

Kaspersky Lab

Providing unparalleled protection for computers and networks since 1997

You Are Under Attack



Today, virtually every computer user is a Web user, and the first thing all Web users must understand is that at any moment they are connected to the Internet, they are under attack. As your network users browse the web, check their email, or simply work locally on their desktop computer, notebook/netbook or smartphone connected to the Internet, it's a safe bet that someone, somewhere will be attempting to infect their computers and take them under control. To understand just how enormous is the scale of online crime circa 2010, consider the following:

- Over the last three years malware (short for malicious software) has literally exploded on the Web.
- In 2008 and 2009, around 32 million new malware samples were uncovered in the Web – i.e., more than 40 000 new malicious programs every day.
- Approximately 18,000 new malicious URLs appear on the Web every day.
- Viruses, backdoors, keyloggers, password stealers, Word and Excel macro viruses, boot sector viruses, script viruses (batch, windows shell, java, etc.), Trojans, crimeware, spyware and adware are examples of what lies in wait for a careless and unprotected user.

New Threats, Every Minute

Of course, most advanced anti-virus solutions neutralize over 95% of known viruses and malware that attack protected networks. However, a question needs to be asked – what happens when a new threat, one that is sufficiently different in appearance and behavior from earlier e-bugs, emerges on the web?

It is no longer sufficient for anti-malware suites to intercept and neutralize only known threats. The new challenge for any comprehensive anti-malware solution is to detect and contain new threats as soon as they appear 'in the wild' – immediately or, in the worst case, a few hours after an outbreak becomes apparent. In fact, one could argue that such 'zero-day' detection has become more important than the traditional anti-virus solution quality criterion – overall malware detection rate.

Introducing Kaspersky Lab

Today, Kaspersky Lab, world's leading provider of anti-malware technologies and solutions, is readier than ever to protect the global networks, computer systems and users from innumerable threats. Our solutions thwart cyber-threats every step of the way: from security gateway partners, with comprehensive Kaspersky technology integrated inside, to our renowned corporate solutions for servers, workstations, mobile computers, and even smartphones.

By virtue of—

- state-of-the-art core anti-malware engine,
- advanced heuristic algorithms,
- 24x7 anti-malware laboratory analysis,
- industry-leading zero-day protection technologies,
- frequent malware database updates, and
- unmatched in-the-cloud community services,

—Kaspersky Lab is the company that will ensure your computers, networks and data stay safe.

Read on about our approaches to systems protection and why you should choose Kaspersky technologies.

We're Here To Protect

Start using Kaspersky Anti-Malware technologies to receive comprehensive and reliable protection against:

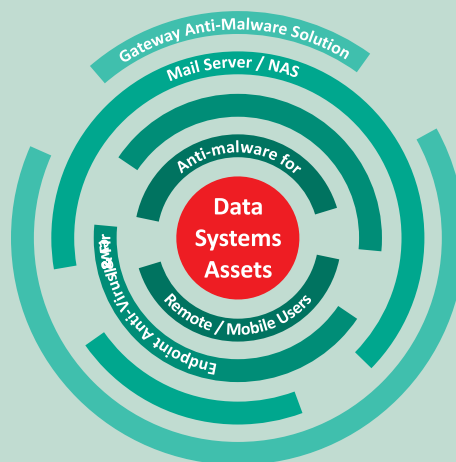
- Viruses, Trojans, worms and other malware, spyware and adware
- Rootkits, bootkits and other complex threats
- Identity theft by keyloggers, screen capture malware
- Botnets and various illegal methods of hijacking your PC
- Zero-day attacks and unknown threats
- Drive-by download infections

Understanding Multi-Layered Defense

Of course, no single product, on its own merits, is enough to reliably protect the customer's network and ensure that no malware penetrates the perimeter and adversely affects the users. That is why the 'Multi-layered defense' concept was conceived and put into operation. As in traditional warfare, this concept implies that the end-user needs to be protected by several layers, or tiers, of hardware- and software-based security. A multi-layered approach is schematically defined in the adjacent diagram.

Moving from the 'outside' – i.e., the Whole Wide World – to the 'inside' – i.e., system core where the company's assets and data are located, a hypothetical threat will first have to pass:

- Tier 1 – Gateway anti-malware solution – a broad range of best-of-breed products from Kaspersky Lab's Technology Partners offering comprehensive malware protection at the entry point to the corporate network.
- Tier 2 – Mail server / NAS – a high-performance anti-malware solution deployed on corporate servers and network attached storage systems.
- Tier 3 – Endpoint Anti-Virus / Firewall – personal endpoint anti-malware suite deployed on corporate user's workstation.
- Tier 4 – Anti-malware for Remote / Mobile users – endpoint anti-malware solution protecting employee laptop computers, smartphones and other remote intelligent devices.



Now suppose each of these layers has only 80% chance to detect an incoming threat (a pretty conservative estimate, considering that Kaspersky products provide much higher detection levels, generally above 97%). In this case:

- 1st level detection probability = 80%
- 2nd level detection probability = 96%
- 3rd level detection probability = 99.2%
- 4th level detection probability = 99.84%

Why is Zero-Day Protection Important?

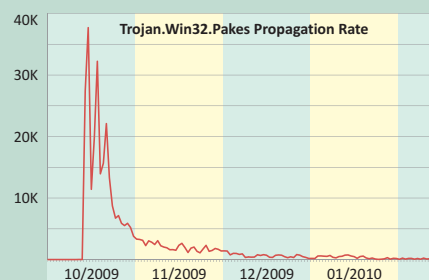
Many 'traditional' anti-malware solutions are unable to cope with brand-new or, as they are called, 'zero-day' threats. They have new source code and modes of behavior, and thus cannot be picked up by the majority of detection routines. After some time (usually, days to weeks), when the new threat's code is disassembled and analyzed by anti-virus labs, and its signatures are added to virus databases, the outbreak becomes contained and eventually defeated – but is it any consolation to users who had their data corrupted, trade secrets stolen, work interrupted during these first hours-to-days of outbreak?

All in all, typical outbreaks of new dangerous malware usually appear as shown on the adjacent diagram (with specific rates of infection and propagation speed varying for each threat). Here, the number of infected machines is shown along the vertical axis, and the timeline along the horizontal one. This is why zero-day protection rate becomes a key characteristic of modern anti-virus solutions.

The vast majority of malware only lives in the wild for a few weeks to a few months, and you are incredibly unlikely to encounter a year-old threat in Internet. It follows therefore that it's becoming less important to hoard huge databases of outdated malware (against which solutions are often checked to determine the detection rate) – and, conversely, more important than ever to be prepared for rapid-fire outbreaks of new and dangerous threats.

The ways used to ensure top-notch zero-day detection vary across the products available in the market today and may include constant surveillance of the web, sophisticated heuristic algorithms, and in-the-cloud community services.

All of these considerations were taken into account during the development of Kaspersky anti-malware products that are implemented today into a variety of software and hardware platforms. In addition to traditional advantages of Kaspersky anti-malware solutions, such as top-class detection rate, frequent signature database updates, and support of thousands of packer and archiver formats, Kaspersky provides the answer to today's most pressing challenge – protection from zero-day malware.



Why Kaspersky Anti-Malware?

Kaspersky anti-malware solutions deliver industry-leading protection against a wide range of malware including viruses, Trojans, worms, rootkits, spyware and adware. The Kaspersky anti-malware engine, integrated into all Kaspersky products, incorporates a unique combination of technologies necessary for the successful detection of malicious code. The engine is designed on the basis of a powerful and flexible logical subsystem that employs state-of-the-art methods to find and remove malware. The key features of Kaspersky anti-malware solutions are outlined below:



- Award-winning Kaspersky anti-malware technologies ensure supreme malware detection rate
- Kaspersky security solutions will immediately detect any new malware on the web, protecting the users even from zero-day threats. Reliable zero-day detection is ensured by:
 - 24x7x365 Human Analysis – Kaspersky anti-malware technology is supported by a team of professional virus analysts and engineers that explore the global virus weather and develop new detection methods and anti-malware technologies.
 - Advanced heuristics – Kaspersky heuristic analyzer emulates suspect program performance and logs all suspicious activities. It successfully detects malicious code (including new script viruses and malware for Microsoft Office) in executable files, disk sectors and computer memory.
 - Kaspersky Security Network (KSN) – The Kaspersky in-the-cloud community reporting service facilitates the detection of new malware even before regular database updates – in many cases literally minutes after the malware in question appears in the wild.
- Hourly anti-malware signature database updates for optimum frequency/content ratio
- Updatable anti-malware core – new detection technologies and procession logic can be upgraded/modified by means of regular AV database updates
- Support of more than 4000 packer and archiver formats and growing – more than *any* other solution in the world provides today

The following criteria are generally considered to be critical for modern anti-malware solutions. Please see for yourself how Kaspersky Anti-Malware excels at them.

Criteria	Description	Kaspersky Anti-Malware
Quality of detection	The effectiveness with which the solution detects viruses, worms, Trojans and other malware	Excellent (above 97%)
Level of proactive detection	The solution's ability to find unknown threats	Excellent (see awards)
Zero-day protection rate	Ability to detect and contain new threats as soon as they appear 'in the wild'	Excellent (see above)
Number of false alarms	Undesirable propensity to flag legitimate programs and data as malware	Minimum (see awards)
Malware detection in archives	Ability to detect malicious code inside compressed, archived and packed formats	Over 4,000 formats (world's best)
Update size and frequency	Frequent updates to the anti-virus databases guarantee that a user will be constantly protected from the latest threats	Hourly updates (optimum frequency/content ratio)
Engine-only updating	Indicates solution's flexibility and versatility, saves user's time, allows the developer to quickly improve the engine and/or extend its functionality.	Available
Engine performance	Critical when considering the impact on hardware and operating system resources as well as the user's work efficiency during scanning.	Excellent (see awards)

Experience and Expertise

Kaspersky Lab was founded in 1997 by Eugene Kaspersky, one of the world's biggest IT security experts. Now, more than 12 years later, Kaspersky Lab is:



- One of the top internationally-recognized developers of secure content management solutions protecting against viruses, Trojans, spyware, spam and hacker attacks
- Over 1800 employees
- Over 300 million users worldwide protected by Kaspersky products and solutions
- World's fastest growing vendor of IT security software
- Second largest retail end-point, anti-malware security solutions provider globally and #1 in key markets including Germany and CIS
- Vast technical know-how proven by numerous U.S. and European patents
- Truly global reach with headquarters in Moscow (Russia) and regional headquarters in five global regions (Western Europe; Eastern Europe & Middle East and Africa; North and South America; Asia-Pacific; and Japan)
- Technology partnerships with world's leading IT vendors, including:



- Consistently leading the pack in excellence awards from top independent test labs and IT periodicals, including, just over the last few months:



Kaspersky Lab

10/1 1st Volokolamsky Proezd, Moscow, 123060 Russian Federation

Web site: <http://www.kaspersky.com/oem> Email: oem@kaspersky.com

Tel: +7 495 797 8700 Fax: +7 495 780 3368