay-resident) viruses. Many non-resident viruses simply infect one or more files whenever an infected file runs. These are also called parasitic viruses, file infectors, or file infecting viruses.

## Firewall

A firewall prevents computers on a network from communicating directly with external computer systems. A firewall typically consists of a computer that acts as a barrier through which all information passing between the networks and the external systems must travel. The firewall software analyzes information passing between the two and rejects it if it does not conform to pre-configured rules.

## H

### Hacker

A hacker is a person who creates and modifies computer software and hardware, including computer programming, administration, and security-related items. This can be done for either negative or positive reasons. Criminal hackers create malware in order to commit crimes. Also see: malware, cyber criminals, cyber gangs.

### Heuristic analysis

Heuristic analysis is behavior-based analysis of a computer program by anti-virus software to identify a potential virus. Often heuristic scanning produces false alarms when a clean program behaves as a virus might.

### Hijacking

Hijacking is an attack whereby an active, established session is intercepted and used by the attacker. Hijacking can occur locally if, for example, a legitimate user leaves a computer unprotected. Remote hijacking can occur via the Internet.

### Hole

A hole is a vulnerability in the design software and/or hardware that allows circumvention of security measures.

### Host

Host is a term often used to describe the computer file to which a virus attaches itself. Most viruses run when the computer or user tries to execute the host file.

## I

### In the wild (ITW)

A virus is "in the wild" (ITW) if it is verified as having caused an infection outside a laboratory situation. Most viruses are in the wild and differ only in prevalence. Also see: zoo virus.

### Infection

Infection is the action a virus carries out when it enters a computer system or storage device.

## J

### JavaScript

JavaScript is a scripting language that can run wherever there is a suitable script interpreter such as web browsers, web servers, or the Windows Scripting Host. The scripting environment used to run JavaScript greatly affects the security of the host machine: A web page with JavaScript runs within a web browser in much the same way as Java applets and does not have access to host machine resources.

An Active Server Page (ASP) or a Windows Scripting Host (WSH) script containing JavaScript is potentially hazardous since these environments allow scripts unrestricted access to machine resources (file system, registry, etc.) and application objects.

## **Joke programs**

Joke programs are not viruses, but may contain a virus if infected or otherwise altered. These are also called practical joke programs.

## **K**

### **Key**

The Windows Registry uses keys to store computer configuration settings. When a user installs a new program or the configuration settings are otherwise altered, the values of these keys change. If viruses modify these keys, they can do damage.

### **Keylogger**

Keyloggers are malicious programs that record the key strokes a user types on their PC, including instant message and email text, email addresses, web sites visited, passwords, credit card and account numbers, addresses, and other private data.

## **L**

### **Library file**

Library files contain groups of often-used computer code that different programs can share. Programmers who use library code make their programs smaller since they do not need to include the code in their program. A virus that infects a library file automatically may appear to infect any program using the library file.

In Windows systems, the most common library file is the Dynamic Link Library; its extension is DLL.

### **Logic bomb**

A logic bomb is a type of Trojan horse that executes when specific conditions occur. Triggers for logic bombs can include a change in a file, a particular series of keystrokes, or a specific time or date. Also see: time bomb.

## **M**

### **Macro**

A macro is a series of instructions designed to simplify repetitive tasks within a program such as Microsoft Word, Excel, or Access. Macros execute when a user opens the associated file. Microsoft's latest macro programming language is simple to use, powerful, and not limited to Word documents. Macros are in mini-programs and can be infected by viruses. Also see: macro virus.

### **Macro virus**

A macro virus is a malicious macro. Macro viruses are written in a macro programming language and attach to a document file such as Word or Excel. When a document or template containing the macro virus is opened in the target application, the virus runs, does its damage, and copies itself into other documents. Continual use of the program results in the spread of the virus.

## **Mail bomb**

A mail bomb is an excessively large email (typically many thousands of messages) or one large message sent to a user's email account. This is done to crash the system and prevent genuine messages from being received.

## **Malicious code**

Malicious code is a piece of code designed to damage a system and the data it contains, or to prevent the system from being used in its normal manner.

## **Malware**

Malware is a generic term used to describe malicious software such as viruses, Trojan horses, spyware, and malicious active content.

## **Mapped drives**

Mapped drives are network drives assigned local drive letters that are locally accessible. For example, the directory path \\MAIN\JohnDoe\ might be mapped as drive G: on a computer.

## **Master boot record (MBR)**

The master boot record (MBR) is the 340-byte program located in the master boot sector. This program reads the partition table, determines what partition to boot, and transfers control to the program stored in the first sector of that partition. There is only one master boot record on each physical hard disk. It is also called the partition table. Also see: boot record.

## **Master boot sector**

The master boot sector is the first sector of a hard disk. This sector is located at sector 1, head 0, track 0. The sector contains the master boot record. Also see: master boot record.

## **Master boot sector virus**

Master boot-sector viruses infect the master boot sector of hard disks, though they spread through the boot record of floppy disks. The virus stays in memory, waiting for DOS to access a floppy disk. It then infects the boot record on each floppy disk DOS accesses. They are also called master boot-record viruses. Also see: boot record.

## **Memory-resident virus**

A memory-resident virus stays in memory after it executes, and it infects other files when certain conditions are met. In contrast, non-memory-resident viruses are active only while an infected application runs.

## **MP3 File**

MP3 files are Moving Picture Experts Group Audio Layer 3 files. They are highly compressed audio tracks, and are very popular on the Internet. MP3 files are not programs, and viruses cannot infect them. This file type has the extension MP3.

## **MS-DOS**

MS-DOS is the Microsoft Disk Operating System. Microsoft developed this operating system for the IBM platform before Windows. Windows operating systems rely heavily on MS-DOS and can execute most MS-DOS commands.

## **Multipartite virus**

Multipartite viruses use a combination of techniques including infecting documents, executables and boot sectors to infect computers. Most multipartite viruses first become resident in memory and then infect the boot sector of the hard drive. Once in memory, multipartite viruses may infect the entire system.

Removing multipartite viruses requires cleaning both the boot sectors and any infected files. Before you attempt the repair, you must have a clean, write-protected rescue disk.

## **Mutating virus**

A mutating virus changes, or mutates, as it progresses through its host files making disinfection more difficult. The term usually refers to viruses that intentionally mutate, though some experts also include non-intentionally mutating viruses. Also see: polymorphic virus.

## **N**

### **Newsgroup**

A newsgroup is an electronic forum where readers post articles and follow-up messages on a specified topic. An Internet newsgroup allows people from around the world discuss common interests. Each newsgroup name indicates the newsgroup's subject in terms of increasingly narrow categories, such as alt.comp.virus.

### **Not in the wild**

Viruses "not in the wild" are in the real world but fail to spread successfully. Also see: in the wild, zoo virus.

### **NTFS**

NTFS is the NT File System; a Windows NT file system used to organize and keep track of files. Also see: FAT.

## **O**

### **On-access scanner**

An on-access scanner is a real-time virus scanner that scans disks and files automatically in the background as the computer accesses the files.

### **On-demand scanner**

An on-demand scanner is a virus scanner the user starts manually. Most on-demand scanners allow the user to set various configurations and to scan specific files, folders, and disks.

### **Operating system**

The operating system (OS) is the underlying software that enables you to interact with the computer. The operating system controls computer storage, communications, and task management functions. Examples of common operating stems are MS-DOS, MacOS, Linux, and Windows 98.

## **Overwriting virus**

An overwriting virus copies its code over its host file's data, thus destroying the original program. Disinfection is possible, although files cannot be recovered. It is usually necessary to delete the original file and replace it with a clean copy.

## **P**

### **Password attacks**

A password attack is an attempt to obtain or decrypt a legitimate user's password. Hackers can use password dictionaries, cracking programs, and password sniffers in password attacks. Defense against password attacks is rather limited but usually consists of a password policy including a minimum length, unrecognizable words, and frequent changes. Also see: password sniffing.

### **Password Sniffing**

Password sniffing is the use of a sniffer to capture passwords as they cross a network. The network could be a local area network, or the Internet itself. The sniffer can be hardware or software. Most sniffers are passive and only log passwords. The attacker must then analyze the logs later. Also see: sniffer.

### **Payload**

Payload refers to the effects produced by a virus attack. It sometimes refers to a virus associated with a dropper or Trojan horse.

### **Peer-to-peer (P2P) networking**

Peer-to-peer (P2P) networking is a distributed system of file sharing where any PC on the network can see any other PC on the network. Users access each other's hard drives to download files. This type of file sharing is valuable, but it brings up copyright issues for music, movies, and other shared media files. Users are also vulnerable to viruses, Trojans, and spyware hiding in files. Also see: Trojan horse, spyware.

### **Pharming**

Pharming is the exploitation of a vulnerability in DNS server software that allows a hacker to redirect a legitimate web site's traffic to a counterfeit web site. The spoofed site is designed to steal personal information such as usernames, passwords, and account information.

### **Phishing**

Phishing is a form of criminal activity using social engineering techniques through email or instant messaging. Phishers attempt to fraudulently acquire other people's personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication.

### **Piggyback**

To piggyback is to gain unauthorized access to a system by exploiting an authorized user's legitimate connection.

### **Polymorphic virus**

Polymorphic viruses create varied (though fully functional) copies of themselves as a way to avoid detection by anti-virus software. Some polymorphic virus use different encryption schemes and require different decryption routines. Thus, the same virus may look completely different on different systems or

even within different files. Other polymorphic viruses vary instruction sequences and use false commands in the attempt to thwart anti-virus software. One of the most advanced polymorphic viruses uses a mutation engine and random-number generators to change the virus code and its decryption routine. Also see: mutating virus.

## **Program infector**

A program infector virus infects other program files once an infected application is executed and the activated virus is loaded into memory.

## **R**

### **Ransomware**

Ransomware is malicious software that encrypts the hard drive of the PC that it infects. The hacker then extorts money from the PC's owner in exchange for decryption software to make the PC's data usable again.

### **Real-time scanner**

A real-time scanner is an anti-virus software application that operates as a background task, allowing the computer to continue working at normal speed while it works. Also see: on-access scanner.

### **Redirect**

A redirect is an action used by some viruses to point a command to a different location. Often this different location is the address of the virus and not the original file or application.

### **Rename**

A rename is an action by which a user or program assigns a new name to a file. Viruses may rename program files and take the name of the file so that running the program inadvertently runs the virus. Anti-virus programs may rename infected files, making them unusable until they are manually cleaned or deleted.

### **Replication**

Replication is the process by which a virus makes copies of itself in order to carry out subsequent infections. Replication is one of major criteria separating viruses from other computer programs.

### **Resident extension**

A resident extension is a memory-resident portion of a program that remains active after the program ends. It essentially becomes an extension to the operating system. Many viruses install themselves as resident extensions.

### **Resident virus**

A resident virus loads into memory and remains inactive until a trigger event. When the event occurs, the virus activates, either infecting a file or disk, or causing other consequences. All boot viruses are resident viruses and so are the most common file viruses.

### **Rogue program**

A rogue program is a term the media uses to denote any program intended to damage programs or data, or to breach a system's security. It includes Trojan horse programs, logic bombs, and viruses.

## RTF file

RTF stands for Rich Text Format. It is an alternative format to the DOC file type supported by Microsoft Word. RTF files are ASCII text files and include embedded formatting commands. RTF files do not contain macros and cannot be infected with a macro virus.

This makes RTF files a good document format for communicating with others via email. However, some macro viruses attempt to intercept saving a file as an RTF file and instead save it as a DOC file with an RTF extension. Users can catch this trick by first reading the file in a simple text editor like Notepad. DOC files will be nearly unreadable, while RTF files will be readable.

## S

### Scanner

A scanner is a virus detection program that searches for viruses. Also see: anti-virus software, on-demand scanner, on-access scanner.

### Sector viruses

See: boot-sector infector, master boot-sector virus.

### Self-encrypting virus

Self-encrypting viruses attempt to conceal themselves from anti-virus programs. Most anti-virus programs attempt to find viruses by looking for certain patterns of code (known as virus signatures) that are unique to each virus. Self-encrypting viruses encrypt these text strings differently with each infection to avoid detection. Also see: self-garbling virus, encrypted virus.

### Self-extracting files

A self-extracting file decompresses part of itself when executed. Software authors and others often use this file type to transmit files and software via the Internet since compressed files conserve disk space and reduce download time. Some anti-virus products may not search self-extracting file components. To scan these components, you must first extract the files and then scan them.

### Self-garbling Viruses

A self-garbling virus attempts to hide from anti-virus software by garbling its own code. When these viruses spread, they change the way they are encoded so anti-virus software cannot find them. A small portion of the virus code decodes the garbled code when activated. Also see: self-encrypting virus, polymorphic virus.

### Shared Drive

A shared drive is a disk drive available to other computers on the network. Shared drives use the Universal Naming Convention (UNC) to differentiate themselves from other drives. Also see: mapped drives.

### Shareware

Shareware is software distributed for evaluation without cost, but that requires payment to the author for full rights. If, after trying the software, you do not intend to use it, you simply delete it. Using unregistered shareware beyond the evaluation period is pirating.

## Signature

A signature is a search pattern—often a simple string of characters or bytes—expected to be found in every instance of a particular virus. Usually, different viruses have different signatures. Anti-virus scanners use signatures to locate specific viruses.

## Slow infector

Slow infectors are active in memory and only infect new or modified files. Also see: fast infector.

## SMTP

SMTP stands for Simple Mail Transport Protocol. It is the Internet email delivery format for transmitting email messages between servers.

## Sniffer

A sniffer is a software program that monitors network traffic. Hackers use sniffers to capture data transmitted over a network.

## Spam

Spam is unsolicited or undesired bulk electronic messages. There is email spam, instant messaging spam, Usenet newsgroup spam, web search-engine spam, spam in blogs, and mobile phone-messaging spam. Spam includes legitimate advertisements, misleading advertisements, and phishing messages designed to trick recipients into giving up personal and financial information.

## Spam Filter

A spam filter is a program used to detect unsolicited email to prevent spam from making it to a user's inbox. Filters use heuristics, keyword scans, whitelists and blacklists, and other processes. The filters are placed on email and ISP servers, in anti-spam software, and in anti-phishing browsers. Also see: Bayesian filter, heuristic analysis.

## Sparse Infector

Sparse infector viruses use conditions before infecting files. Examples include files infected only on the 10th execution or files that have a maximum size of 128kb. These viruses use the conditions to infect less often and therefore avoid detection. They are also called sparse viruses.

## Spim

Spim is spam for instant messaging. The messages can be simple unsolicited ads, or fraudulent phishing mail. Also see: spam, phishing.

## Spoofed web site

A spoofed web site is one that mimics a real company's site—mainly financial services sites—in order to steal private information (passwords, account numbers) from people that are tricked into visiting it. Phishing emails contain links to the counterfeit site, which looks exactly like the real company's site, down to the logo, graphics, and detailed information. Also see: phishing.

## Spyware

Spyware is a wide range of unwanted programs that exploit infected computers for commercial gain. They can deliver unsolicited pop-up advertisements, steal personal information (including financial

information such as credit card numbers), monitor web-browsing activity for marketing purposes, or route HTTP requests to advertising sites.

## **Stealth virus**

Stealth viruses attempt to conceal their presence from anti-virus software. Many stealth viruses intercept disk-access requests, so when an anti-virus application tries to read files or boot sectors to find the virus, the virus feeds the program a "clean" image of the requested item. Other viruses hide the actual size of an infected file and display the size of the file before infection.

Stealth viruses must be running to exhibit their stealth qualities. They are also called interrupt interceptors.

## **String**

A string is a consecutive series of letters, numbers, and other characters. "afsH(\*&@~" is a string; so is "The Mad Hatter." Anti-virus applications often use specific strings, called virus signatures, to detect viruses. Also see: signature.

## **T**

### **Template**

Certain applications use template files to pre-load default configurations settings. Microsoft Word uses a template called NORMAL.DOT to store information about page setup, margins, and other document information.

### **Time bomb**

A time bomb is a malicious action triggered at a specific date or time. Also see: logic bomb.

### **Timestamp**

The timestamp is the time of creation or last modification recorded on a file or another object. Users can usually find the timestamp in the Properties section of a file.

### **TOM**

TOM stands for Top of Memory. It is a design limitation at the 640kb mark on most PCs. Often the boot record does not completely reach top of memory, thus leaving empty space. Boot-sector infectors often try to conceal themselves by hiding around the top of memory. Checking the top of memory value for changes can help detect a virus, though there are also non-viral reasons this value changes.

### **Triggered event**

A triggered event is an action built into a virus that is set off by a specific condition. Examples include a message displayed on a specific date or reformatting a hard drive after the 10th execution of a program.

### **Trojan horse**

A Trojan horse is a malicious program that pretends to be a benign application. It purposefully does something the user does not expect. Trojans are not viruses since they do not replicate, but they can be just as destructive.

## **TSR**

TSR stands for Terminate and Stay Resident. TSR programs stay in memory after being executed. They allow the user to quickly switch back and forth between programs in a non-multitasking environment, such as MS-DOS. Some viruses are TSR programs that stay in memory to infect other files and program. They are also called memory resident programs.

## **Tunneling**

Tunneling is a virus technique designed to prevent anti-virus applications from working correctly. Anti-virus programs work by intercepting the operating system before it can execute a virus. Tunneling viruses try to intercept the actions before the anti-virus software can detect the malicious code. New anti-virus programs can recognize many viruses with tunneling behavior.

## **U**

### **UNC**

UNC stands for Universal Naming Convention. This is the standard for naming network drives. For example, a UNC directory path has the following form: \\server\resource-pathname\subfolder\filename.

## **V**

### **Vaccination**

Vaccination is a technique some anti-virus programs use to store information about files in order to notify the user about file changes. Internal vaccines store the information within the file itself, while external vaccines use another file to verify the original for possible changes.

### **Variant**

A variant is a modified version of a virus. It is usually produced on purpose by the virus author or another person amending the virus code. If changes to the original are small, most anti-virus products will also detect variants. However, if the changes are large, the variant may go undetected by anti-virus software.

### **VBS**

Visual Basic Script. Visual Basic Script is a programming language that can invoke any system function--including starting, using and shutting down other applications without--user knowledge. VBS programs can be embedded in HTML files and provide active content via the Internet. Since not all content is benign, users should be careful about changing security settings without understanding the implications. This file type has the extension VBS.

### **Virus**

A virus is a computer program file capable of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission. Some viruses attach to files so when the infected file executes, the virus also executes. Other viruses sit in a computer's memory and infect files as the computer opens, modifies, or creates the files. Some viruses display symptoms, and others damage files and computer systems, but neither is essential in the definition of a virus; a non-damaging virus is still a virus.

There are computer viruses written for several operating systems including DOS, Windows, Amiga, Macintosh, Atari, UNIX, and others. McAfee.com presently detects more than 57,000 viruses, Trojans,

and other malicious software. Also see: boot sector infector, file viruses, macro virus, companion virus, worm.

## Virus Hoaxes

Virus hoaxes are not viruses, but are usually emails warning people about a virus or other malicious software program. Some hoaxes cause as much trouble as viruses by causing massive amounts of unnecessary email.

Most hoaxes contain one or more of the following characteristics:

- Warnings about alleged new viruses and their damaging consequences
- Demands that the reader forward the warning to as many people as possible
- Pseudo-technical "information" describing the virus
- Bogus comments from officials: FBI, software companies, news agencies, etc.

If you receive an email message about a virus, check with a reputable source to ensure the warning is real. Sometimes hoaxes start out as viruses and some viruses start as hoaxes, so both viruses and virus hoaxes should be considered a threat.

## W

### Warm Boot

Warm booting is restarting a computer without first turning off the power. Using CTL+ALT+DEL or the reset button on many computers can warm boot a machine. Also see: cold boot, reset.

### Windows Scripting

Windows Scripting Host (WSH) is a Microsoft-integrated module that lets programmers use any scripting language to automate operations throughout the Windows desktop.

### Worm

Worms are parasitic computer programs that replicate, but unlike viruses, do not infect other computer program files. Worms can create copies on the same computer, or can send the copies to other computers via a network. Worms often spread via Internet Relay Chat (IRC).

## Z

### ZIP File

A ZIP file is a compressed file. A zip archive contains compressed collections of zipped files. ZIP files are popular on the Internet because users can deliver multiple files in a single container, and the compressed files save disk space and download time. A ZIP file can contain viruses if any of the files packaged in it contain viruses, but the ZIP file itself is not directly dangerous. Other archive files include RAR, and LHA files. This file type has the extension ZIP.

## **Zombie**

A zombie is a PC that has been infected with a virus or Trojan horse that puts it under the remote control of an online hijacker. The hijacker uses it to generate spam or launch Denial of Service attacks. Also see: spam, Denial of Service.

## **Zoo**

A zoo is a collection of viruses used for testing by researchers. Also see: in the wild, zoo virus.

## **Zoo Virus**

A zoo virus exists in the collections of researchers and has never infected a real-world computer system. Also see: in the wild.