Avast Business

Ebook

Malware 101

Everything you need to know about malicious software

15 November 2023

Avast Business

Nowadays, we're no longer able to imagine a world without modern technology. Nearly everyone uses mobile devices every day and businesses can no longer operate without the internet. This modern age, comes with modern risks. Are you aware of the risks of Malware? Do you know how it gets into your system and how you can prevent it? Everything you need to know about Malware and how to protect yourself is covered in this eBook.

What is Malware?

Malware is a term used for Malicious Software. This software can get into your computer and perform actions without your permission, giving hackers full access to your machine. You could compare it to a common cold. You probably can't remember the exact time you got infected and it may even stay dormant. However, once it's active, you start to notice the damage its actually doing. Just like a cold, malware changes over time. It develops constantly and fi nds new ways to access your device or go around your antivirus software.

Malware was initially designed as a form of cyber vandalism, breaking computers or changing your background. It has since been adopted by cyber criminals and is used to hold fi les for ransom, steal passwords to access bank accounts or track information to steal identities.

How does Malware affect me?

Malware can affect almost any device, from your computer, phone or tablet all the way to larger systems, such as servers and databases. It is not limited to devices that are on-line either, malware can get into debit card readers, POS systems, ATMs and other types of devices via a usb, infected cards, or even loaded on at the factory. Malware is also a growing threat to small and medium businesses.

Malware causes damage to your device or software, which might mean your device will not operate the way it used to or might even shut down completely. Other types of malware, known as ransomware, lock or delete fi les. Malware can also lead to your personal or organizational information falling into the wrong hands. For businesses, even small ones, this could result in fines, loss of customers, and reputational damage.

Want to understand the terms people use when talking about malware?
Please read out glossary at the end of this eBook!

Avast Business

Types of malware

Malware comes in all shapes and sizes. Again, think of a cold; there's the flu, a stomach bug, a sinus infection; they all have different symptoms and treatments. This chapter will explore the most common types of malware and how to recognize them.:

Ransomware

Ransomware locks your files and demands you to pay a ransom to unlock your files. This type of malware is rapidly becoming more advanced. Sometimes it even starts deleting fi les as soon as you are infected pressuring you to pay up.

Trojans

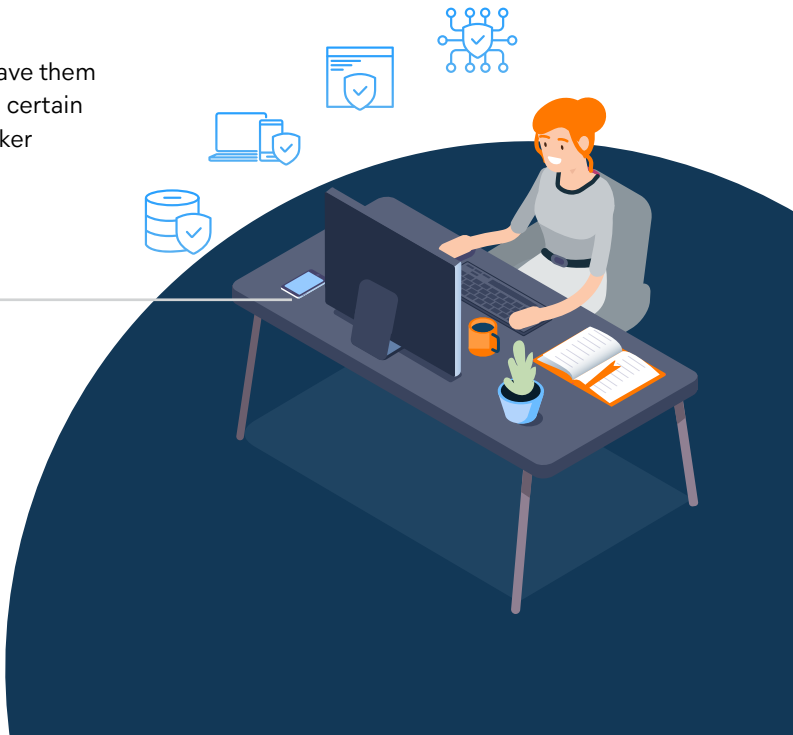
It's already in the name; Trojans behave like a Trojan horse in the Greek tale. The soldiers hid inside of the horse to penetrate the city wall of Troy and waited until nightfall to attack. A Trojan works exactly the same. They disguise themselves as a trusted program to get into your system and attack later.

Worms

Worms are renowned for the amount of damage it does to your device. This mainly due to the fact that worms are self-replicating. They continue to spread through your computer, without you having to do anything. A worm infection can even spread to an entire network.

Key loggers

Key Loggers track your keystrokes and save them in a hidden file on your computer. After a certain amount of time the file is sent to the hacker automatically, who will use the keystroke data to get your passwords or personal information.



Avast Business

Types of malware (continued)

Bots

The name "Bot" comes from the word "robot." This type of malware often automates tasks and provides information like a robot does. They are used to gather information through chats, IM's or similar web based programs. Bots can also be used for attacking websites often in the form of bot nets where a hacker controls multiple bot infected computers. A hacker can use the bot net to blast comment sections of blogs by submitting spam, overload servers by generating huge amounts of traffi c, or quickly attempt a trial and error approach to cracking passwords on secure sites.

Rootkit

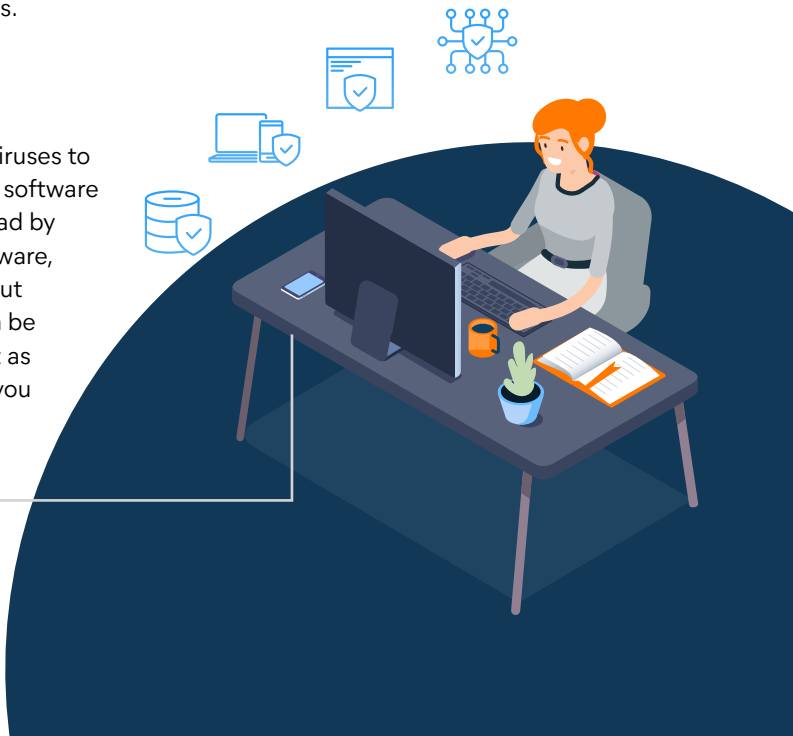
A RootKit is able to remotely access or control a computer without being detected by users or security programs. This way cyber criminals are able to execute fi les, steal information, modify configurations, alter software, or even install more malware. A RootKit is very diffi cult to remove, so prevention is key!

Spyware

This type of malware spies on user activity, from collecting keystrokes to browser history to data harvesting. However, spyware often has additional capabilities as well, ranging from modifying your security settings to interfering with network connections. Spyware spreads by bundling itself with trusted programs or by using Trojans.

Virus

Most people have heard of viruses. For viruses to be effective you actually need to run the software that contains the virus. They do not spread by disguising themselves as legitimate software, but often are files that contain nothing but the malicious code. However, viruses can be embedded in a Word or Excel document as a macro. The virus will be enabled once you agree to enable macros.



Avast Business

Malware attacks explained

Most types of malware require a user to open the door. This means that you will first have to perform an action, in order to get infected with malware. Malware can be very clever and trick you into inviting them in.

Email

You have probably seen emails with subject lines like "You Have Won…","Past Due Invoice","Your Refund has been approved." or have received a message from someone you don't know. Often, these types of emails contain malicious software or a link that enables malware. Using Social Engineering, the message just has to be interesting enough to have you click. The best thing to do when you receive these emails, is delete them.

Websites

Malware can also spread through websites. These websites can include pop-up advertisements, that launch malware when you click on them. Malware can also be hiding behind links to free gambling, clothing deals or warnings that appear on your screen claiming that you have a virus. If something appears too good to be true or if seems untrustworthy, don't click it.

Opening The Backdoor

Programs or operating systems you are using may have weaknesses. These weaknesses or vulnerabilities allow a person who is technically inclined to make changes to the program from outside of the device. These vulnerabilities are very dangerous, as hackers can gain direct access to your computer to launch the type of malware they prefer. In some cases, the hacker can even disable your antivirus software. That's why it is important to always ensure you are running the most up to date versions of your operating system and software, ensuring that known vulnerabilities are minmized.

Avast Business

Shut your doors to malware

Prevention is cheaper than the alternative. There are a few ways to protect yourself and your business from a malware infection.

Update

Keep your operating system software and 3rd party applications (Adobe Reader, Adobe Flash, Microsoft Offi ce, etc.) up to date, to ensure all possible vulnerabilities are covered.

Back Up Your Files

You want your files to be available at all times. It is important to back up your fi les regularly. By using an external drive or the cloud to do so, you will ensure the malware attack cannot spread to your back up as well.

Know How To Spot Malware

Now that you know the types of links to avoid in an email or on a web page, it should be easier to prevent malware attacks. When in doubt, always delete the email or close the web page.

Educate Your Employees

Transfer this knowledge to your employees so they also know how to spot a malware attack once they see one. Most attacks succeed through human error or uninformed clicking.

Create Policies For Reporting And Dealing With Malware

When an employee receives a malicious email or spots a fi le that contains malware, they should know where to report this or how to deal with it. By knowing when one of your employees or co-workers has been attacked, you can prevent others from inviting malware into your business.

Use A Good Multi-Layer Antivirus Program

Not all antivirus solutions are able to scan fi les to a level that can actually prevent a malware attack. Make sure you use protection that utilizes a multi-layered approach to detecting and eliminating malware.

Avast Business

Here's how Avast Business by protects you

1 Business Never Slows Down. Neither Do We

Stop threats and keep your business moving. With Avast Business award winning products, you'll protect your business from the latest viruses and threats.

2 Save time and focus on your business

Avast Business solutions minimize security distractions so you and your employees can focus on driving your business forward.

3 Keep employees safe online with network antivirus

Free your workforce to surf, search and download with confi dence. Smart prevention technology checks every web page and alerts you if it detects anything suspicious.

4 Keep customer information safe from hackers

Maintain your integrity as a reliable business partner by ensuring all your customer data is kept private and all online transactions are conducted safely.

5 Secure and manage your computers from a single console

Manage your Avast Business Antivirus software remotely on your business network and stay in control no matter where you are. Easily deploy and manage your network antivirus software on your PCs and laptops.

6 Free phone support

Breathe easy knowing that Avast Business experts are always a phone call away.

7 Smart, actionable alerts

Detects and alerts you to problems that you can address easily from the simple dashboard.

8 Trust avast business to protect your businesses!

To learn how Avast Business can help protect your business from malware visit us at avast.com

Avast Business

Glossary of malware terms

Advanced persistent threat:

an adversary that possesses sophisticated levels of expertise and signifi cant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.G., Cyber, physical, and deception)

Antispyware software:

a program that specializes in detecting and blocking or removing forms of spyware

Antivirus software:

a program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents. Sometimes by removing or neutralizing the malicious code

Behavior monitoring::

observing activities of users, information systems, and processes and measuring the activities against organizational policies and rule, baselines of normal activity, thresholds, and trends

Code:

all files are made of code

Dark web:

underground network that has controlled access that can be used for buying and selling of user data and malicious code

Encryption:

to protect and lock data from being tampered with and read

Decrypt:

is unencrypted reversing the encryption see above

Hacktivist:

someone who hacks someone for political gain rather than financial

Nation state:

an attack funded by a government or political movement

Script kiddy:

someone in his bed room, students that write malicious code

Threat landscape:

all the different types of attacks that are in use.

Threat surface:

the part of your network or devices that are attacked. Macines without Antivirus, unpatched operating systems, devices with default passwords.

Threat vectors:

the different ways that an attack happens; email with a link, email with attachments, malicious links on web pages, redirection to malicious websites, pop-ups.

About Avast Business

Avast delivers easy-to-use, affordable, and award-winning cybersecurity solutions for small and growing businesses. Avast provides integrated security services to protect your devices, data, applications, and networks. Backed by 30 years of innovation, we have one of the largest, most globally dispersed threat detection networks in the world. Our cybersecurity solutions are built to provide maximum protection so that you can worry less about cyberthreats and focus more on growing your business. For more information about our cybersecurity solutions, visit **www.avast.com/business**.