Malware

This article is an introduction to the world of malware. It explains how malware works in general, and also discusses the most common routes of infection and harmful behaviour patterns. In the process, we explain how our "5 steps for your digital security" will provide effective protection each time.

The most important points to remember:

- Malware denotes computer programs with undesirable and frequently harmful functions.
- There are different types of malware, requiring different preventative measures.
- Over the past years, risks posed by malware have increased further.
- You can effectively reduce such malware risks by following our "5 steps for your digital security (https://www.ebas.ch/en/5-steps-for-your-digital-security/) ".

Malware – an undesirable computer program

The word "malware" is an umbrella term for computer programs usually created deliberately to harm users.

Similar to conventional software, malware creation and distribution methods have also developed further. The former is increasingly pursued at a professional level, contributing to a higher volatility of malware developments. An increasingly targeted approach is also used to then spread this malware. Private individuals and SME are subject to systematic attack.

Infection

Similar to other computer programs, malware is nothing but a series of instructions executed by a computer.

To exert its harmful impact, malware will therefore have to be executed by the system. This either involves users or programs already running giving instructions to do so.

It is a well-known fact that the former happens when users are led to believe that they can either benefit or avoid harm this way. Malware executed in this manner is denoted by the umbrella term Trojan Horse, or Trojan for short. It masquerades as a useful program and is generally initiated by users themselves. Once executed, it takes full harmful effect.

And this doesn't necessarily have to involve executable program files in the classic sense. Office documents and PDF files can also contain so-called macros, which are executed by this software.

Such attempted deception can often be exposed and prevented by taking our "Step 5 – Exercising care and remaining alert (https://www.ebas.ch/en/5-exercising-care-and-remaining-alert/) ".

If malware is executed by a program already running without any user action, this happens by exploiting a so-called security gap, or vulnerability. This is an error in a program's logic which could affect security.

Vulnerabilities in browsers (https://www.ebas.ch/en/browsers/) for instance allow for so-called drive-by downloads (https://www.ebas.ch/en/drive-by-download/) to occur. Operating system vulnerabilities are often exploited, too, for in-

stance to infiltrate a device via external data carriers such as USB sticks or a network. Malware spreading autonomously via such vulnerabilities is called a worm.

Software manufacturers regularly fix such vulnerabilities by providing updates. The most important measure to take to prevent a malware infection is therefore considered to be "Step 3 – Preventing with software updates (https://www.ebas.ch/en/3-preventing-with-software-updates/) ".

Once executed, most malware variants seek to ensure they can run their malicious code time and again, employing a variety of methods. A virus will write its own malware code into other programs to do so. So-called rootkits will directly infiltrate your operating system code.

Damaging effects

You cannot completely avoid all risks of catching a malware infection. It is therefore recommended you also take measures in case there is a successful infection.

Below we will introduce some common damage scenarios and explain how the harm caused can be mitigated by following our "5 steps for your digital security (https://www.ebas.ch/en/5-steps-for-your-digital-security/) ".

System slowdown

The fraudulent abuse of system and network resources can slow you down considerably when you are working on an infected device, or even make doing so impossible altogether. The one type of malware with a huge effect on system performance is that created for such purposes as mining cryptocurrency (Crypto Miner), cracking passwords, or carrying out attacks on other systems (for instance Distributed Denial of Service).

This type of malware benefits from infecting the largest number of systems possible, which are then combined into a so-called botnet.

Such malware is designed to wreak havoc on a system over the longer term, and should be discovered by your anti-virus software sooner or later. For this to work properly though, you will have to make sure to regularly update it and run repeated complete scans of your whole system. You can find further information on this under "Step 2 – Monitoring with antivirus software and firewall (https://www.ebas.ch/en/2-monitoring-with-antivirus-software-and-firewall/) "

Ad displays

Programs known as adware make themselves unpopular with their victims by continuously displaying ads.

If a system is plagued by an uncommonly high number of ads, this might indicate another kind of malware infection and should serve as an opportunity to clean your system (https://www.ebas.ch/en/clean-windows-10-installation/) .

If the ads displayed are limited to websites only, and are only shown inside your browser, it could be worthwhile following up on our tips for increased levels of privacy and data protection on the Internet (https://www.ebas.ch/en/privacy-and-data-protection-on-the-internet/) , or on how to use an adblocker (https://www.ebas.ch/en/ad-blocker-and-anti-tracking-tools/) .

Data collection

Malware with spyware properties is characterised by specifically collecting and passing on information about its victims. This could for instance entail analysing your surfing habits, capturing keystrokes (keylogger) or stealing sensitive data.

To mitigate the risk of spyware activities, we recommend you segment your own digital activities, and only disclose

your data very sparingly. By following our "Step 4 – Protecting online access (https://www.ebas.ch/en/4-protecting-online-access/) ", you can effectively reduce the extent of damage caused by a successful spyware attack. Using two-factor authentification for instance ensures your e-banking account is not automatically compromised in case your password is captured.

Encryption or destruction of data

Data encryption is mainly used as leverage for blackmail attempts by so-called ransomware.

Once you have cleaned your system, usually the only remedy here is to restore your data from a back-up you have created previously. "Step 1 – Backing up data (https://www.ebas.ch/en/1-backing-up-data/) " is the cornerstone for successful data recovery.

Combined attacks

Malware does not just limit itself to the scenarios described above. Several of these approaches can for instance be combined, or completely new approaches developed.

The former is achieved with the help of so-called downloaders, which will download further malware to the system under attack automatically or upon request.

One prominent example for a combined attack are blackmail attempts where spying out a targeted system is the first step, with its data then being encrypted in a second step. This allows blackmailers to exert more pressure on their victims, for instance by threatening to publish the data captured, or to pass them on to a competitor.

Identification and cleaning

If you follow our "5 steps for your digital security (https://www.ebas.ch/en/5-steps-for-your-digital-security/) ", you will effectively reduce the risk of a malware infection occurring, and of any ensuing damage scenarios, too.

You cannot however completely rule out any such risks completely. Read our article on "Malware infections (https://www.ebas.ch/en/malware-infection/) " to find out how to recognise and resolve an infection.

"Malware" is a term used to denote computer programs developed to execute undesirable and potentially harmful functions on a victim's device. The term is a combination of "malicious" and "software".