

Protection from Virus and Malicious Codes

1. What is EICAR?

EICAR refers to the European Institute for Computer Anti-Virus Research. The Institute provides an independent and impartial platform for IT security experts in the field of science, research, development, implementation and management. The aim is to develop best practice scenarios and guidelines with the efforts of a bundled Know-how-pool. EICAR can be found at < <http://www.eicar.org> >.

2. What is the WildList?

The WildList is a list of the most common computer viruses found spreading around the world at the present time. The list is available on the website of WildList Organization International. Joe Wells and Sarah Gordon founded the organisation in 1996. They work closely with anti-virus professionals and volunteers around the world to update the list regularly, aiming to provide accurate, timely and comprehensive information about current computer viruses. The organisation makes the WildList available to the public free of charge.

3. Are there any CMOS viruses?

Although a computer virus can write to (and corrupt) a PC's CMOS memory, it can NOT "hide" there, because CMOS memory is not "addressable". A malicious virus could alter the values in CMOS as part of its payload, causing the system to fail on reboot, but it cannot spread or hide itself in the CMOS. A virus could use CMOS memory to store part of its code, but executable code stored there must first be moved to the computer's main memory in order to run. There is no known virus that stores code in CMOS memory. There were reports of a "trojanised" AMI BIOS. This was not a computer virus, but a "joke" program that did not replicate. The malicious program was not on the disk, nor in CMOS, but was directly coded into the BIOS ROM chip on the system board. If the date is 13th of November, the virus stops the boot process and plays ' Happy Birthday ' through the PC speaker.

4. Are there any BIOS viruses?

Theoretically, it is possible to have a virus that "hides" in BIOS and can be executed from BIOS. Current technology enables programs to write code into BIOS, which is used for storing the first piece of a program being executed when a PC boots up.

There are viruses that can corrupt the system BIOS; one example is the CIH virus, also known as Chernobyl or Spacefiller.

5. Are there any viruses or malicious code targeted at mobile devices, such as mobile phones?

Yes. In fact viruses and malicious code for mobile devices have been increasing in complexity at a surprising pace.

Mobile phones that allow users to install applications on the device are susceptible to virus and malicious code attacks. There have already been some reports of minor viruses attacks on mobile devices, of which one example is Cabir.

In 2007, malicious code for mobile devices evolved to a complexity that took 20 years on desktop PCs. For example, there are already blends of Trojan Horses and viruses that can spread through mobile phones using multiple wireless protocols. This could be problematic, as current mobile devices and platforms do not support sophisticated anti-virus software.

6. Can data files be infected?

A pure data file such as a TXT file, is not susceptible to virus and malicious code infection. However, viruses and malicious code can infect data files embedded with executable code. For example, there have been some viruses and malicious code spread via Microsoft Word and Adobe PDF documents.

7. What is a macro virus, and how does it spread?

A macro virus is a program written in the macro language provided with some software applications (word processors, spreadsheets, etc.). To propagate, macro viruses exploit the capabilities of the macro language to transfer themselves from one infected file (document or spreadsheet) to another. For example, when a Word document containing infected macros is opened, the virus usually copies itself into Word's global template file (typically NORMAL.DOT). Any document opened or created subsequently will be infected. Macro viruses become part of the document itself, and are transferred with the file, further infecting other files.

8. What's the worst damage a macro virus can do?

Like all computer viruses, macro viruses can destroy files and data. In some cases, a macro virus might reformat all the hard drives in a computer. While most of the known macro viruses are not so destructive, but more of a nuisance, the loss of productivity and time is what affects users the most.

9. How can I minimize the destruction a macro virus may cause to hard disks and files?

You should backup all data files regularly, install and enable real-time protection using anti-virus software with the latest virus signatures and detection and repair engines, and conduct full system scan periodically.

10. Can viruses and malicious code infect a Microsoft Access database?

Yes. The first Access macro virus JETDB_ACCESS-1 was able to infect the Microsoft Access 97 database. Once infected, the virus would search and infect all .MDB files in the current directory, the parent of the current directory, and the root directory.

11. Can viruses and malicious code infect my machine if I connect to the Internet and view Web pages/download programs?

If your computer is not fully patched, or if you run Active X controls, active scripting and JAVA applets, or run programs downloaded from untrusted sources over the Internet, it is possible for these programs to contain viruses or malicious code that could infect your machine.

You should take the following security precautions when surfing the Internet:

- Ensure that your operating system and software on your computer have the latest security patches.
- Enable real-time scanning of anti-virus software and use the latest virus signatures and corresponding detection and repair engines.
- Avoid visiting suspicious/untrusted websites.
- Do not execute unsigned ActiveX controls, or ActiveX control from untrusted sources. If possible, disable active scripting in your browser settings.
- Avoid downloading programs from un-trusted websites, since they carry a high risk of virus infection.

12. Can email messages be infected?

Viruses do not infect plain electronic mail messages with plain text formatting and no executable code. However, HTML emails, which can contain executable scripts as well as files attached to the email message, may be infected. Nowadays, most anti-virus software can be configured to scan emails and their attachments.

13. I have received an email which appears to be a bogus message regarding a new virus, or a promotion that sounds too good to be true. What should I do?

A hoax virus-warning message is an untrue rumour, warning or alert initiated by malicious individuals, with the aim of tricking a recipient into believing the message. Typical examples of these messages include hoaxes related to new computer viruses, promotions, or other hot issues attracting public interest. Hoax messages usually have one or more of the following characteristics:

- They use technical jargon and complex technical descriptions.
- They ask recipients to send or forward the message to everyone they know.
- They do not contain sender information, or use bogus sender information.

Although most hoax messages do not cause direct harm to computers, they may contain untrue information and thus cause unnecessary confusion or even panic for recipients. Forwarding hoax messages consumes network bandwidth and system resources, and is a waste of the recipients' time in reading such messages.

The proper way to handle Internet hoax messages is to simply ignore them. In order to help reduce the spread of Internet hoax messages, DO NOT:

- Circulate messages with an unknown origin without first validating them against reliable/authoritative information sources.
- Forward any hoax to others.

14. Can firewalls detect viruses and malicious code?

Firewalls themselves do not screen out computer viruses or malicious code. But because the location of firewalls within a network is usually a good place for virus scanning to take place, some firewalls have plug-in virus-scanning modules. In addition, some programs are available that can scan for viruses at a point either before or after the firewall. It is worth noting that scanning all FTP or HTTP traffic may add a heavy overhead to the network. A firewall is only one of many entry points for viruses; they can also get into a local intranet through other means, such as via floppy disks, removable storage media and emails.

15. What is a scan engine? Why do I have to update the signature file as well as the scan engine of my anti-virus software?

A virus-scanning engine is the program that does the actual work of scanning and detecting viruses, while signature files are the “fingerprints” used by scan engines to identify viruses. New versions of a scan engine are released for a number of reasons. New types of viruses or other malicious code, such as spyware, may not be detected by the old engine. Updated scan engines also have enhanced scanning performance and detection rates. Some vendors provide updates for both the scan engine and signature files in a single file, while others provide them in separate files.

16. What is the most efficient way to update virus signatures in a network of many computers?

It is important that computer systems and networks are updated with the latest virus signatures on a regular and timely basis in order to effectively detect and block the latest viruses and their variants, especially during outbreaks of high-threat viruses. To enhance the virus signature updating process, organisations should consider automating the operation of updating all network-connected computers when computers are in operation or logged in to a network server. Organisations may also consider implementing automatic virus signature update systems available from major anti-virus software vendors.

17. When attempting to clean certain files infected with viruses and malicious code, the operation fails. Why is this?

Most likely, the operating system or other programs are using the infected files you are trying to clean. It is better to restart the machine in Safe Mode, then clean the files with anti-virus software or use other removal tools for the particular virus.

18. Why can some viruses and malicious code be detected but not cleaned with anti-virus software?

Anti-virus software not only detects viruses, but also other types of malicious code, which may not be possible to clean. A Trojan horse is a type of malicious code that should be deleted instead of trying to clean it. In some cases, the virus may have corrupted the file and made it impossible to recover. Nevertheless, there are some tips to improve the success of cleaning away a virus from a file:

- Use the latest virus signature files and detection and repair engine from the anti-virus vendor.
- Make sure there is enough free space on your disk.
- Check if the removal instructions or if an automatic removal tool is available from anti-virus vendor websites.

- If still unsuccessful, obtain a virus sample and send it to your anti-virus vendor for advice and recommended action.

19. My department has up-to-date anti-virus software installed at the Internet gateway. Why do some computers still get infected by viruses?

According to past experience with virus infection cases, most of them are related to operational practices when handling email, or other IT security management issues. For instance, it is not uncommon to see a user access his or her private Internet email account, hosted by an external ISP or email service provider, directly via the office PC. Such private email services may not have gone through the same virus detection processes as those on the central managed Internet or email gateway. Hence, users are strongly advised not to use private Internet email services at work. See the question [What should I do if private Internet email must be used?] for more details on using personal Internet email accounts in a corporate setting.

Another similar cause is direct Internet connections in the office, such as broadband or dial-up modem access arranged for individual staff, which effectively bypasses the perimeter defence measures provided by the centralised Internet gateway. Notebook computers that have been infected with virus when used outside the office, and are then used by staff in the office are another source of infection.

In addition, there are viruses that can ride on software vulnerabilities and cannot be effectively stopped unless the corresponding security patches have been applied. Notwithstanding the above, user awareness of security best practices also plays a very important role, and users should always be wary when handling files and emails. They should not open or forward suspicious emails or their attachments to reduce the possibility of virus infection.

20. What is the benefit of using the Central Internet Gateway (CIG) from a virus protection perspective?

If an email downloaded from an external ISP contains a virus and the user's workstation does not have appropriate virus protection (i.e. auto-protection by anti-virus software with the latest virus signatures), the workstation could easily become infected. The infected machine may further proceed to infect files on interconnected servers and directories, spreading the virus through internal networks and triggering a massive infection. Deploying a central managed Internet gateway is an effective solution, providing an additional layer of virus protection and blocking risky emails and file attachments, such as those with the extension .EXE. Moreover, it is relatively easy to conduct timely and regular updates to the central gateway using the latest virus signatures, rather than trying to update all user computers. It is thus much more reliable and secure.

21. What should I do if private Internet email must be accessed in the work environment?

On some occasions, there is operational need to use a private Internet email service in the office. Nevertheless, as far as practicable an isolated computer with a dedicated Internet connection for Internet email exchange should be used for this purpose only. In addition, this isolated computer should be fully patched and protected by anti-virus software with the latest virus signatures, and all incoming emails and attachments should be screened before they are processed further by internal systems and networks.

22. What is a phishing attack?

Phishing is a kind of social engineering attack that tricks legitimate users into revealing private details, such as their e-banking login names and passwords, by using emails that link to fraudulent websites.

23. What is malicious code?

Malicious code is any program that causes undesirable effects on an information system. Examples of malicious code include computer viruses, network worms, trojan horses, logic bombs, spyware, adware and backdoor programs. Because they pose a serious threat to software and information processing facilities, precautions must be taken to prevent and detect malicious code.

24. What is a worm?

A worm is a program that spreads over a network. Unlike a virus, a worm does not need to attach itself to a host program for propagation. Some worms use email to spread, sending themselves out as an attachment to other users. Some of them exploit the vulnerabilities in software running on a victim's machine, aiming to take control of those systems. Some worms also spread by using cross-site scripting vulnerabilities in web servers or services.

25. What is a Trojan?

A Trojan or Trojan horse is a software application that pretends to provide legitimate functionality, but actually carries out malicious functions, exploiting the legitimate authority of the person who starts up the program. It can be used as an attack tool to capture sensitive information such as user accounts and passwords. Unlike a virus, a Trojan does not replicate itself. It spreads usually by enticing the user to install software such as "shareware" which is embedded with a Trojan horse.

26. What is spyware?

Spyware is a type of software that secretly forwards information about a user's online activities to third parties without the user's knowledge or permission. The information is mainly used for purposes related to advertising. For example, sending spam emails to the user in order to deliver targeted advertisements by marketers. Some spyware might also be able to steal a victim's files or even keystrokes to gain sensitive and personal information.

27. What is adware?

Adware is a type of software that displays advertising banners while a program is running. Most adware is also spyware. In many cases, freeware developers offer their products free-of-charge to users, receiving financial support from adware marketers by bundling adware into freeware products.

You should carefully read the terms of use before installing any freeware or shareware. The use of freeware and shareware may sometimes imply that you agreed to install adware systems as well.

28. What are backdoor programs?

Backdoor is a general term for a malicious program that listens for commands on a certain network port. Most backdoors consist of a client component and a server component. The client component resides on the attacker's remote computer, and the server part resides on the infected system. When a connection between client and server is established, the remote attacker has a degree of control over the infected computer. For example, a backdoor may allow an attacker to monitor or take control of an infected computer, stealing data from it, uploading and activating viruses, or erasing user data and so on.

29. What is a rootkit?

A rootkit is a program/tool designed to gain root or administrator access to a system. It often has malicious intent without going through proper authorization and/or authentication processes. A rootkit might consist of backdoor programs as well as tools to hide any trace of hacking activities.

30. What is a Zombie computer (or Zombie)?

A Zombie is a computer connected to the Internet that has been compromised by an intruder, usually with computer viruses or Trojan horses. The intruder then manipulates the computer without the knowledge of the owner. The computer is often used to perform malicious activities such as launching denial of service attacks on a targeted system via remote control.

31. What is a botnet?

A botnet is a network of zombie computers under the remote control of an attacker.

32. Why is it that Anti-Virus software cannot repair files that are infected by a Trojan or a worm?

Strictly speaking, there is no such thing as "file infected by a Trojan or a worm". One difference between a virus and a Trojan or a worm is that a virus will replicate itself to a clean file, which will in turn infect other clean files when the infected file is executed or opened.

A Trojan is a malicious program installed on an infected computer which does not attach itself to any file. Worms are also malicious software that spread across networks but do not replicate onto a clean file. Therefore, there is no file to repair when it comes to a Trojan or a worm.

33. What is the best defence against phishing scams?

The following are some best practices to avoid being caught by phishing scams:

- Do not respond to emails that request personal information (such as passwords), or follow URL links from untrusted sources and suspicious emails. In this way, you can avoid being re-directed to malicious websites by links that seem legitimate.
- Verify the legitimacy of websites for organizations such as banks by contacting the organization by traditional mail or telephone.
- Type the URL to the desired website manually, or use bookmarks you have saved previously when visiting important or crucial websites.

- Log into any online accounts you have regularly to check the account status and last login time; determine whether there has been any suspicious activity.
- Always be wary when giving sensitive personal or account information over the web. Banks and financial institutions seldom ask for your personal or account information through email. Consult the relevant organization if in doubt.
- Always ensure your computer is updated with the latest security patches and virus signatures. This will reduce the chance of being affected by fraudulent emails or websites riding on software vulnerabilities. This also helps protect your computer from other security or virus attacks.
- Consider using desktop spam-filtering products to detect and block fraudulent emails; however, beware of false alarms.
- Send any phishing emails you receive to the relevant organization and/or the police for further investigation.

34. How can I prevent my PC from becoming a zombie?

The following best practices can help protect your computer from being taken over as a zombie:

- Install and enable proven anti-virus and personal firewall software on your computer.
- Update your anti-virus software frequently with the latest virus signatures.
- Keep your anti-virus software up-to-date, because outdated anti-virus software can be ineffective when it comes to newly discovered viruses.
- Apply the latest security updates and patches to any software you use.
- Disconnect your computer from the Internet when not in use. Computers connected to the Internet all the time are at constant risk of infection, and they have a greater likelihood of being hacked.

35. How can I protect my PC against viruses and malicious code?

Always install and enable anti-virus software or malicious code detection and repair tools. You can also consider similar products that work against spyware and adware. You should enable and configure the live update feature of your virus signature and malicious code definition files, if available, setting the frequency to update daily. If automatic update is not possible, manual updates should be conducted at least once a week.

In addition, users should:

- Enable real-time detection to scan, for example, email attachments, files on removable media, and files downloaded from the Internet.
- Schedule a regular full system scan.
- Regularly review and apply the latest security patches/hot-fixes released by product vendors for operating systems and application programs.
- Before installing any software, verify its integrity (e.g. by comparing checksum values) and ensure it is free of computer viruses and malicious code.
- Avoid using personal Internet email, which is more susceptible to computer virus infection. If personal Internet email services must be used for business purposes, emails should be downloaded to an isolated computer via a dedicated Internet connection.
- Always boot from the primary hard disk. As far as possible, do not boot workstations from removable storage devices.
- Backup your data regularly.

If you suspect your computer is infected, you should stop using it, because that may spread the computer virus or malicious code further. If it is your office computer or mobile device, you should report the incident to the management and LAN/System Administrator immediately.

While you can use anti-virus software to clean malicious code, it may not be possible to fully recover infected files. You should replace any infected files with original copies from your backup systems. After recovery, a complete scan of your PC and other removable storage media is vital to ensure everything is now free of viruses or malicious code.

36. How can LAN/System administrators protect their corporate networks against viruses and malicious codes?

LAN/System administrators should install anti-virus software or malicious code detection and repair software on all servers and workstations, and configure the updating of virus signatures and malicious code definitions to be automatic, preferably on a daily basis. If automatic updating is not possible, manual updates should be conducted at least once a week.

The following should also be considered:

On the network side:

- Install anti-virus and content filtering gateways to scan all incoming and outgoing traffic. The gateway should stop messages or files with malicious content, quarantine / drop them, and create audit logs for reference.
- Regularly review and apply the latest security patches/hot-fixes from product vendors to the network operating systems and o gateway devices.
- Apply the same security protection measures to both production systems and the development / testing systems.
- Perform full system scans on all computers before connecting them into your networks.
- Perform full system scans after every installation of a new machine, service maintenance and installation of new software.

On the server side:

- Always boot from the primary hard drive. If the server must be booted from removable storage media (such as USB drives, USB hard drives, CD, DVD), the removable media must first be scanned for malicious code.
- Regularly review and apply the latest security patches/hot-fixes from product vendors to operating systems and application programs.
- Enforce access controls to protect the server. For example, directories containing applications should be set to 'read only'. The 'Write' and 'Modify' access right should be granted on a need-to-have basis only.
- Use document management solutions when sharing documents so as to minimize any potential propagation of infected files in an uncontrolled manner.
- Scan all newly installed software before it is released for general use.
- Schedule regular full-system scans.
- Perform regular data backups.

In addition, administrators should keep abreast of the latest security advisories by, for example, subscribing to online security notifications and advisories. They should quickly disseminate critical and major computer virus alerts to all end-users, educate users about the impact of massive malicious code attacks, and ensure users follow best practices to protect their workstations against computer viruses and malicious code.

37. Mass-mailing Viruses with Spoofing Characteristics

37-1. I have heard of viruses with mass-mailing and spoofing capabilities. What are the characteristics of these viruses?

Certain viruses are able to send emails carrying virus-infected attachments to as many recipients as they can in an attempt to further spread themselves. Such mass-mailing viruses usually

harvest email addresses from the hard disk of an infected computer (such as the address book of an email program) and then send out virus-infected emails with the FROM and TO fields spoofed by randomly choosing names from the harvested email address list, faking the sender and recipient addresses.

As a result, the sender name viewed in the virus-infected email may not be the true sender. This can make it appear that another person is sending out virus-infected emails while in fact they are not. This is a common trick used by such viruses in order to deceive recipients and cover their tracks.

If you receive such virus-infected emails, it likely means your email address was in the records or address list of someone else's infected computer, and has been picked by the virus during the process of spreading infected emails. When this happens, there is a good chance that your email address will also be used by the virus as a spoofed sender address for sending out more virus-infected emails to other users.

37-2. What should I do if I receive virus-infected emails generated by mass-mailing viruses?

You should reject and delete such virus-infected emails and never open any attachment in such messages. You should also ensure that you have adequate virus protection measures in place on your computers, and that anti-virus software is kept up to date with the latest virus signatures and detection and repair engines. Unless it is possible to verify the apparent sender address of the virus-infected email, do not send any enquiry message to the apparent sender because in most of the cases, the sender address is spoofed and the sender whose email address it is has nothing to do with the virus-infected message. This avoids further confusion and unnecessary allegations.