Kaspersky Security Network

Kaspersky Security Network is a progressive technology implemented in the latest versions of Kaspersky Lab's personal products. When it comes to new malware, it ensures a prompt response and an unprecedented level of detection that provides outstanding protection.

Kaspersky Security Network not only allows previously unknown threats to be detected and blocked but can also locate and blacklist the online source, protecting users from subsequent threats that emerge from the same sources.

Kaspersky Security Network combines the capabilities of continuous globally distributed monitoring of real-life threats, a centralized analysis of threats using Kaspersky Lab's substantial expert and technology resources, and the immediate generation and distribution of protection measures. This produces a powerful synergy effect, providing users of Kaspersky Lab products with comprehensive real-time protection against new malware.

The computer world needs new methods of protection

Malware such as viruses, worms and Trojans, have become the principle threat to the normal functioning of computers and to the information stored in them. The scope and range of malicious software is constantly expanding, presenting an ever-growing challenge to security. Malware is making use of new methods to penetrate computer systems, concealing their activities and bypassing detection by security software. No conventional malware detection methods can now provide complete protection when used as a stand-alone tool.

The conventional signature-based detection of malware relies on unique code signatures or behavior patterns that are compared with suspicious programs. This approach, however, is incapable of detecting new or previously unknown malware and is less effective at detecting real-life threats that are constantly mutating. It also takes longer for a security response to be formed, since information about a new malware outbreak doesn't always reach the antivirus vendor immediately.

Heuristic detection methods based on code analysis and the emulated execution of a suspicious program are capable of detecting new malicious software. However, these methods cannot yet provide a sufficiently reliable level of detection and often take a long time to respond to new threats because of the complexities of customizing the system settings.

Whitelisting is an alternative approach and is based on listing secure rather than malicious software, blocking all non-secure programs from running, and categorizing unknown programs as malicious or safe. This method also has its limitations, primarily due to the difficulties of entering the constantly growing number of legal software into a white list.

Today's computer world requires new integrated approaches to ensure computer security. These approaches have to combine the advantages and minimize the deficiencies of the aforementioned methods of combating malicious software, as well as

harnessing the potential of global monitoring and automatic updating of new real-life threats. Namely this approach has been implemented in Kaspersky Security Network.

The basic principles of Kaspersky Security Network

Kaspersky Security Network includes several subsystems: continuous geographically distributed global monitoring of real-life threats on users' computers, instantaneous delivery of collected data to Kaspersky Lab's host servers, analysis of collected data and the creation of protection measures against new threats, and the fast distribution of those measures to users.

Kaspersky Security Network utilizes users' computers that have the latest versions of Kaspersky Lab products working on them. This system allows information about attempted infections to be automatically collected and sent to Kaspersky Lab, as well as reporting on all unknown suspicious files downloaded to and executed on users' computers, whether they arrive from websites, in email attachments, from peer-to-peer networks or other sources.

This is done strictly voluntarily and confidentially – the user has to agree to participate in the system. No personal information such as passport data, passwords or any other personal details is collected.

The information collected on attempted infections is sent to Kaspersky Lab's central servers and analyzed using the company's powerful in-house technology and expert resources. This ensures extremely fast and reliable detection of both new malicious and secure software.

The decision on the safety of a program is made based on the availability of a digital signature verifying the source and integrity of the program, as well as a number of other factors. A program recognized as secure is entered to the list of trustworthy applications.

A program is deemed malicious after the required detecting procedures are completed. As soon as a program is deemed malicious, it is reported to Kaspersky Lab's Urgent Detection System, so that the information becomes available to Kaspersky Lab product users even before the signature for that piece of malware is created and updated on their computers.

If a program is launched by a user, it is checked against whitelists and Urgent Detection System lists, and is granted rights to access computer resources or blocked accordingly. Kaspersky Security Network technology plays an important role in replenishing these lists and keeping them up to date, ensuring reliable control over applications.

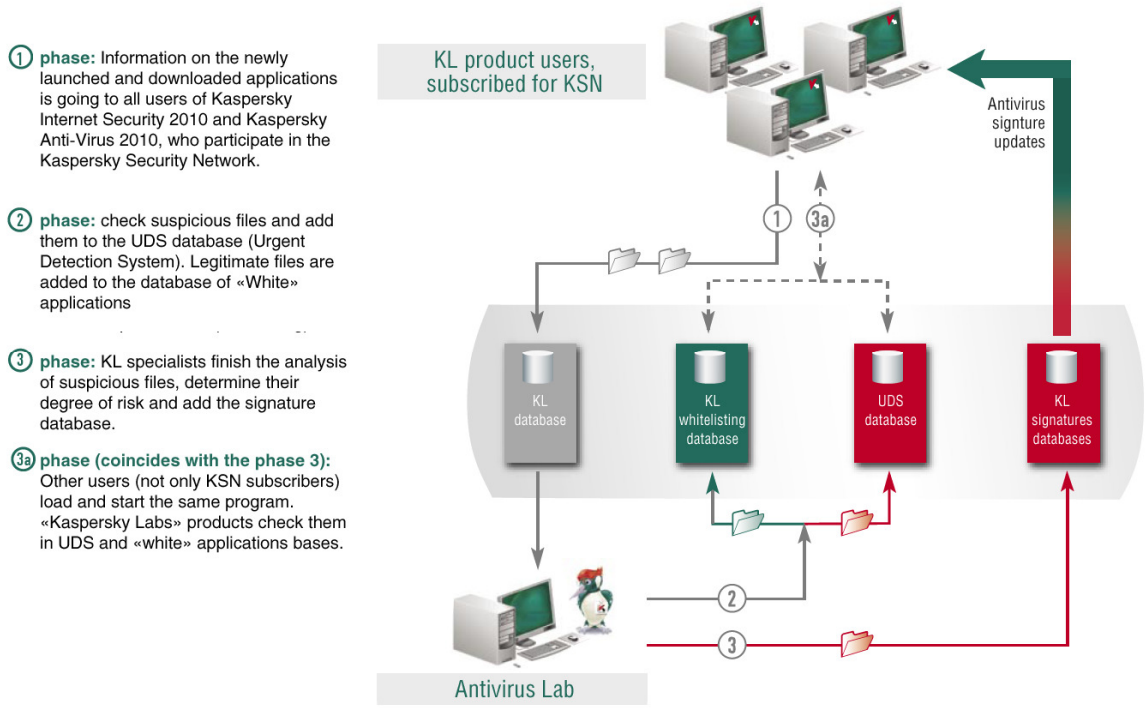

Figure 1. Kaspersky Security Network flow chart.

After the analysis of a new malicious program is completed, a signature is also generated and placed in the antivirus databases that are regularly updated on computers of Kaspersky Lab users.

Whitelisting is not the only technology that allows the user to make a decision about a program with the assistance of KSN resources. The system includes the reputational technology 'Wisdom of the Crowd' (WoC), which provides information about how popular a certain program is and its reputation among other users – the members of KSN.

Moreover, the latest versions of Kaspersky Lab consumer products include an opportunity to get Global Security Ratings (GSR) direct from the cloud. Each GSR is calculated using a flexible, customizable algorithm and various reputational data.

Kaspersky Security Network therefore makes use of a combination of signature and heuristic malware detection methods as well as application control technologies using white- and blacklists, WoC and GSR

The benefits of Kaspersky Security Network

Uninterrupted global monitoring of new threats and threat sources, metadata collection in real-life conditions under strict confidentiality, instantaneous data transfers, in-depth analysis of potential threats using the powerful resources of a leading antivirus vendor, and immediate availability of new protection measures all ensure an unprecedentedly rapid response by Kaspersky Lab to new threats and an unrivalled protection service for the company's clients.

Today, Kaspersky Security Network technology is used on millions of personal computers around the world, presenting a global but detailed picture of how new malware evolves and circulates, where new threats originate and how many infection attempts occur within specific time periods. The diagram below presents an example of how a typical Banker Trojan
circulated from 1 January to 20 June, 2010, as recorded in Kaspersky Security Network data. The diagram shows there were several dramatic surges in infection attempts during the time.

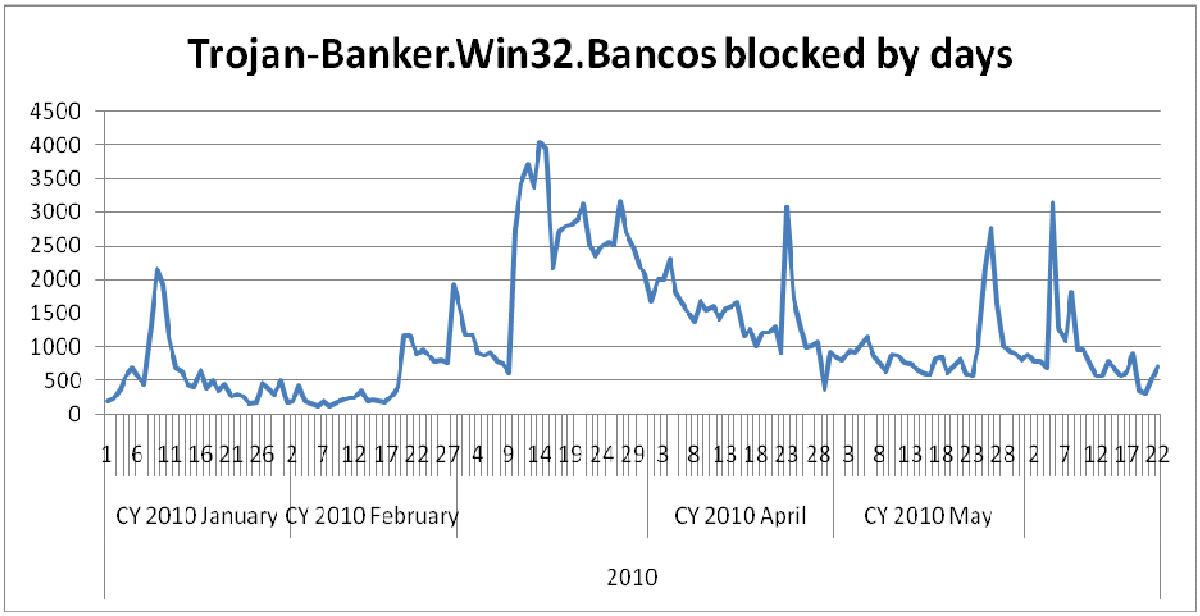

Figure 2. Diagram of typical Banker Trojan infections, as recorded by Kaspersky Security Network. The Y-axis shows the number of Kaspersky Internet Security users' computers on which the Trojan was blocked.

The globally distributed malware monitoring carried out by Kaspersky Security Network provides an effective response to new threats no matter where the sources and targets are located.

Real-time malware monitoring on workstations helps track actual threats and block them in their "in-the-wild" environments immediately after an infection attempt takes place.

Continuous malware monitoring and immediate reporting of suspect files to Kaspersky Lab ensure that the malware databases and the protection measures to combat these threats are always up to date. Automation ensures a much faster, more accurate and complete response than the conventional manual reporting of suspicious files to the antivirus vendor via email.

Strict confidentiality is ensured: personal information such as usernames, passwords, personal data and document contents, is not collected or transferred to Kaspersky Lab servers.

Moreover, users participating in Kaspersky Security Network enjoy more complete protection against personal data theft, as new malware designed to steal personal data is blocked in their computers, be it programs spying for files stored on the hard disk that send copies to hackers, keyloggers, screenshot senders, network activity spies, etc.

Any antivirus software installed on user computers consumes CPU resources and is therefore limited in terms of complexity and resource intensity. Analysis of new or unknown software using Kaspersky Lab's powerful centralized resources rather than just home PC-based antivirus software dramatically boosts the level and quality of malware detection.

Therefore Kaspersky Security Network provides proactive defense, i.e., it identifies and blocks new threats before they become widespread and can cause any significant damage to users' machines. A proactive defense system is essential to ensure stable and uninterrupted operation of IT equipment and the business processes it supports.