Kaspersky Lab Transparency Principles

Kaspersky Lab Transparency Principles

"We believe that everyone – from home computer users through to large corporations and governments – should be able to protect what matters most to them. Whether it's privacy, family, finances, customers, business success or critical infrastructure, we've made it our mission to secure it all. We succeed in this by delivering security expertise, working closely with international organizations and law enforcement agencies to fight cybercriminals, as well as developing technologies, solutions and services that help you stay safe from all the cyberthreats out there."

Eugene Kaspersky, chairman and CEO of Kaspersky Lab

Kaspersky Lab is an international company operating in almost 200 countries and territories around the globe, with 37 representative offices in 32 countries. We protect more than 400 million people and over 270,000 clients, ranging from small and medium-sized businesses, all the way up to large governmental and commercial organizations worldwide. Our business model is based on trust. One of the company's key assets is its credibility in the eyes of its clients. This is why we are committed to business ethics and adhere to the highest standards of transparency in all areas of our business.

This document sets out our principles of transparent business: what guides us and how our business works. These principles present our position in fighting cyberthreats, how we cooperate with governments and law enforcement agencies, our vision of data processing, etc.

1. Our principles of fighting cyberthreats

Cyberthreats have become a global problem which spread far beyond any geographical borders. 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.

We have a clear policy concerning the detection of malware: we detect and remediate any malware attack. There is no such thing as "right" or "wrong" malware for us. Our research team has been actively involved in the discovery and disclosure of several malware attacks with links to governments and state organizations. Over the past few years we have published in-depth research into Flame, Gauss, The Mask/Careto, Regin, Equation, Duqu 2.0, ProjectSauron. Sofacy (Fancy Bear), CozyDuke (Cozy Bear), Black Energy (Sand Worm) – some of the biggest state-sponsored cyber-espionage operations known to date. We have combined our efforts with INTERPOL, Europol and authorities from different countries to uncover the Carbanak APT, and our experts also assisted in an investigation into the Lurk gang, resulting in the most significant arrest of hackers to have taken place in Russia.

We report on any kind of threat we discover, and it does not matter which language the threat 'speaks' - Russian, Chinese, Spanish, German, or English. The following list of threats, as reported by our GReAT team, shows the different languages used in each case:

Russian speaking: RedOctober, CloudAtlas , Miniduke, CosmicDuke, Epic Turla, Penquin Turla, Black Energy, Agent.BTZ, Teamspy, Lurk, GCMAN, Metel, Carbanak, Sofacy
English speaking: Regin, Equation, Duqu 2.0, ProjectSauron
Chinese speaking: IceFog, SabPub, Nettraveler, Danti
Spanish speaking: Careto/Mask, El Machete
Korean speaking: Darkhotel, Kimsuky, Lazarus

French speaking: Animal Farm
Arabic speaking: Desert Falcons

However, the use of these different languages doesn't 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. For this reason, we don't attribute threats to individual countries.

The GReAT team currently tracks the activity of more than a hundred threat actors and sophisticated malicious operations that, between them, target commercial and government organizations in 80+ countries around the world.

2. Principles of trustworthy development of our technologies and solutions

Every year the IT industry becomes more dynamic, and so does cybercrime. To continue detecting and preventing cybercrimes effectively, the company has to be sensitive to the slightest change in the online environment. That's why we invest in the best specialists, education and research, and develop new solutions to ensure we offer world-leading protection.

The company has been dedicated to excellence from day one and our security solution was first named the best in the world by Hamburg University in 1994. Since then, we have 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[i].

Kaspersky Lab has about 120 global technology OEM and pre-installation agreements with companies including Microsoft, Amazon Web Services, Cisco, ZyXEL, Parallels, Lenovo, Facebook and Check Point.

Kaspersky Lab's products undergo mandatory certification in those countries where it 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 legal requirements for use in government agencies and state institutions[ii].

3. Our principles of cooperation with the IT security industry

We believe that joint effort is the most effective way of fighting cybercriminals. We openly share our knowledge and technical findings with the world's security community and publish our 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, OpenDNS Security Research Team, GoDaddy Network Abuse Department, Seculert, SurfNET, Kyrus Tech Inc. and Honeynet Project. We also actively collaborate 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".

We support 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.

In addition to regularly working with security researchers in the industry to exchange knowledge about emerging threats, the annual Kaspersky Lab Security Analyst Summit brings together the world's best IT security experts to collaborate and exchange research alongside international organizations, law

enforcement agencies and technology companies. Previous delegates include Adobe, Arbor, Barracuda, BlackBerry, Boeing, Google, HB Gary, INTERPOL, ISEC Partners, Lockheed Martin and Microsoft.

4. Our principles of cooperation with governments and law enforcement agencies

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

Other cybersecurity vendors do the same. Without the expertise of security professionals, successful law enforcement operations would be an unattainable dream. When cybercrime cases are domestic, IT security companies work with their law enforcement agencies to assist in investigations. When they are international, they work with the appropriate law enforcement authorities of the affected countries to abide by legal policies and federal jurisdictions. This cooperation is crucial in fighting cybercrime worldwide.

We work 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.

In October 2014, Kaspersky Lab and Europol signed a memorandum of understanding which paves the way for closer cooperation between the two organizations. Moreover, Kaspersky Lab has supported INTERPOL's launch of the Digital Crime Center at the Global Complex for Innovation (IGCI) in Singapore which is responsible for carrying out the technical part of INTERPOL's investigations into cyber-incidents with its products and intelligence.

We also hold special training courses for international police forces, as well as for INTERPOL and Europol officers on a regular basis.

5. The 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. We investigate 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.

Alongside such investigations, Kaspersky Lab protects user privacy with relevant product features. For example, users of the Kaspersky Internet Security for Android product can choose to hide incoming calls and SMS from specific contacts. Kaspersky Lab's solutions for Windows ensures that no one can watch users through their webcam without their consent via the Webcam Protection feature, or listen to their web traffic while connected to Wi-Fi thanks to Secure Connection technology. In addition, they can choose to stop the tracking of their browser activities when online by switching on Private Browsing, irreversibly delete private files with File Shredder and remove traces of their activity on their computers with the Privacy Cleaner feature.

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 our products and technologies do not process confidential data. Kaspersky Lab's solutions obtain depersonalized cyberthreat-related data from

the devices of those users across the globe who have agreed to participate in the Kaspersky Security Network (an expert cloud-based system that automatically processes depersonalized statistics to maximize the effectiveness of discovering new and unknown threats). Similar technologies are used by other leading vendors of security solutions.

Kaspersky Security Network (KSN) participants do not send data which would be regarded as "personal" according the laws of most countries. Kaspersky Lab does not locate or track the movement of a particular person and has no intention to do so. The law enforcement agencies of the countries where Kaspersky Lab operates may request information in order to conduct investigative work. However, due to the fact that the data stored in KSN is in the form of depersonalized statistics, this information is not suitable for investigative purposes.

Moreover as a socially-responsible company, Kaspersky Lab fully understands that while the antimalware security solution is a basic cybersecurity measure, in some cases it is not enough to provide reliable levels of privacy for customers. To address this, Kaspersky Lab makes efforts to educate people about the latest privacy protection technologies available on the Internet.

What clients and partners say about Kaspersky Lab

Vittorio Boero, Chief Information Officer, Ferrari S.p.A
"To protect our sensitive intellectual property, we needed a strong technological partner with a complete, cutting-edge IT security solution. Kaspersky Lab delivers exactly what we need."

"Kaspersky Lab's ability to intercept malware not detected by other players and its flexibility to adapt to Ferrari's requirements make for a compelling and innovative roadmap for future years."

Joe Sullivan, Former Chief Security Officer, Facebook
"As a truly innovative company, we appreciate the values we have in common with Kaspersky Lab. The company is an industry leader and helps provide us with the latest threat information; they're constantly monitoring global trends and deliver advanced protection."

Noboru Nakatani, Executive Director, INTERPOL Global Complex for Innovation
"INTERPOL has been working with Kaspersky Lab in the field of cybersecurity since April 2013 and has had a very positive experience in doing so. The Internet security company has been actively assisting us in the run up to the launch of the INTERPOL Global Complex for Innovation (IGCI) in Singapore. It has provided training courses for our officers and one of the company's top researchers will stay in Singapore to support the launch of the IGCI's new Digital Forensics Laboratory. Kaspersky Lab has also been sharing its threat intelligence with INTERPOL and assisting in several investigations into cyber-incidents. I believe that Kaspersky Lab has made a serious contribution to providing security on a global scale by actively helping INTERPOL's efforts to form a Global Alliance against Cybercrime. In doing so the company has demonstrated its continued commitment to making cyberspace a safer and more secure place, while respecting its openness."

Ronald Noble, Former INTERPOL Secretary General
"The complex and ever-changing nature of the cyberthreat landscape requires high-level technical expertise, and it is essential that law enforcement collaborates across sectors to effectively combat cybercrime and enhance digital security.

"INTERPOL's agreement with Kaspersky Lab is a significant step forward towards forging a global alliance against cybercrime and ensuring that we provide our member countries with the most up-to-date support in addressing this threat."

Adrian Leppard, Commissioner, City of London Police

"City of London Police, the UK National Police lead for Fraud and Economic Crime, is partnering with cyber security industry leader, Kaspersky Lab, to take advantage of its expert malware analysis training and intelligence services in a bid to reduce cybercrime and other online threats."

Rimma Perelmuter, CEO, MEF

"Kaspersky Lab's heritage as a leading expert in digital security, combined with its deep understanding of the rising challenges of mobile security, make it a strong partner for companies looking to understand and implement solutions in this complicated arena."

Sources:

---

[i]The company was rated fourth in the IDC 'Worldwide Endpoint Security Market Shares, 2015: Currency Volatility Headwind Vendors' report (IDC # US41867116, 2015 - Nov 2016)

Gartner, Magic Quadrant for Endpoint Protection Platforms, 30 January 2017. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

According to summary results of independent tests in 2016 for corporate, consumer and mobile products. Summary includes independent tests conducted by: AV-Comparatives, AV-Test, SELabs, MRG Effitas, VirusBulletin, ICSA Labs. Tests performed in these programs assess all protection technologies against known, unknown and advanced threats. The size of the bubble reflects the number of 1st places achieved.

[ii] Kaspersky Lab's Product Documentation and User Manuals can be found here