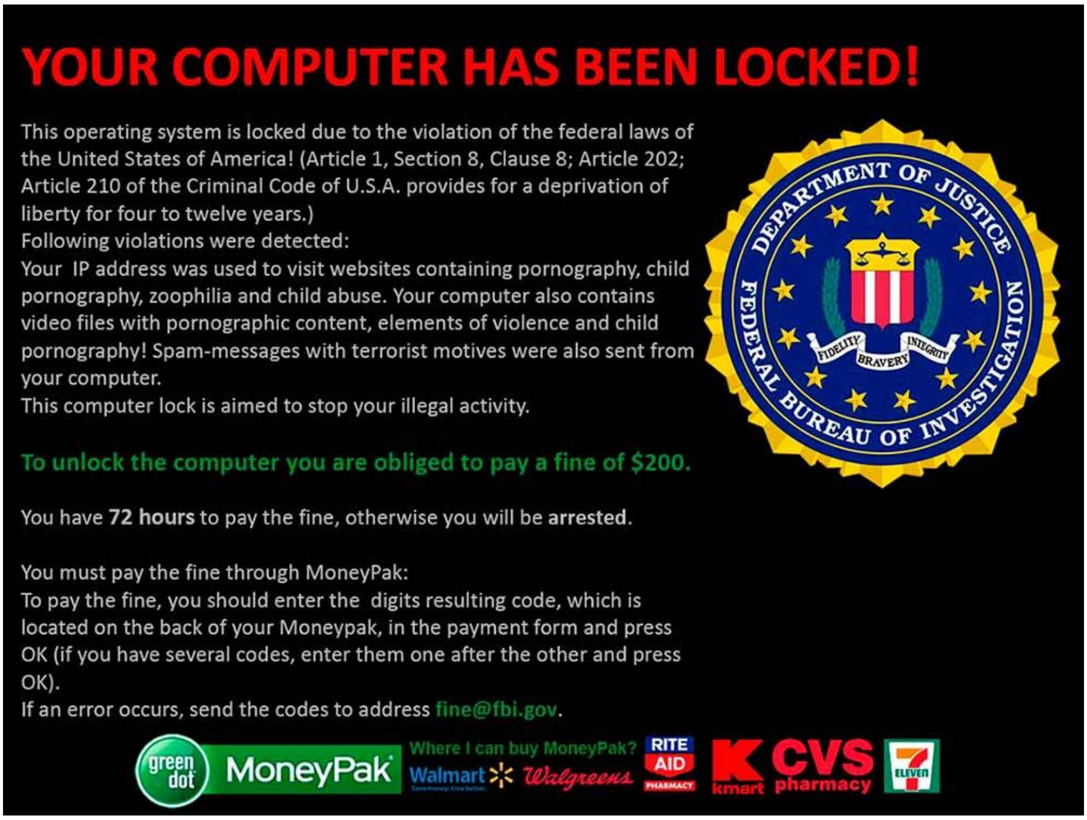
KASPERSKY lab

Anti-Blocker technology: effective protection against Windows Blockers

It’s difficult to imagine life without a computer, cut off from access to programs, movies, music, games and websites. The computer has long become a household appliance which takes its place in almost every family.

Unfortunately, this has not escaped the attention of cybercriminals who make their business developing and spreading malware. One of their tools is the so-called Trojan blocker family, which hinders or in some cases completely blocks the operation of key applications - or even the whole computer. The scam is simple – having blocked a computer, the fraudsters extort money from users to pay for unblocking the system. Trojan blockers are typically concealed in music files, images, videos etc.

Although malicious Trojan blockers appeared almost a decade ago, they are still regularly used for malware attacks on users.



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be **arrested**.

You must pay the fine through MoneyPak:
To pay the fine, you should enter the digits resulting code, which is located on the back of your Moneypak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

Even though these programs are well-known, and routinely detected by antivirus products, more and more of them are appearing. One reason for this growth is that even on protected computers users often fall victims to such attacks because they ignore the warnings of their antivirus programs and download and run files that look like, for example, an mp3 sound recording but in fact is a malicious Trojan blocker.

However the main reason for the upsurge is that very often people give in to blackmail and pay the required sum, encouraging cybercriminals to launch such attacks again and again.

Ransomware forms and anatomy

There are relatively few malicious programs of this type and most of them are very primitive. However the fraudsters have recently started using rather complex blockers. For example, one of them displays a window demanding the ransom on top of all other windows opened by the user. Any attempts to deactivate it using built-in Windows tools such as Task Manager are suppressed.

Yet another variation – a more dangerous one – makes it impossible for users to perform any operation on the system. In this case, cybercriminals abuse the standard features available in Windows OS, introducing serious modifications to the user environment and thwarting any interaction with the system

In particular, these features allow the application to intercept any commands from the keyboard and the mouse connected to the computer. As a result, the computer is infected with these types of blockers and the user can no longer interact with the PC. Often users are forced to turn to third parties, using an uninfected computer to download an antivirus utility which can eliminate the problem or creating a boot disc which can restore the OS parameters of the infected computer.

In an effort to protect computers from all types of cyber threats, Kaspersky Lab has developed a convenient and efficient technology to easily and quickly combat even the most dangerous variations of Trojan blockers.

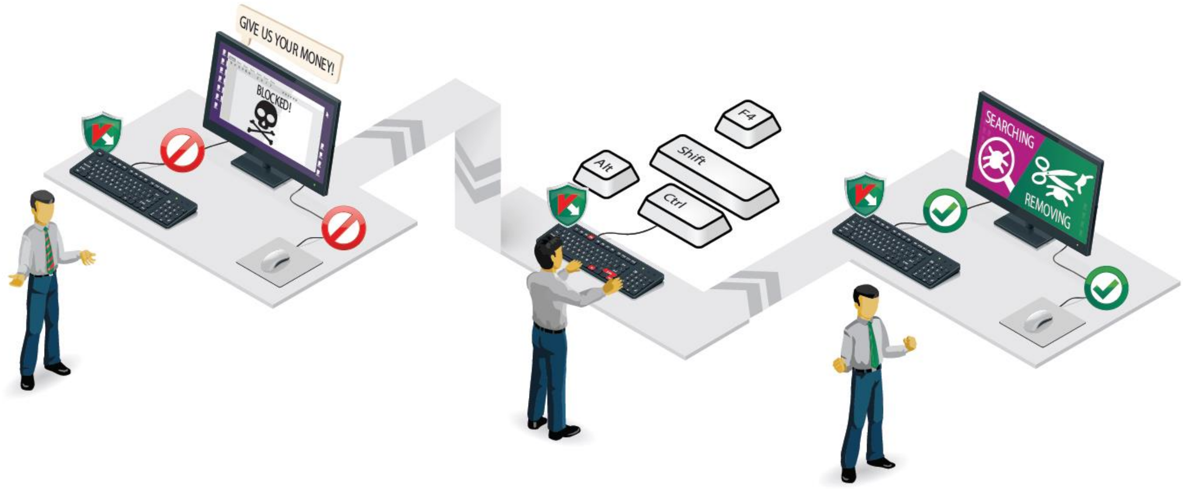
How Anti-Blocker works

The Anti-Blocker technology effectively combats this type of malware. This is achieved using two components – the Secure Keyboard driver and a set of heuristic algorithms capable of identifying and rolling back any changes the blocker makes to the OS.

The Secure Keyboard driver was initially developed to protect keyboard-entered user data from keyloggers. However, in tandem with Anti-Blocker it acts as a link between the user of the infected computer and Kaspersky Internet Security 2014. When Kaspersky Lab’s product is installed, the Secure Keyboard driver replaces the standard keyboard driver, thus ensuring a secure exchange of data between the keyboard and the antivirus solution. The driver receives signals from the keyboard and converts them into the commands "familiar" to Kaspersky Lab's product before transmitting them further, for example, to the login and password fields of social networking sites or online banking services. This ultimately eliminates the possibility of sensitive data interception. In Kaspersky Internet Security 2014, this technology has found a new use.

In fact, the blocker mechanism does not completely prevent the OS from receiving signals from the keyboard; it merely “locks” those signals into the blocker. However, with Secure Keyboard the signal passes through the driver before it reaches the malicious program. Both the Anti-Blocker technology and the Secure Keyboard driver are components of Kaspersky Internet Security 2014, ensuring that Kaspersky Lab’s product remains able to interact with users even if the system is infected by a blocker.

To activate the technology the user has to press the special key combination Ctrl + Alt + Shift + F4 (the activation also occurs following multiple Ctrl + Alt + Del keystrokes). Kaspersky Internet Security 2014 recognizes this keystroke as evidence that a blocker is in operation, and immediately activates the Anti-Blocker technology which, using a set of heuristic algorithms, identifies the processes launched by the malicious program and blocks them, enabling users to continue working smoothly on the computer. After that the blocker is removed from the operating system with the help of Kaspersky Internet Security 2014 antivirus tools.



Benefits of using Anti-Blocker

Anti-Blocker has a number of advantages such as:

- automatic protection against "sophisticated" blockers which can bypass the antivirus protection if the user unwittingly allows it;
- no need to use Live CD or any other third party assistance to treat the infection;
- if a blocker launches when the user is working with important information, Anti-Blocker allows him to save the data. Traditional methods of treating such infections require a reboot, which inevitably leads to the loss of important information.

Any high-quality anti-virus product is expected to protect the users against all types of threats while remaining easy to use. Kaspersky Internet Security 2014, which integrates Anti-Blocker technology to deal with the most dangerous Trojan blockers by pressing just four keys, is exactly what you need.

Availability

- Kaspersky Internet Security
- Kaspersky Internet Security – Multi-Device (for Windows only)
- Kaspersky Total Security – Multi-Device (for Windows only)