KASPERSKY lab

Protecting your PC against any malware using Kaspersky Lab's Trusted Applications technology

Computers and the Internet are no longer a minority interest. Just ten years ago, they were mostly used by enthusiasts who had a certain level of IT proficiency. However, technologies evolved, making PCs easier to use. New uses for computers emerged which made them attractive to ordinary, non-IT savvy people, not just enthusiasts. Communicating on social networks, buying goods online, downloading books, films, games and other content opened up the IT world, even for users with minimal knowledge of computer technologies. In other words, PCs and the Internet became part of people's everyday life much in the same way as telephones and TVs.

At the same time, while computers and the Internet were evolving towards maximum simplicity and user-friendliness, cyber-threats – Trojans, worms, viruses, spyware etc. – were becoming much more sophisticated and varied. This gives rise to a potentially dangerous situation: there are numerous Internet users who lack the necessary knowledge to avoid the multitude of cyber-threats – and numerous cyber-threats created by cybercriminals wishing to take advantage of users' naivety.

It goes without saying that this risk is greatly reduced by continually developing all sorts of security technologies. For each new threat, developers design effective means of neutralizing it. As a result, even inexperienced users who have a good security solution can use their computers and the Internet without significant risk.

But there are always exceptions. According to Kaspersky Security Network data, about 315,000 new malicious program samples appear globally every day. The vast majority of these malicious programs are essentially variations of other, known malware, so they pose no real threat if there is a regularly updated security solution installed on the computer. At the same time, a small proportion of this malware is new and previously unknown. This does not prevent various antivirus technologies from remaining effective: even new malware is quickly detected and blocked by antivirus solutions. At the same time, the likelihood – however minor – that some malicious programs will penetrate a user machine still remains. Is there a way to make this possibility vanishingly small? According to Kaspersky Lab experts, the solution is to combine protection technologies based on antipodal underlying principles.

Why Default Deny?

The main idea behind this method is simple: for obvious reasons blacklisting cannot provide 100% protection against cyber-threats, so why not complement it with whitelisting?

The most valuable quality of security solutions based on so-called 'white lists' is that this security scenario only allows legitimate and secure applications to run on the computer. All others – including malware – are blocked.

This approach to protection is known as Default Deny (blocking everything that is not allowed). It has proved to be an effective method of safeguarding the information security of corporate IT infrastructure. For example, according to a survey conducted jointly by B2B International, a research agency, and Kaspersky Lab in spring 2013 among companies across the globe, 62% of corporations use Application Control solutions based on the Default Deny principle.

At the same time, Default Deny is relatively rarely used in consumer security solutions due to an important issue: the approach is effective only if the 'white list' includes very nearly all of the programs a PC user protected by the solution might need. In the case of corporate customers, the number of known trusted applications is not as important, since the list of programs needed by employees to do their work is usually small and changes relatively infrequently.

For ordinary users, who might install and launch dozens of different new programs every day, this is a critical issue. A security solution based on the Default Deny principle can make life difficult for users by blocking legitimate applications that are missing from its 'white list'. In other words, although the Default Deny approach promises an extremely high level of protection, its practical implementation is fraught with a number of difficult-to-resolve issues: how do you determine which programs are legitimate and which are not? How do you stay on top of the constantly growing number of new applications appearing on the computer? How do you provide high-quality computer protection without needlessly inconveniencing the user?

In their quest for answers to these questions, Kaspersky Lab experts developed a unique technology that develops the Default Deny approach without complicating PC use.

Kaspersky Lab Trusted Applications technology

The technology is called "Trusted Applications". It is available as one of the features in security products for home users. Trusted Applications includes three main components:

- Dynamically updated 'white list' of applications (Dynamic Whitelisting), based on Kaspersky Security Network;
- A set of mechanisms for determining the trust status of each application (Trusted Chain), which includes a set of rules regulating which application trust inheritance and a constantly updated databases of security certificates and trusted domains;
- A 'trusted corridor' system to control individual applications.

Each of these components plays its own role in determining whether an application is trusted or not.

Dynamic Whitelisting

Dynamic Whitelisting is the main protection component based on the Default Deny method. Essentially, it is an extensive and constantly updated knowledge base of existing applications. The database contains information on about one billion unique files, covering the overwhelming majority of popular applications, such as office packages, browsers, image viewers etc.

The database is constantly updated using input from nearly 450 Kaspersky Lab partner companies specializing in software development. Close cooperation with software developers helps to keep the database up-to-date and, as a consequence, highly effective. Software developers regularly release updates for their products and this can affect the structure of their applications. In theory, this can lead to a security product generating false positives. However, information about upcoming changes in many applications is included in Kaspersky Lab's database before the relevant programs become available to users for download.

Naturally, even when using the most extensive application databases it is always possible that Kaspersky Lab's 'white list' will be missing data on a small number of legitimate programs, perhaps because a developer has not provided advance warning of the latest updates. This is why Trusted Applications includes two additional mechanisms for confirming program legitimacy: application trust inheritance and a further check against a database of trusted domains and certificates, which makes it possible to create a so-called 'trusted environment' on the computer.

Trusted chain

Trusted chain is a set of mechanisms that confirm or refute the legitimacy of an application based on certain characteristics, such as its compliance with application trust inheritance rules, the authenticity of the file's digital signature and whether the file was downloaded from a trusted source.

▶ Application trust inheritance principle

Many programs create other applications during their operation. Information about these applications may be absent from the Kaspersky Lab knowledge base. For example, in order to download an update a program may have to launch a specialized module, which will connect to the software vendor's server and download a new version of the program. In effect, the update module is a new application created by the original program and there may be no data on it in the Whitelisting database. However, since this application was created and launched by a trusted program, it is regarded as trusted.

▶ Digital signature

A program's update module might automatically download a new version of an application, and the 'footprint' of that new version could be different from the one in the Whitelisting database. However, its legitimacy can be determined based on other characteristics, e.g., by checking new files for the presence of unique digital signatures.

Many software vendors sign their program files using a unique digital signature, which protects the files from unauthorized modification. Kaspersky Lab analyses these signatures, rates their reliability and maintains a constantly updated database of security certificates used by software vendors to create digital signatures. This can determine whether a specific file's digital signature is genuine or not. If it is, the new version of the application is considered trusted. If any of these signatures are compromised they will be immediately removed from the database, even if the OS still regards them as trusted.

- **Verifying whether the source is trusted**

However, it is not uncommon for a file to have no unique signature. In this situation, Trusted Applications uses one more source – a trusted domains database – and searches it for the domain from which the file in question was downloaded. If the domain is on the list of trusted domains (in most cases, these are domains of well-known software vendors), the object being downloaded is also deemed legitimate.

In addition to software vendors' sites the trusted domains database includes distributor sites – file collections which have not been detected as sources of malware. If it turns out that one of these sites has been used to distribute malicious code, it is immediately removed from the trusted domains database.

As a result, the Whitelisting database, together with additional application trust verification tools – application trust inheritance rules and checks against a security certificate and trusted domain database – create a fault-tolerant chain of mechanisms for trust verification, providing a high level of protection for the computer.

However, even if all of these components are used, there is still a danger that cybercriminals will try to infect the computer via vulnerabilities in legitimate programs. Trusted Application technologies were developed with this in mind.

Security corridor

Attackers often take advantage of vulnerabilities in legitimate software. This means that any trusted program, even if it was downloaded from a trusted source and is digitally signed, can be used by cybercriminals to penetrate the system. To provide an effective countermeasure against such infection scenarios, Kaspersky Lab experts have developed the 'security corridor' model.

The underlying idea of the model is based on the fact that most trusted programs perform a strictly defined set of operations implemented by their developers. For example, a word processor's function is to handle text-based documents and a browser's function is to handle web content – download web pages, files etc.

In their efforts to take advantage of a vulnerability in a program, malware writers often attempt to exploit vulnerable applications to make them perform tasks they were not designed to perform, e.g., modify system files, inject code into system processes, install drivers etc. With this in mind, Kaspersky Lab experts have developed several protection mechanisms that monitor the operation of such potentially dangerous applications, allowing only those operations which were implemented by the applications' developers, making it virtually impossible to exploit vulnerabilities in these applications. In simpler words, Kaspersky Lab technologies are fully 'aware' of what a program should or shouldn't do, making it operate in a kind of 'secure corridor', performing only a restricted range of functions.

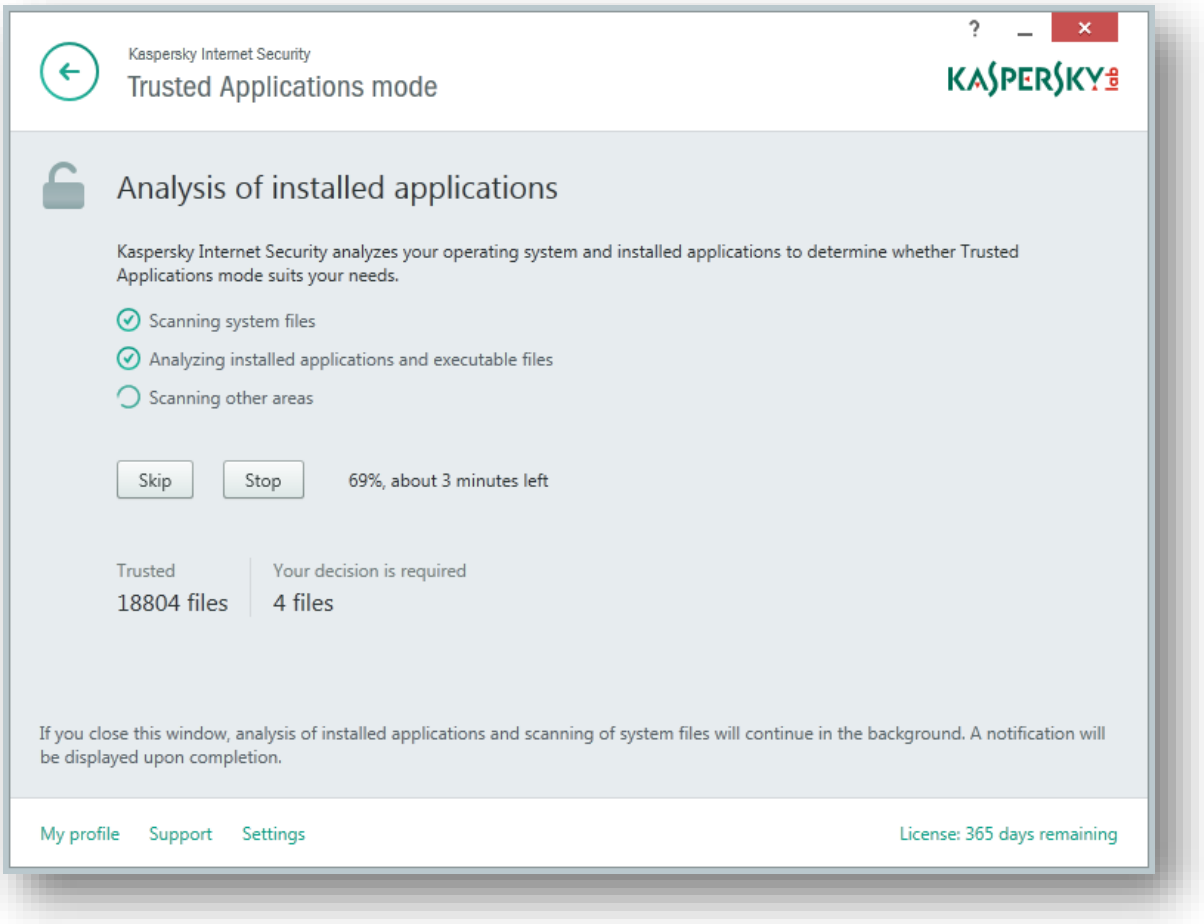

Figure 1. Trusted Application Mode during the application analysis process

How the technology works

Trusted Application Mode requires Application Control, File Anti-Virus and System Watcher to be enabled. When the mode is activated for the first time, it analyzes the operating system and all installed applications, checks them against the cloud database and evaluates which of them are reliable. Later it will verify any new program. Trusted Application Mode analyses not only common PE (portable executable) files, but also scripts, .NET applications, installation packages and Windows 8-style applications. To speed up the work, PE files that do not contain executable code, and therefore cannot cause any harm, are not checked against the whitelist database. If unknown system files or applications are encountered, users should decide whether they want to turn Trusted Application Mode off (which is highly unadvisable, because it poses a threat to system security) or to go on and block these programs. Users can look at the list of disabled applications and unblock the group at any time. For enhanced usability, this list of files can be sorted by folders, vendors or applications.

Trusted Applications mode also incorporates an EarlyBoot function that analyses files and scripts that were launched before the Kaspersky Lab product started. If some of them turn up to be suspicious, the user is alerted and given a choice to allow or block their launch when the system is rebooted.

It should be noted that if users do not respond to any notification about unknown files, Trusted Applications Mode will choose the most secure course of action. Therefore a malicious program will not cause any harm even if users miss a notification or ignore it for some reason.

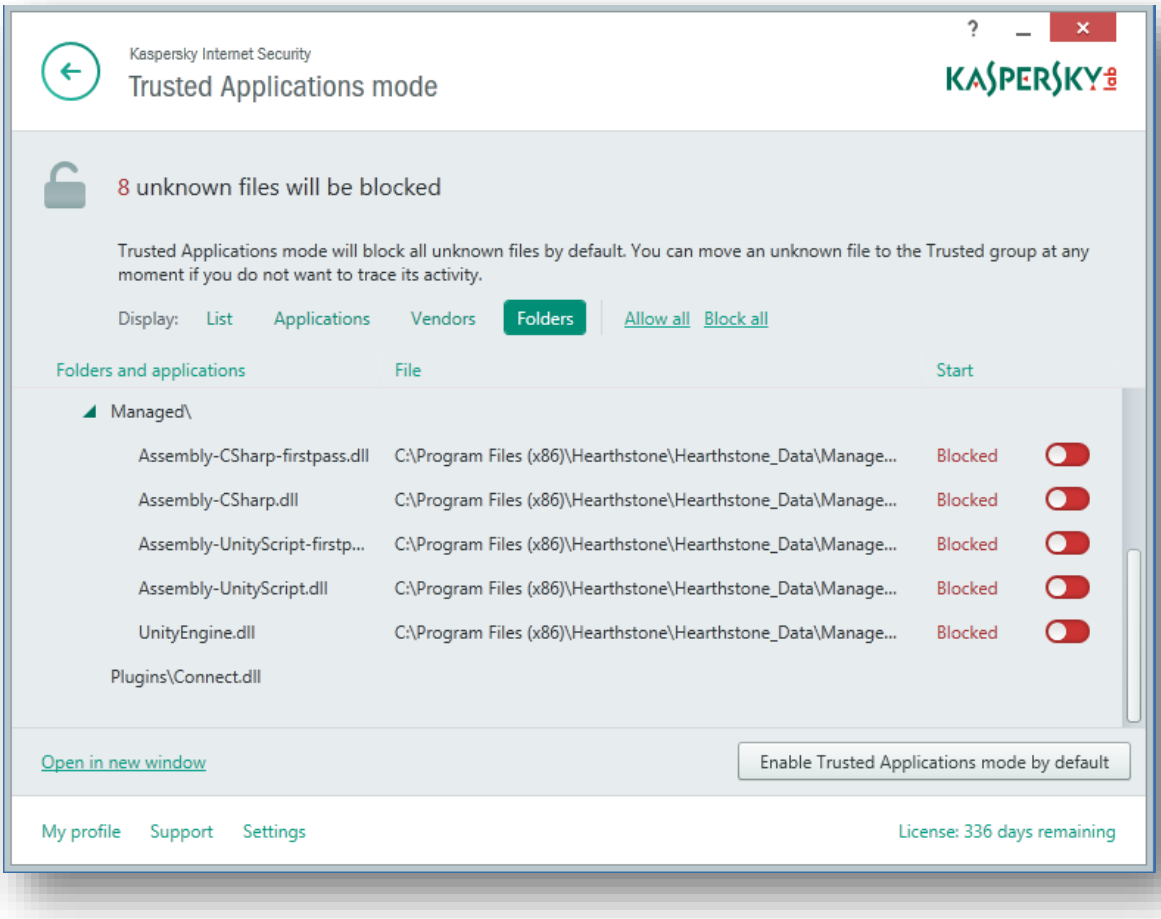

Figure 2. List of unknown programs awaiting a user decision

Overall, in addition to traditional anti-malware protection with advanced proactive technologies, Kaspersky Lab's solutions, incorporating Trusted Applications technology, offer users the following advantages:

- Effective protection against malicious applications based on a 'Launch only what is allowed' principle working in parallel with 'traditional' anti-malware technologies and proactive detection mechanisms;
- Stringent control over the execution of popular applications which are vulnerable to exploits from cybercriminals;

- Low false-positive rates achieved by using a multi-tier application legitimacy verification system;
- An intelligent system which adapts to user preferences.

However dangerous the cyber-threats, high-quality security solutions should provide effective protection against them in a way that ensures users have no trouble accessing legitimate programs and websites. Kaspersky Lab's products with the Trusted Applications technology secure the computer and user data in accordance with this principle.

Availability

Trusted Applications Mode technology is integrated into products for home users:

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