ESET Glossary

User guide

Click here to display the online version of this document

Digital Security
Progress. Protected.

ESET Glossary was developed by ESET, spol. s r.o.

For more information visit https://www.eset.com.

Technical Support: https://support.eset.com

REV. 5/25/2022

Introduction to the ESET Glossary

The ESET Glossary provides a comprehensive overview of current threats and the ESET technologies that protect you from them.

Topics are divided into the following chapters which describe:

- Detections – Including computer virus, worm, Trojan horse, Potentially unwanted application etc.
- Remote attacks – Threats that occur over a local network or the internet
- Email threats – Including hoax, phishing, scam and so on.
- ESET technologies – Product features available in the ESET security solutions

Adware

Adware is a short for advertising-supported software. Programs displaying advertising material fall under this category. Adware applications often automatically open a new pop-up window containing advertisements in an Internet browser, or change the browser's home page. Adware is frequently bundled with freeware programs, allowing their creators to cover development costs of their (usually useful) applications.

Adware itself is not dangerous – users will only be bothered with advertisements. Its danger lies in the fact that adware may also perform tracking functions (as spyware does).

If you decide to use a freeware product, please pay particular attention to the installation program. The installer will most likely notify you of the installation of an extra adware program. Often you will be allowed to cancel it and install the program without adware.

Some programs will not install without adware, or their functionality will be limited. This means that adware may often access the system in a "legal" way, because users have agreed to it. In this case, it is better to be safe than sorry. If there is a file detected as adware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

Botnet

A bot, or a web robot is an automated malware program that scans blocks of network addresses and infects vulnerable computers. This allow hackers to take control of many computers at the same time and turn them into bots (also known as a zombie). Hackers typically use bots to infect large numbers of computers, which form a network or a botnet. Once the botnet is in your computer, it can be used in distributed denial of service (DDoS) attacks, proxy and also can be used to perform automated tasks over the Internet, without you knowing it (for example sending spam, viruses or stealing personal and private information such as bank credentials or credit card numbers).

False positive (FP)

Realistically, there is not a 100% detection rate guarantee or a 0% chance to avoid incorrect categorization of clean objects as detections.

A false positive is a clean file/application falsely classified as malware or a PUA.

Packer

Packer is a runtime self-extracting executable that rolls up several kinds of malware into a single package.

The most common packers are UPX, PE_Compact, PKLite and ASPack. The same malware may be detected differently when compressed using a different packer. Packers also have the ability to make their "signatures" mutate over time, making malware more difficult to detect and remove.

Potentially unsafe applications

There are many legitimate programs whose function is to simplify the administration of networked computers. However, in the wrong hands, they may be misused for malicious purposes. ESET provides the option to detect such applications.

Potentially unsafe applications is the classification used for commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications, and keyloggers (a program that records each keystroke a user types).

If you find that there is a potentially unsafe application present and running on your computer (and you did not install it), please consult your network administrator or remove the application.

Potentially unwanted applications

Grayware or Potentially Unwanted Application (PUA) is a broad category of software, whose intent is not as unequivocally malicious as with other types of malware, such as viruses or trojan horses. It may however install additional unwanted software, change the behavior of the digital device, or perform activities not approved or expected by the user.

Categories that may be considered grayware include: advertising display software, download wrappers, various browser toolbars, software with misleading behavior, bundleware, trackware, crypto-miners, registry cleaners (Windows operating systems only) or any other borderline software, or software that uses illicit or at least unethical business practices (despite appearing legitimate) and might be deemed undesirable by an end user who became aware of what the software would do if allowed to install.

A Potentially Unsafe Application is in itself legitimate (possibly commercial) software but which might be misused by an attacker. Detection of these types of applications can be enabled or disabled by users of ESET software.

Some situations where a user may feel that the benefits of a potentially unwanted application outweigh the risks. For this reason, ESET assigns such applications a lower-risk category compared to other types of malicious software, such as trojans or worms.

- Warning - Potentially unwanted application found
- Settings
- Software wrappers

- Registry cleaners
- Potentially unwanted content

Illustrated instructions
To scan and remove Potentially Unwanted Applications (PUAs) in ESET Windows home products, see our ESET Knowledgebase article.

Warning - Potentially unwanted application found

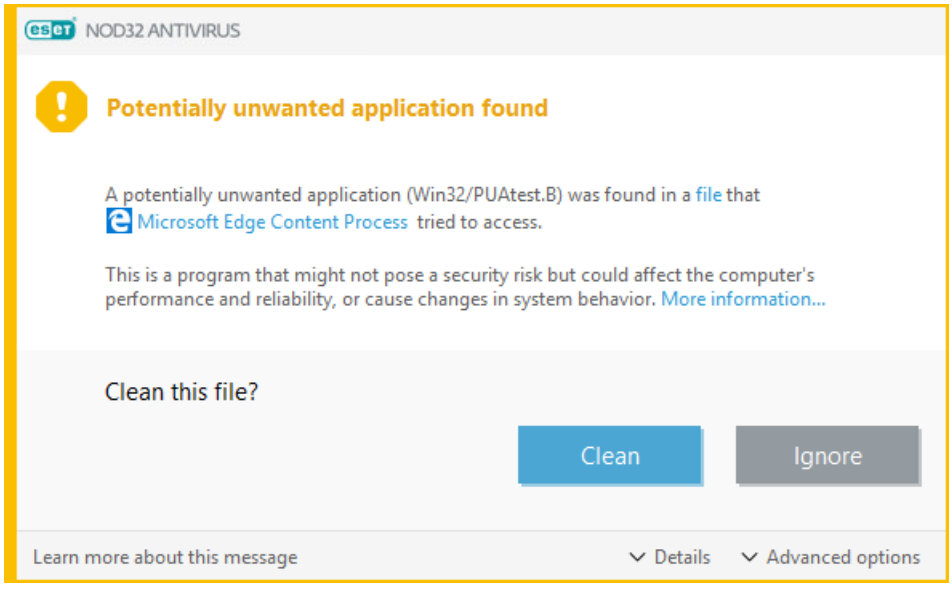
When a potentially unwanted application is detected, you can decide which action to take:

1.**Clean/Disconnect**: This option ends the action and prevents the PUA from entering your system. You will see the **Disconnect** option for PUA notifications during download from a website and the **Clean** option for notifications for a file on disk.

2.**Ignore**: This option allows a PUA to enter your system.

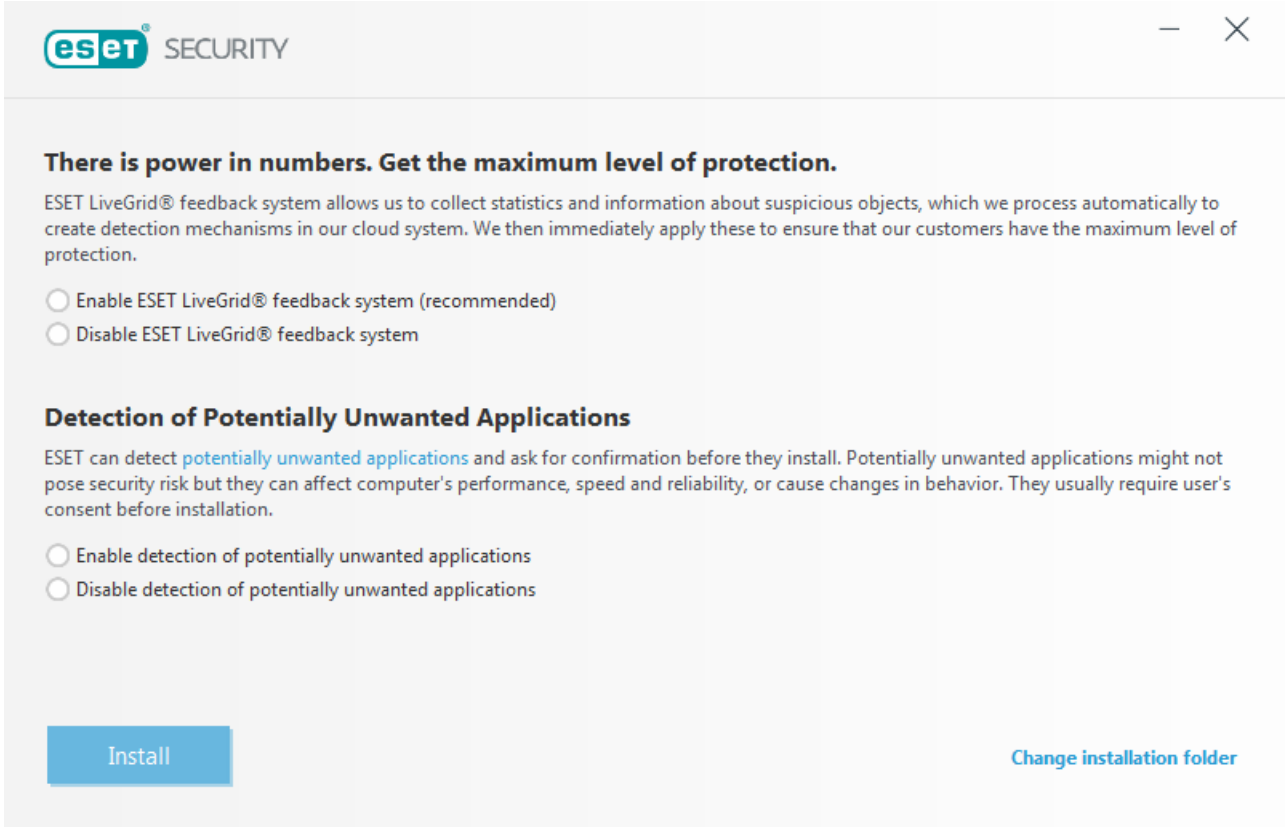
3.**Exclude from detection**: To allow the detected file that is already on the computer to run in the future without interruption, click **Advanced options**, select the check box next to **Exclude from detection** and click **Ignore**.

4.**Exclude signature from detection**: To allow all files identified by a specific detection name (signature) to run on your computer in the future without interruption (from existing files or web download), click **Advanced options**, select the check box next to **Exclude signature from detection** and click **Ignore**. If additional detection windows with an identical detection name are displayed immediately afterward, click Ignore to close them (any additional windows are related to a detection that occurred before you excluded signature from detection).



Settings

While installing your ESET product, you can decide whether to enable detection of potentially unwanted applications, as shown below:



Warning

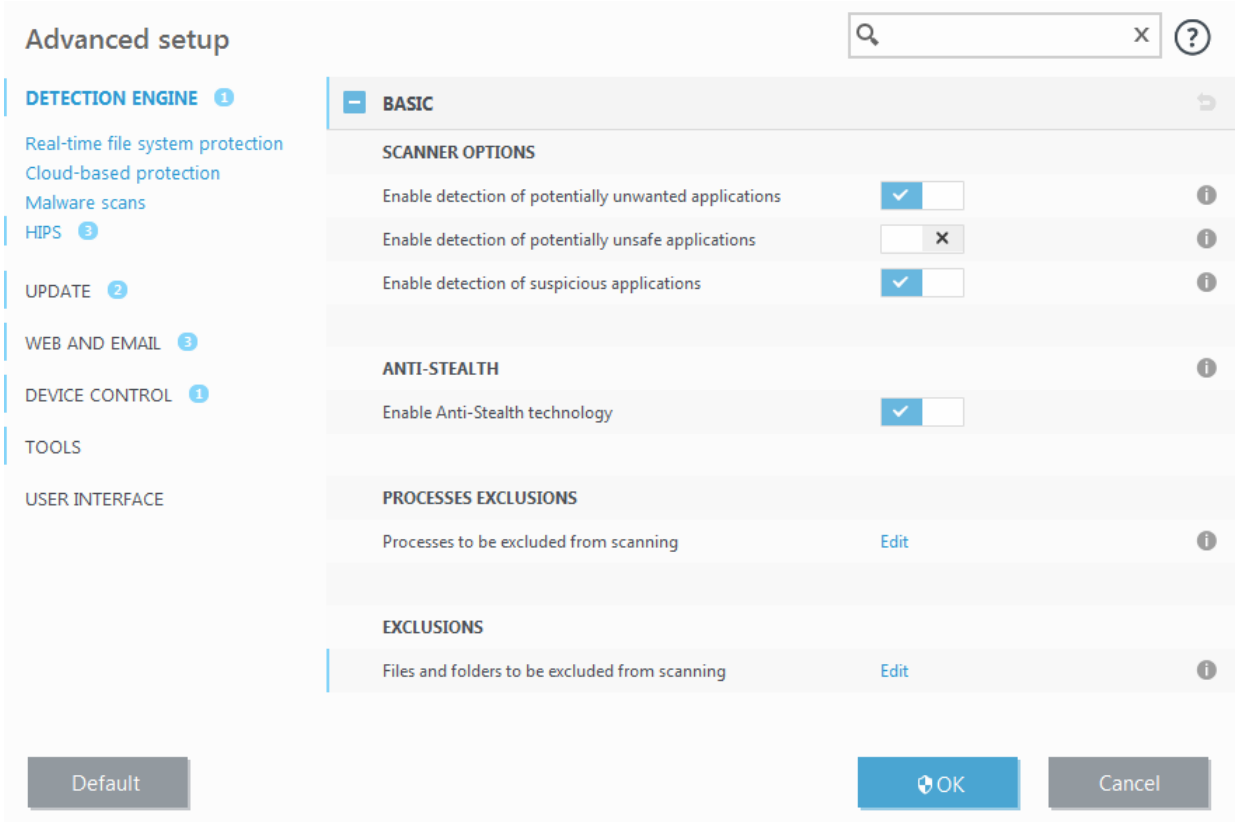
Potentially unwanted applications may install adware, toolbars, or contain other unwanted and unsafe program features.

You can modify these settings in your program settings at any time. To enable or disable the detection of Potentially unwanted, unsafe or suspicious applications, follow these instructions:

1. Open your ESET product.

2. Press the **F5** key to access **Advanced setup**.

3. Click **Detection engine** (in earlier versions also known as **Antivirus** or **Computer**) and enable or disable options **Enable detection of potentially unwanted applications**, **Enable detection of potentially unsafe applications** and **Enable detection of suspicious applications** according to your preferences. Confirm by clicking **OK**.



Illustrated instructions

For more detailed instructions how to configure products to detect or ignore PUAs, visit ESET Knowledgebase articles:

- ESET NOD32 Antivirus / ESET Internet Security / ESET Smart Security Premium
- ESET Cyber Security for macOS / ESET Cyber Security Pro for macOS
- ESET Endpoint Security / ESET Endpoint Antivirus for Windows
- ESET Mobile Security for Android

Software wrappers

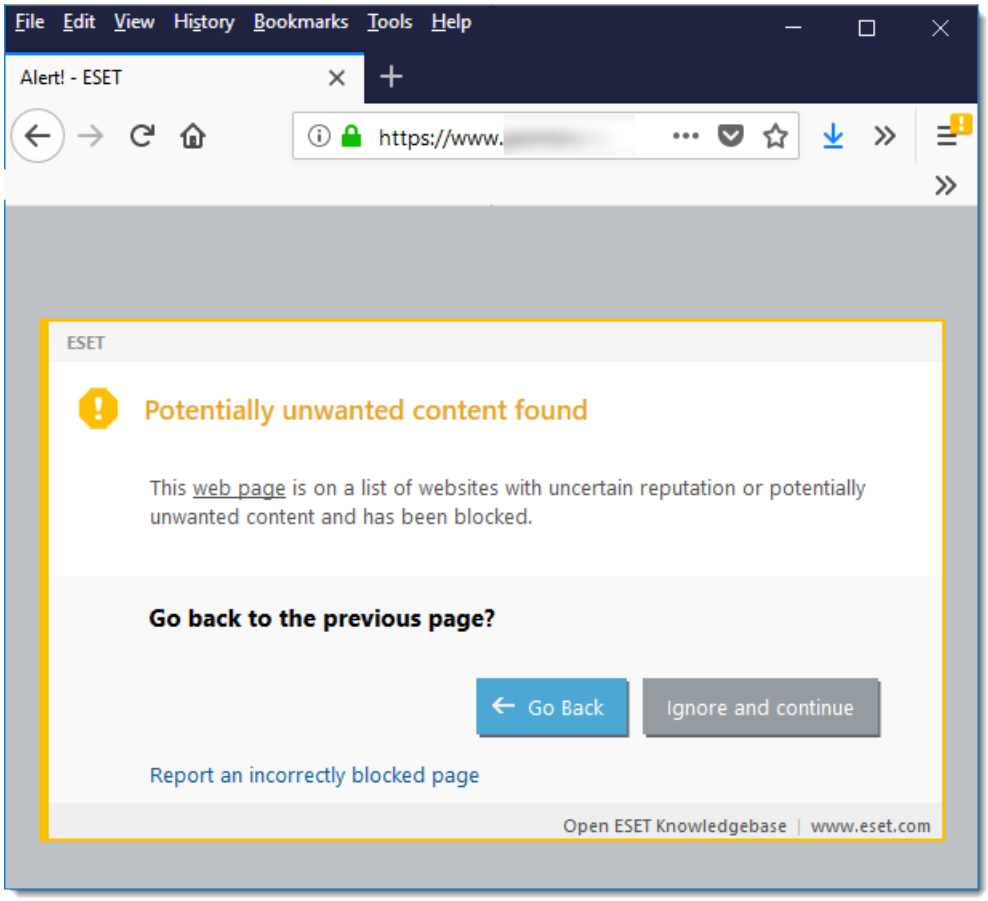
A software wrapper is a special type of application modification that is used by some file-hosting websites. It is a third-party tool that installs the program you intended to download but adds additional software, such as toolbars or adware. The additional software may also make changes to your web browser's home page and search settings. Also, file-hosting websites often do not notify the software vendor or download recipient that modifications are made, and often hide options to opt out. For these reasons, ESET classifies software wrappers as a type of potentially unwanted application to allow users to accept the download or not.

Registry cleaners

Registry cleaners are programs that may suggest that the Windows registry database requires regular maintenance or cleaning. Using a registry cleaner might introduce some risks to your computer system. Additionally, some registry cleaners make unqualified, unverifiable, or otherwise unsupportable claims about their benefits or generate misleading reports about a computer system based on the results of a "free scan". These misleading claims and reports seek to persuade you to purchase a full version or subscription, usually without allowing you to evaluate the registry cleaner before payment. For these reasons, ESET classifies such programs as PUA and provides you the option to allow or to block them.

Potentially unwanted content

If PUA detection is enabled in your ESET product, websites that have a reputation for promoting PUAs or that have a reputation for misleading users into performing actions that might have negative implications on their system or browsing experience will be blocked as potentially unwanted content. You can receive a notification that a website you are attempting to visit is categorized as potentially unwanted content. Click **Go Back** to navigate away from the blocked web page or click **Ignore and continue** to allow the site to load.



Further information about this topic can be found in this ESET Knowledgebase article.

Ransomware

Ransomware (also known as filecoder) is a type of malware that locks your device or encrypts the content on your device and extorts money from you to restore access to your content. This kind of malware can also have a built-in timer with a pre-programmed payment deadline that must be met. If the deadline is not met, the price increases, or the device ultimately becomes inaccessible.

When the device is infected, the filecoder may attempt to encrypt the shared drives on the device. This process can make it seem as though the malware is spreading over the network, but it is actually not. This situation occurs when the shared drive on a file server is encrypted, but the server itself does not contain a malware infection (unless it is a terminal server).

Ransomware authors generate a pair of keys, public and private, and insert the public one into the malware. The ransomware itself may be a part of a Trojan or appear to be a file or a picture that you could receive in an email, on social networks, or in instant messengers. After infiltrating your computer, the malware will generate a random symmetric key and encrypt the data on the device. It uses the public key in the malware to encrypt the

symmetric key. The ransomware then demands a payment to decrypt the data. The payment demand message displayed on the device may be a false warning that your system has been used for illegal activities or contains illegal content. The ransomware victim is asked to pay the ransom using a range of payment methods. The options are usually the ones that are difficult to trace, such as digital (crypto) currencies, premium-rate SMS messages, or pre-paid vouchers. After receiving the payment, the ransomware author should unlock the device or use their private key to decrypt the symmetric key and decrypt the victims' data; however, this operation is not guaranteed.

> **More information about ransomware protection**
> ESET products use multiple layered technologies that protect devices from ransomware. See our ESET Knowledgebase article for the best practices to protect your system against ransomware.

Rootkit

Rootkits are malicious programs that grant Internet attackers unlimited access to a system, while concealing their presence. Rootkits, after accessing a system (usually exploiting a system vulnerability), use functions in the operating system to avoid detection by antivirus software: they conceal processes, files and Windows registry data. For this reason, it is almost impossible to detect them using ordinary testing techniques.

There are two levels of detection to prevent rootkits:

1. When they try to access a system: They are still not present, and are therefore inactive. Most antivirus systems are able to eliminate rootkits at this level (assuming that they actually detect such files as being infected).

2. When they are hidden from the usual testing: ESET users have the advantage of Anti-Stealth technology, which is also able to detect and eliminate active rootkits.

Spyware

This category covers all applications which send private information without user consent/awareness. Spyware uses tracking functions to send various statistical data such as a list of visited websites, email addresses from the user‘s contact list, or a list of recorded keystrokes.

The authors of spyware claim that these techniques aim to find out more about users’ needs and interests and allow better-targeted advertisement. The problem is that there is no clear distinction between useful and malicious applications and no one can be sure that the retrieved information will not be misused. The data obtained by spyware applications may contain security codes, PINs, bank account numbers, etc. Spyware is often bundled with free versions of a program by its author in order to generate revenue or to offer an incentive for purchasing the software. Often, users are informed of the presence of spyware during a program‘s installation to give them an incentive to upgrade to a paid version without it.

Examples of well-known freeware products which come bundled with spyware are client applications of P2P (peer-to-peer) networks. Spyfalcon or Spy Sheriff (and many more) belong to a specific spyware subcategory – they appear to be antispyware programs, but in fact they are spyware programs themselves.

If a file is detected as spyware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

As a subcategory of spyware, keyloggers can be hardware or software-based. Software-based keyloggers can only

collect the information typed into a single website or application. More sophisticated keyloggers can record everything you type, including the information you copy/paste. Some keyloggers targeting mobile devices can record calls, information from messaging applications, locations, or even microphone and camera captures.

Trojan

Historically, computer Trojans (Trojan horses) have been defined as a class of threats which attempt to present themselves as useful programs and thus trick users into running them.

Since Trojans are a very broad category, it is often divided into several subcategories:

- Downloader – Malicious programs with the ability to download other threats from the Internet.
- Dropper – Malicious programs with the ability to drop other types of malware onto compromised computers.
- Backdoor – Malicious programs which communicate with remote attackers, allowing them to gain access to the computer and take control over it.
- Keylogger – (keystroke logger) – A program which records each keystroke that a user types and sends the information to remote attackers.
- Dialer – Malicious programs designed to connect via premium-rate numbers instead of the user's Internet service provider. It is almost impossible for a user to notice that a new connection was created. Dialers can only cause damage to users with dial-up modems, which are no longer regularly used.

If a file on your computer is detected as a Trojan, it is advisable to delete it, since it most likely contains nothing but malicious code.

Virus

A computer virus is a piece of malicious code that is prepended or appended to existing files on your computer. Viruses are named after biological viruses because they use similar techniques to spread from one place to another. “Virus” is often misused to refer to any threat. This usage is gradually being replaced with a more accurate term, "malware" (malicious software).

Computer viruses primarly attack executable files and documents. In short, this is how a computer virus works: after running the infected file, the malicious code is called and executed prior to the execution of the original application. A virus can infect any files that the current user has write permissions for.

Computer viruses can range in purpose and severity. Some of them are extremely dangerous because of their ability to delete files purposely from the hard drive. On the other hand, some viruses do not cause any damage – they only serve to annoy the user and demonstrate the technical skills of their authors.

If your computer is infected with a virus and cleaning is not possible, submit it to the ESET Research Lab for perusal. In certain cases, infected files can be modified to such an extent that cleaning is not possible, and the files must be replaced with a clean copy.

Worm

A computer worm is a program containing malicious code that attacks host computers and spreads via network. The basic difference between a virus and a worm is that worms have the ability to propagate by themselves; they are not dependant on host files (or boot sectors). Worms spread to email addresses in your contact list or exploit security vulnerabilities in network applications.

Worms are therefore much more viable than computer viruses. Due to the wide availability of the Internet, they can spread across the globe within hours or even minutes after their release. This ability to replicate independently and rapidly makes them more dangerous than other types of malware.

A worm activated in a system can cause a number of inconveniences: It can delete files, degrade system performance, or even deactivate programs. The nature of a computer worm qualifies it as a “means of transport“ for other types of infiltrations.

If your computer is infected with a worm, we recommend you delete the infected files because they likely contain malicious code.

DNS Poisoning

Using DNS (Domain Name Server) poisoning, hackers can trick the DNS server of any computer into believing that the fake data they supplied is legitimate and authentic. The fake information is cached for a certain period of time, allowing attackers to rewrite DNS replies of IP addresses. As a result, users trying to access Internet websites will download computer viruses or worms instead of their original content.

DoS attack

DoS, or Denial of Service, is an attempt to make a computer or network unavailable for its intended users. The communication between afflicted users is obstructed and can no longer continue in a functional way. Computers exposed to DoS attacks usually need to be restarted in order to work properly.

In most cases, the targets are web servers and the aim is to make them unavailable to users for a certain period of time.

ICMP attack

The ICMP (Internet Control Message Protocol) is a popular and widely-used Internet protocol. It is used primarily by networked computers to send various error messages.

Remote attackers attempt to exploit the weaknesses of the ICMP protocol. The ICMP protocol is designed for one-way communication requiring no authentication. This enables remote attackers to trigger so-called DoS (Denial of Service) attacks, or attacks which give unauthorized individuals access to incoming and outgoing packets.

Typical examples of an ICMP attack are ping flood, ICMP_ECHO flood and smurf attacks. Computers exposed to the ICMP attack are significantly slower (this applies to all applications using the Internet) and have problems connecting to the Internet.

Port scanning

Port scanning is used to determine which computer ports are open on a network host. A port scanner is software designed to find such ports.

A computer port is a virtual point which handles incoming and outgoing data – this is crucial from a security point of view. In a large network, the information gathered by port scanners may help to identify potential vulnerabilities. Such use is legitimate.

Still, port scanning is often used by hackers attempting to compromise security. Their first step is to send packets to each port. Depending on the response type, it is possible to determine which ports are in use. The scanning itself causes no damage, but be aware that this activity can reveal potential vulnerabilities and allow attackers to take control of remote computers.

Network administrators are advised to block all unused ports and protect those that are in use from unauthorized access.

SMB Relay

SMB Relay and SMB Relay 2 are special programs that are capable of carrying out attacks against remote computers. The programs take advantage of the Server Message Block file sharing protocol, which is layered onto NetBIOS. A user sharing any folder or directory within the LAN most likely uses this file sharing protocol.

Within local network communication, password hashes are exchanged.

SMB Relay receives a connection on UDP port 139 and 445, relays the packets exchanged by the client and server, and modifies them. After connecting and authenticating, the client is disconnected. SMB Relay creates a new virtual IP address. The new address can be accessed using the command “net use \\192.168.1.1“. The address can then be used by any of the Windows networking functions. SMB Relay relays SMB protocol communication except for negotiation and authentication. Remote attackers can use the IP address, as long as the client computer is connected.

SMB Relay 2 works on the same principle as SMB Relay, except it uses NetBIOS names rather than IP addresses. Both can carry out “man-in-the-middle” attacks. These attacks allow remote attackers to read, insert and modify messages exchanged between two communication endpoints without being noticed. Computers exposed to such attacks often stop responding or restart unexpectedly.

To avoid attacks, we recommend that you use authentication passwords or keys.

TCP desynchronization

TCP desynchronization is a technique used in TCP Hijacking attacks. It is triggered by a process in which the sequential number in incoming packets differs from the expected sequential number. Packets with an unexpected sequential number are dismissed (or saved in the buffer storage, if they are present in the current communication window).

In desynchronization, both communication endpoints dismiss received packets, at which point remote attackers are able to infiltrate and supply packets with a correct sequential number. The attackers can even manipulate or modify communication.

TCP Hijacking attacks aim to interrupt server-client, or peer-to-peer communications. Many attacks can be avoided by using authentication for each TCP segment. It is also advised to use the recommended configurations for your network devices.

Worm attack

A computer worm is a program containing malicious code that attacks host computers and spreads via a network. Network worms exploit security vulnerabilities in various applications. Due to the availability of the Internet, they can spread all over the world within a few hours of their release.

Most worm attacks (Sasser, SqlSlammer) can be avoided by using default security settings in the firewall, or by blocking unprotected and unused ports. Also, it is essential that your operating system is updated with the most recent security patches.

Credential stuffing

Credential stuffing is a cyber attack that uses data from leaked credentials databases. Attackers use bots and other automatization methods to log into accounts on numerous websites using the leaked data. Attackers take advantage of users that recycle their login credentials through multiple websites and services. When the attack is successful, attackers can gain full access to the account and users' data stored in this account. Attackers can exploit this access to steal personal data for identify theft, fraudulent transactions, distributing spam, or other malicious actions.

Email threats

Email is a form of communication with many advantages.

Unfortunately, with a high level of anonymity, email and the internet leave room for illegal activities such as spamming. Spam includes unsolicited advertisements, hoaxes and, the proliferation of malicious software – malware. The inconvenience and danger to you are increased by the fact that the cost of sending spam is minimal, and authors of spam have many tools to acquire new email addresses. In addition, the volume and variety of spam make it very difficult to regulate. The longer you use your email address, the more likely it will end up in a spam engine database.

Some hints for prevention:

- If possible, do not publish your email address on the internet
- Only give your email address to trusted individuals
- If possible, do not use common aliases – with more complicated aliases, the probability of tracking is lower
- Do not reply to spam that has already arrived in your Inbox
- Be careful when filling out internet forms – be especially cautious of options such as “Yes, I want to receive information”
- Use “specialized” email addresses – for example, one for business, one for communication with your friends, etc.

- Change your email address periodically
- Use an Antispam solution

Advertisements

Internet advertising is one of the most rapidly growing forms of advertising. Its main marketing advantages are minimal costs and a high level of directness; what's more, messages are delivered almost immediately. Many companies use email marketing tools to effectively communicate with current and prospective customers.

This type of advertising is legitimate, since you may be interested in receiving commercial information about some products. But many companies send unsolicited bulk commercial messages. In such cases, email advertising crosses the line and becomes spam.

The amount of unsolicited email has become a problem and it shows no signs of slowing. Authors of unsolicited email often attempt to disguise spam as legitimate messages.

Hoaxes

A hoax is misinformation which is spread across the Internet. Hoaxes are usually sent via email or communication tools like ICQ and Skype. The message itself is often a joke or Urban Legend.

Computer Virus hoaxes try to generate fear, uncertainty and doubt (FUD) in the recipients, bringing them to believe that there is an "undetectable virus" deleting files and retrieving passwords, or performing some other harmful activity on their system.

Some hoaxes work by asking recipients to forward messages to their contacts, perpetuating the hoax. There are mobile phone hoaxes, pleas for help, people offering to send you money from abroad, etc. It is often impossible to determine the intent of the creator.

If you see a message prompting you to forward it to everyone you know, it may very well be a hoax. There are many websites on the Internet that can verify if an email is legitimate. Before forwarding, perform an Internet search on any message you suspect is a hoax.

Phishing

The term phishing defines a criminal activity which uses techniques of social engineering (manipulating users in order to obtain confidential information). Its aim is to gain access to sensitive data such as bank account numbers, PIN codes, etc.

Access is usually achieved by sending email masquerading as a trustworthy person or business (e.g., financial institution, insurance company). The email can look very genuine, and will contain graphics and content which may have originally come from the source it is impersonating. You will be asked to enter, under various pretenses (data verification, financial operations), some of your personal data – bank account numbers or usernames and passwords. All such data, if submitted, can easily be stolen and misused.

Banks, insurance companies, and other legitimate companies will never request usernames and passwords in an unsolicited email.

Recognizing spam scams

Generally, there are a few indicators which can help you identify spam (unsolicited emails) in your mailbox. If a message fulfills at least some of the following criteria, it is most likely a spam message.

- Sender address does not belong to someone on your contact list.
- You are offered a large sum of money, but you have to provide a small sum first.
- You are asked to enter, under various pretenses (data verification, Financial operations), some of your personal data – bank account numbers, usernames and passwords, etc.
- It is written in a foreign language.
- You are asked to buy a product you are not interested in. If you decide to purchase anyway, please verify that the message sender is a reliable vendor (consult the original product manufacturer).
- Some of the words are misspelled in an attempt to trick your spam filter. For example, “vaigra” instead of “viagra”.

Rules

In the context of Antispam solutions and email clients, rules help to manipulate email functions. They consist of two logical parts:

1. Condition (e.g., an incoming message from a certain address or with a certain email subject)
2. Action (e.g., a removal of the message or a transfer to a specified folder)

The number and combination of rules varies with the Antispam solution. These rules serve as measures against spam (unsolicited email). Typical examples:

1. Condition: An incoming email message contains some of the words typically seen in spam messages
2. Action: Delete the message

1. Condition: An incoming email message contains an attachment with an .exe extension
2. Action: Delete the attachment and deliver the message to the mailbox

1. Condition: An incoming email message arrives from your employer
2. Action: Move the message to the “Work” folder

In order to facilitate administration and to filter spam more effectively, we recommend that you use a combination of the rules in Antispam programs.

Whitelist

In general, a whitelist is a list of items or persons who are accepted, or have been granted permission. The term email whitelist (allowed addresses) defines a list of contacts from whom the user wishes to receive messages. Such whitelists are based on keywords searched for in email addresses, domain names, or IP addresses.

If a whitelist works in “exclusivity mode“, then messages from any other address, domain, or IP address will not be received. If a whitelist is not exclusive, such messages will not be deleted, but filtered in some other way.

A whitelist is based on the opposite principle to that of a blacklist. Whitelists are relatively easy to maintain, more so than blacklists. We recommend that you use both the Whitelist and Blacklist to filter spam more effectively.

Blacklist

Generally, a blacklist is a list of unaccepted or forbidden items or persons. In the virtual world, it is a technique enabling acceptance of messages from all users not present on such a list.

There are two types of blacklist: Those created by users within their Antispam application, and professional, regularly updated blacklists which are created by specialized institutions and can be found on the Internet.

It is essential to use blacklists to successfully block spam, but they are difficult to maintain, since new items to be blocked appear every day. We recommended you use both a whitelist and a blacklist to most effectively filter spam.

Exception

The Exception list (also known as List of Exceptions) usually contains email addresses that may be spoofed and used for sending spam. Email messages received from addresses listed in the Exception list will always be scanned for spam. By default, the Exception list contains all email addresses from existing email client accounts.

Server-side control

Server-side control is a technique for identifying mass spam based on the number of received messages and the reactions of users. Each message leaves a unique digital footprint based on the content of the message. The unique ID number tells nothing about the content of the email. Two identical messages will have identical footprints, while different messages will have different footprints.

If a message is marked as spam, its footprint is sent to the server. If the server receives more identical footprints (corresponding to a certain spam message), the footprint is stored in the spam footprints database. When scanning incoming messages, the program sends the footprints of the messages to the server. The server returns information on which footprints correspond to messages already marked by users as spam.

Advanced Memory Scanner

Advanced Memory Scanner works in combination with Exploit Blocker to strengthen protection against malware that has been designed to evade detection by antimalware products through the use of obfuscation and/or encryption. In cases where ordinary emulation or heuristics might not detect a threat, the Advanced memory

Scanner is able to identify suspicious behavior and scan threats when they reveal themselves in system memory. This solution is effective against even heavily obfuscated malware.

Unlike Exploit Blocker, Advanced Memory Scanner is a post-execution method, which means that there is a risk that some malicious activity could have been performed before it detecting a threat; however in the case that other detection techniques have failed, it offers an additional layer of security.

Banking & Payment Protection

Banking & Payment protection is an additional layer of protection designed to protect your financial data during online transactions.

ESET Smart Security Premium and ESET Internet Security contain a built-in list of predefined websites that will trigger a secure browser to open. You can add a website or edit the list of websites in the product configuration.

Turn on Secure all browsers to start all supported web browsers in a secure mode.

For more details about this feature, read the following ESET Knowledgebase articles:

- How do I use ESET Banking and Payment protection?
- Pause or disable Banking & Payment Protection in ESET Windows home products
- ESET Banking & Payment protection—common errors

The use of HTTPS encrypted communication is necessary to perform protected browsing. Banking & Payment Protection is supported by the following browsers:

- Internet Explorer 8.0.0.0
- Microsoft Edge 83.0.0.0
- Google Chrome 64.0.0.0
- Firefox 24.0.0.0

Open Banking & Payment Protection in your preferred web browser

When you open Banking & Payment Protection directly from the **Tools** tab in the product menu, it is opened in the web browser that you set as default in Windows. Otherwise, when you open your preferred web browser (not from the product menu), websites from the protected websites list will be redirected to the same type of web browser secured by ESET.

Botnet Protection

Botnet Protection discovers malware through analyzing its network communication protocols. Botnet malware is changing frequently in contrast to network protocols, which have not changed in the last couple of years. This new technology helps ESET defeat malware which tries to avoid detection and tries to connect your computer to botnet network.

DNA Detections

Detection types range from very specific hashes to ESET DNA Detections, which are complex definitions of malicious behavior and malware characteristics. While the malicious code can be easily modified or obfuscated by attackers, the behavior of objects cannot be changed so easily and ESET DNA Detections are designed to take advantage of this principle.

We perform deep analysis of the code and extract “genes” that are responsible for its behavior and construct ESET DNA Detections, which are used to assess potentially suspect code, whether found on the disk or in the running process memory. DNA Detections can identify specific known malware samples, new variants of a known malware family or even previously unseen or unknown malware which contains genes that indicate malicious behavior.

ESET LiveGrid®

ESET LiveGrid® (built on the ESET ThreatSense.Net advanced early warning system) utilizes data that ESET users have submitted worldwide and sends it to the ESET Research Lab. By providing suspicious samples and metadata from the wild, ESET LiveGrid® enables us to react immediately to the needs of our customers and keep ESET responsive to the latest threats.

ESET malware researchers use the information to build an accurate snapshot of the nature and scope of global threats, which helps us focus on the right targets. ESET LiveGrid® data plays an important role in setting priorities in our automated processing.

Additionally, it implements a reputation system that helps to improve the overall efficiency of our anti-malware solutions. A user can check the reputation of running processes and files directly from the program's interface or contextual menu with additional information available from ESET LiveGrid®. When an executable file or archive is being inspected on a user’s system, its hashtag is first compared against a database of white- and blacklisted items. If it is found on the whitelist, the inspected file is considered clean and flagged to be excluded from future scans. If it is on the blacklist, appropriate actions are taken based on the nature of the threat. If no match is found, the file is scanned thoroughly. Based on the results of this scan, files are categorized as threats or non-threats. This approach has a significant positive impact on scanning performance. This reputation system enables effective detection of malware samples even before their signatures are delivered to the user’s computer via an updated virus database (which happens several times a day).

In addition to the ESET LiveGrid® reputation system, ESET LiveGrid® feedback system collects information about your computer related to newly detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the filename, the date and time, the process by which the threat appeared on your computer and information about your computer‘s operating system.

ESET LiveGrid® servers

Our ESET LiveGrid® servers are located in Bratislava, Vienna, and San Diego; however, those are only the servers that are responding to requests from the clients. Submitted samples are processed in Bratislava, Slovakia.

Enable or disable ESET LiveGrid® in ESET products

For more detailed and illustrated instructions on how to enable or disable ESET LiveGrid® in ESET products, visit our ESET Knowledgebase article.

Exploit Blocker

Exploit Blocker is designed to fortify commonly exploited application types such as web browsers, PDF readers, email clients and Microsoft Office components. It works by monitoring the behavior of processes for suspicious activity that might indicate an exploit.

When Exploit Blocker identifies a suspicious process, it immediately stops the process and records and sends threat data to the ESET LiveGrid® cloud system. This data is processed by the ESET Research Lab and used to better protect all users from unknown threats and zero-day attacks (newly released malware without a pre-configured remedy).

Java Exploit Blocker

Java Exploit Blocker is an extension to the existing Exploit Blocker technology. It monitors Java and is looking for an exploit-like behavior. Blocked samples can be reported to malware analysts, so they can create signatures to block them on different layers (URL blocking, file download, etc.).

Machine learning

ESET has been working with machine learning algorithms to detect and block threats since 1990. Neural networks were added to ESET product's detection engine in 1998.

Machine learning includes DNA detections, which use models based on machine learning to work effectively with or without cloud connection. Machine learning algorithms are also a vital part of the initial sorting and classification of incoming samples as well as placing them on the imaginary “cyber-security map”.

ESET has developed its own in-house machine learning engine. It uses the combined power of neural networks (such as, deep learning and long short-term memory) and a handpicked group of six classification algorithms. This allows it to generate a consolidated output and help correctly label the incoming sample as clean, potentially unwanted or malicious.

The ESET machine-learning engine is fine-tuned to cooperate with other protective technologies such as DNA, sandbox and memory analysis as well as with the extraction of behavioral features, to offer the best detection rates and lowest possible number of false positives.

Scanner configuration in ESET product's Advanced setup

- ESET Windows home products (from version 13.1)
- ESET Windows endpoint products (from version 7.2)

Network Attack Protection

Network Attack Protection is an extension of the Firewall that improves the detection of exploits for known vulnerabilities at the network level. By implementing detections for common exploits in widely used protocols such as SMB, RPC and RDP, it constitutes another important layer of protection against spreading malware, network-conducted attacks and exploitations of vulnerabilities for which a patch has not yet been released or

deployed.

Ransomware Shield

Ransomware Shield is a behavior-based detection technique that monitors behavior of applications and processes that try to modify files in the way common for ransomware/filecoders. If an application´s behavior is considered malicious, or the reputation-based scanning shows an application to be suspicious, the application is blocked and process is stopped, or the user will be asked to block or allow it.

ESET LiveGrid® must be enabled for Ransomware Shield to function properly. See our ESET Knowledgebase article to ensure that ESET LiveGrid® is enabled and working in your ESET product.

Script-Based Attacks Protection

Script-Based Attacks Protection consists of a protection against javascript in web browsers and the Antimalware Scan Interface (AMSI) protection against scripts in Powershell.

HIPS
HIPS must be enabled for this feature to work.

Script-Based Attacks Protection supports the following web browsers:

- Mozilla Firefox
- Google Chrome
- Internet Explorer
- Microsoft Edge

Use a supported web browser
The minimum supported versions of web browsers may vary because the file signature of browsers change quite often. The latest version of a web browser is always supported though.

Secure Browser

Secure Browser is an additional layer of protection designed to protect your sensitive data while browsing online (for example, financial data during online transactions).

ESET Endpoint Security 8 and later contains a built-in list of predefined websites that will trigger a protected browser to open. You can add a website or edit the list of websites in the product configuration. Secure Browser is disabled by default after installation.

For more details about this feature, read the following ESET Knowledgebase article.

The use of HTTPS encrypted communication is necessary to perform protected browsing. To use Secure Browser, your web browser must meet the minimum requirements below:

- Internet Explorer 8.0.0.0
- Microsoft Edge 83.0.0.0

- Google Chrome 64.0.0.0
- Firefox 24.0.0.0

Open ESET Secure Browser in your preferred web browser

When you open ESET Secure Browser directly from the **Tools** tab in the product menu, ESET Secure Browser is opened in the web browser that you set as default. Otherwise, when you open your preferred web browser (not from the product menu), the ESET internal list will be redirected to the same type of web browser secured by ESET.

UEFI Scanner

Unified Extensible Firmware Interface (UEFI) Scanner is part of the Host-based Intrusion Prevention System (HIPS) that protects UEFI firmware on your computer. The UEFI firmware loads into memory at the beginning of the boot process. The code is on a flash memory chip soldered onto the mainboard. By infecting it, attackers can deploy malware that survives system reinstallations and reboots. The malware can also easily remain unnoticed by antimalware solutions as most of them are not scanning this layer.

UEFI Scanner is enabled automatically. You can also start a computer scan manually from the main program window by clicking **Computer scan** > **Advanced Scans** > **Custom Scan** and selecting the **Boot sectors/UEFI** target.

> If your computer has already been infected by UEFI malware, read the following ESET Knowledgebase article:
> My computer is infected with UEFI malware, what should I do?

Deadlock

A deadlock is a situation where each computer process waits for a resource that is assigned to another process. In this situation, none of the processes get executed since the resource required is held by another process that is also waiting for another resource to be released. It is important to prevent a deadlock before it can occur. A deadlock occurrence can be detected by the resource scheduler, which helps the operating system keep track of all the resources allocated to different processes. Deadlock can occur if the following four conditions hold simultaneously:

- **No preemptive action** – A resource can be released only voluntarily by the process holding it after that process has finished its task.
- **Mutual exclusion** – A special type of binary semaphore used to control access to the shared resource. It enables current higher priority tasks to be kept blocked for the shortest time possible.
- **Hold and wait** – In this condition, processes must be stopped from holding single or multiple resources while simultaneously waiting for one or more others.
- **Circular wait** – It imposes a total ordering of all resource types. Circular wait also requires that every process request resources in increasing order of enumeration.

There are three ways to handle a deadlock:

- Do not let the system into a deadlock state.
- Let the deadlock occur, then do preemption to handle it when occurred.
- If a deadlock occurs, reboot the system.