WHAT YOU SHOULD KNOW

Company Overview
About Kaspersky Lab

Kaspersky Lab is a private international company with a holding registered in the UK (one of the strictest jurisdictions in the world). It has R&D centers and virus experts around the world, including in Russia, Europe, Japan, Israel, China, the United States and Latin America. More than 80 percent of its operations are international.

It is the world’s largest privately-owned cybersecurity company and is ranked among the world’s top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997, Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.
Kaspersky Lab Principles of Cooperation with Governments and Law Enforcement Agencies

As a private company Kaspersky Lab has no political ties to any government but is proud to collaborate with the authorities of many countries and international law enforcement agencies in fighting cybercrime. The company works with the authorities in the best interests of international cybersecurity, providing technical consultations and expert analysis of malicious programs, in compliance with court orders or during investigations.

The company works together with the global IT security community, international organizations, national and regional law enforcement agencies (e.g. INTERPOL, Europol, Microsoft Digital Crimes Unit, The National High Tech Crime Unit (NHTCU) of the Netherlands’ Police Agency and The City of London Police), as well as Computer Emergency Response Teams (CERTs) worldwide. During investigations, Kaspersky Lab’s security experts provide technical expertise only and focus their research on analyzing malware. The company applies the same methodologies and principles to discovery and analysis as it does to commercially-motivated malware.

Kaspersky Lab’s Principles for Fighting Cyberthreats

As an IT security company, Kaspersky Lab is determined to detect and neutralize all forms of malicious programs, regardless of their origin or purpose. One of Kaspersky Lab’s most important assets in fighting cybercrime is the Global Research & Analysis Team (GReAT), comprising top security researchers from all over the world – Europe, Russia, the Americas, Asia, and the Middle East.

Kaspersky Lab has a clear policy concerning the detection of malware: the company detects and remediates any malware attack. There is no such thing as “right” or “wrong” malware for us. The company’s research team has been actively involved in the discovery and disclosure of a significant proportion of the world’s major malware attacks.

Kaspersky Lab Investigates and Reports on All Threats, Regardless of the Potential Source

The company reports on any kind of threat discovered, and it does not matter which language the threat ‘speaks’ - Russian, Chinese, Spanish, German, or English. The following list of threats, as reported by the GReAT team, shows the different languages used in a representative sample of recent cases:

- English language: Regin, Equation, Duqu 2.0
- Chinese language: IceFog, SabPub, Nettraveler
- Spanish language: Careto/Mask, El Machete
- Korean language: Darkhotel, Kimsuky
- French language: Animal Farm
- Arabic language: Desert Falcons

Duqu 2.0 Regin IceFog Darkhotel Animal Farm Desert Falcons
Kaspersky Lab Does Not Provide Speculative Attribution

Kaspersky Lab reports on any kind of threat discovered, and it does not matter which language the threat ‘speaks’ - Russian, Chinese, Spanish, German, or English; however, the use of these different languages does not permit attribution to any specific country. Language traces cannot be considered reliable evidence because they can be fabricated and deliberately planted in malware code as red herrings for investigators. In addition, other information typically gleaned in the types of investigations the company undertakes are known to not be definitive; they can be falsified and (often are) by attackers. Therefore, Kaspersky Lab cannot definitively attribute attacks to specific entities or groups.

Principles of Trustworthy Development of Kaspersky Lab Technologies and Solutions

The company has been dedicated to excellence from day one and its security solution was first named the best in the world by Hamburg University in 1994. Since then, Kaspersky Lab has continuously scored highly in numerous independent ratings and surveys, as well as receiving some of the most prestigious international awards and numerous first and top-three places in independent tests (such as AV-Test, AV-Comparatives, Dennis Technology Labs, etc.) and reviews.

Kaspersky Lab technologies are trusted by more than 120 global technology and OEM partners including Microsoft, Cisco Meraki, Juniper Networks, Alcatel Lucent, Blue Coat, Check Point, D-Link, Clearswift, Netgear, ZyXel, Alt-N, Parallels, Lenovo, Facebook, Qualcomm, BAE Systems, H3C, Trustwave, Vertu, Stormshield, Amazon Web Services, Openwave Messaging and General Dynamics.

Kaspersky Lab Product Certifications

Kaspersky Lab’s products undergo mandatory certification in countries where this is required by national law. When and if required, the program code can be handed over to the appropriate certification authorities to validate that Kaspersky Lab software fulfills the requirements placed on software purchased for use in government agencies and state institutions.

Kaspersky Lab has a number of certifications from authorized bodies verifying that its products are transparent and recommended for use by companies that deal with confidential data or state secrets. The fact that Kaspersky Lab obtains these certifications demonstrates that the company takes the issue of customer confidentiality very seriously.
Kaspersky Lab Has No Political Ties to ANY Government

Kaspersky Lab has no political ties to ANY government. The company cooperates with Russian law enforcement agencies, providing technical expertise, just as it cooperates with law enforcement in many other countries. Kaspersky Lab offers consultation services and provides expertise during legal trials and investigations. The company’s corporate clients include government bodies in a number of countries, including Russia.

Principles of Cooperation with the IT Security Industry

Kaspersky Lab believes that joint effort is the most effective way of fighting cybercriminals. The company openly shares its knowledge and technical findings with the world’s security community and publishes its research for the wider public to encourage collaborative security practices and increased international cooperation.

Kaspersky Lab collaborates in joint cyberthreat investigations with companies and organizations such as Adobe, AlienVault Labs, Dell Secureworks, Crowdstrike, OpenDNS Security Research Team, GoDaddy Network Abuse Department, Seculert, SurfNET, Kyrus Tech Inc. and Honeynet Project.

The company also actively collaborates with global IT vendors including Google and Microsoft, in order to coordinate responses to newly discovered vulnerabilities which are detected through research or by identifying cases “in the wild.”

The company supports the IT vendor affected by the vulnerability by providing information and relevant telemetry. The vulnerabilities are reported confidentially and adhere to coordinated disclosure guidelines in order to provide the vendor with time to create and administer a security update patch for its users.

Principles of Protecting Privacy

Respecting and protecting people’s privacy is a fundamental principle of Kaspersky Lab’s business and one of the main goals of the company’s activity. Privacy is a basic human right, but nowadays it is violated more and more often. Kaspersky Lab invests a lot of effort into protecting privacy on a global scale. The company investigates advanced cyberespionage and surveillance campaigns violating people’s privacy such as HackingTeam’s legal spyware or Computrace software, and this often leads to the disruption of such cybercriminal activities.

Millions of people around the globe trust Kaspersky Lab to protect their digital valuables, including private data. Kaspersky Lab takes this responsibility seriously, which is why its products and technologies do not process private data. Kaspersky Lab’s solutions obtain depersonalized cyberthreat-related data from the devices of those users who have agreed to participate in the Kaspersky Security Network (an automatic cloud-enabled system that processes depersonalized cybersecurity-related data streams from millions of voluntary participants around the world). This data helps to identify new and as yet unknown threats quicker and more precisely. Similar technologies are used by other leading vendors of security solutions.
More About Our CEO

Eugene Kaspersky went to a special Higher School that was co-sponsored by four state institutions – one of which was the KGB. In the early 1980s, as a teenage graduate of a prestigious Soviet high school specializing in mathematics, Eugene decided he wanted to study cryptography. He had three options, but finally decided on a special program at the Higher School co-sponsored by the KGB because it provided the highest level of education in his chosen field of knowledge (the other two options were the Moscow Institute of Physics and Technology and Moscow State University, both considered inferior). At the time, the Higher School was an inter-ministerial/institutional educational facility sponsored by the KGB, the Ministry of Defense (MoD), the Ministry of Atomic Energy, and the Soviet Space Program.

It was down to the faculty of the School to decide which of the two classes Eugene should enter – the MoD-sponsored class or the KGB-sponsored class. The School chose the MoD-sponsored one. This meant that after graduation Eugene would be sent to a scientific institution working specifically for the MoD.

Eugene’s education focused on cryptography, programming languages and mathematics, and he developed a particular interest in the latter. In the mid-1980s, the department of the Higher School that Eugene studied in was among the best in the world in terms of mathematical education. After graduating in 1987, Eugene joined a MoD scientific research institute where his primary role was that of a software engineer. It was in this job that he first came across a computer virus, in 1989, a discovery that shaped his future career path. Two years later, in 1991, the year the Soviet Union broke up, Eugene left the research institute and formed a small antivirus division at an emerging commercial holding company. In 1997, he and a small group of associates founded Kaspersky Lab.

Eugene Kaspersky
Chairman and CEO, Kaspersky Lab