Let us take you on a journey into the world of Malware...

Click to continue

Learn what drives the evil minds to threaten your computer every day.

We want to equip you with the knowledge to stay safe online!

Fact #1:

The Internet is a more dangerous place than you may think it is.

Why?

Well, today there are not only hackers and malware writers.

But also:
fraudsters,
blackmailers,
money launderers!

And lately more and more unethical freeware software vendors who want to mess your PC up with stuff you don’t need.

“How do they affect me?”

- you may ask.

Here’s a secret:

Fact #2:

Everyone knows viruses…

viruses that spread invisibly…

destroying your files…

made by evil hackers who make fun of you.

But those viruses hardly exist anymore!

Fact #3:

Today we face a wide variety of threats.

Threats that are more sneaky and nasty.

They all have one thing in mind:

Cash!

It’s all about the money.

-

Your money!

These are the top 3 infection scenarios that happen thousands of times every day:

1. Wiping your bank account

You get an email from a well known parcel service, asking you whether the package described in the attached document is expected.

You open the attached PDF file and nothing really happens.

But the email was forged and the attachment was an exploit program that already invisibly manipulated your browser.

You don’t realize that anything bad happened and continue your work.

There is an invoice due today...

You login to your online banking portal and send a payment through the “secure” interface as usual.

Then you check your account balance again and everything looks fine. Your payment was processed as expected - it seems.

What you don’t know: Your bank account is already wiped.

How?!

A financial trojan manipulated the bank’s website.

Instead of executing your transfer, it sent all your money to a fraudster bank account.

Your balance page was manipulated to simulate legitimate transactions.

The scary truth is: Unless your bank gives you a call reporting unusual activity, you won't even know about the theft.

You probably wouldn’t realize until it’s far too late to cancel the transaction.

And then you'd spend weeks getting everything sorted, back to a normal life.

Note: Even PIN confirmations sent to your cell phone are not safe. Several banking trojans for mobiles grab and forward them to the fraudsters.

2. Turning your computer into a zombie bot

A hacker opens up a webserver that was not updated properly and starts manipulating the hosted websites.

While surfing around you see a warning popup on a website telling you to install the latest Flash Player, and you click “OK” to start the update.

But you actually downloaded a tiny trojan dropper onto your PC that already started to hide and begin its harmful actions.

The dropper loads a larger trojan component that converts your PC into a zombie, that waits for instructions from its “master”.

You don’t get suspicious since the PC behaves as usual. No files are damaged, no slow-down can be noticed.

What you don’t know: Your PC is now part of a botnet of 100,000 computers. Together they have an incredible computing power.

Hackers sell that computing power to spammers, blackmailers and others.

A spam bot can drop thousands of emails every day without anyone noticing it. Your new broadband internet does a great job!

Blackmailers can instruct many thousands of bots to connect simultaneously to a company website, overloading it until the owner pays a ransom.

You may not care about all these things, but bots can do much more.

Just think of a cheap data storage for illegal content. Copyrighted data, child porn, terrorism support, fraud, just to name a few.

You would never know about all that's happening on your home computer - until the police knock at your door.

You are responsible for what’s going on on your PC!

3. Forced to pay a ransom

An attacker finds an easy way to drop a little program on your computer because it misses the latest Java Runtime update.

While you are away from your PC, the program starts to encrypt all your data files with a really strong encryption method.

Once it has finished its job, a scary full screen window becomes visible.

You have to pay a $600 ransom to an anonymous Bitcoin or uCash account to get the password for decryption.

Unfortunately there is no possible way to crack the password in less than 50 million years. The password is stored on a webserver you can’t access.

You can either pay or lose all your data if you don’t have recent backups stored on external devices.

Unbelievable, isn’t it?

Well, that’s what we deal with day by day.

To be more precise:
We deal with 300,000 of them.

Every single day!

And we’re really good at it. :)

- At least the antivirus testing agencies say so. -

“So, how shall I protect myself from all those attacks?”

You should use a reliable anti-malware with real-time protection enabled - and not just rely on free cleanup tools.

Use protection software you can trust without restrictions - one that doesn’t mess up your browser.

But one that prevents you from accessing websites that distribute malicious stuff.

Use protection with two major virus- and malware-scanning engines for the best possible detection.

Protection that implements state-of-the-art behavior blocking technology to stop brand new threats.

And also keeps your computer clean from unwanted programs like adware, tracking tools and useless browser toolbars.

Then you will be safe online.

Convince yourself now:

Emsisoft Anti-Malware

Download a free trial here

EMSISOFT