= Eugene Kaspersky =

Eugene Kaspersky (born Yevgeny Valentinovich Kaspersky) is a Russian cybersecurity expert and the CEO of Kaspersky Lab , an IT security company with 3 @,@ 000 employees . He cofounded Kaspersky Lab in 1997 and helped identify instances of government @-@ sponsored cyberwarfare as the head of research . He has been an advocate for an international treaty prohibiting cyberwarfare . There is a debate about whether Kaspersky 's views and security research show favoritism towards Russian political interests .

Kaspersky was born in 1965 in Novorossiysk , Russia . He graduated from the Institute of Cryptography , Telecommunications and Computer Science in 1987 with a degree in mathematical engineering and computer technology . His interest in IT security began when his work computer was infected with the Cascade virus in 1989 and he developed a program to remove it . Kaspersky helped grow Kaspersky Lab through security research and salesmanship . He became the CEO in 2007 .

= = Early life = =

Eugene Kaspersky was born on 4 October 1965 in Novorossiysk , Russia . He grew up near Moscow , where he moved at age nine . His father was an engineer and his mother a historical archivist . As a child he developed an early interest in math and technology . He spent his free time reading math books and won second place in a math competition at age 14 . When he was fourteen , Eugene began attending A.N. Kolmogorov boarding school , which is run by Moscow University and specializes in math . He was also a member of the youth division of the Communist Party of the Soviet Union .

At the age of 16 , Kaspersky entered a five @-@ year program with the Institute of Cryptography , Telecommunications and Computer Science , which was sponsored by the Russian military and KGB . At @-@ the @-@ time , the most prestigious schools in Russia for mathematicians were KGB sponsored . He graduated in 1987 with a degree in mathematical engineering and computer technology . After graduating college , Kaspersky served the Russian military as a software engineer . He met his first wife Natalya Kaspersky at Severskoye , a KGB vacation resort , in 1987 .

= = Kaspersky Lab = =

= = = Origins = = =

Eugene Kaspersky 's interest in IT security began in 1989 , when his PC was infected by the Cascade virus , while working for the Ministry of Defense . He studied how the virus worked and developed a program to remove it . Afterwards he continually found new viruses and developed software to remove them , as a hobby . Early on Kaspersky 's anti @-@ virus software had just 40 virus definitions and was distributed mostly to friends .

In 1991 , Kaspersky was granted an early release from his military service and left the defense ministry to take a job at the Information Technology Center of a private company KAMI , in order to work on his antivirus product full @-@ time . There , he and his colleagues improved the software and released it as a product called Antiviral Toolkit Pro in 1992 . At first the software was purchased by about ten clients per month . It earned about $ 100 per month , mostly from companies in Ukraine and Russia . Kaspersky 's then @-@ future wife Natalya Kaspersky became his coworker at KAMI .

In 1994 , Hamburg University in Germany gave Kaspersky 's software first place in a competitive analysis of antivirus software . This led to more business for Kaspersky from European and American companies . Kaspersky Lab was founded three years later by Kaspersky , his wife and Kaspersky 's friend . Natalya , who pushed Eugene to start the company , was the CEO , while Eugene was the head of research . The following year , the CIH virus (AKA the Chernobyl virus)

created a boon for Kaspersky 's anti @-@ virus products , which Kaspersky said was the only software at @-@ the @-@ time that could cleanse the virus . According to Wired , " their software was advanced for the time . " For example , it was the first software to monitor viruses in an isolated quarantine .

Kaspersky 's company grew quickly in the late 1990s . From 1998 to 2000 , its annual revenue grew 280 percent and by 2000 almost sixty percent of revenues were international . By 2000 , it had a staff of 65 people , up from 13 shortly after its foundation . The antivirus product was renamed to Kaspersky Antivirus in 2000 , after an American company started using the product 's original name , which wasn 't trademarked .

= = = Threat discoveries = = =

As the head of research , Kaspersky authored papers on viruses and went to conferences to promote the software . He was often quoted in the technology press as an antivirus expert . He helped establish the company 's Global Research and Expert Analysis Team (GReAT) , which helps corporations and governments investigate IT security threats . Initially he told his team not to discuss cyber @-@ terrorism publicly , to avoid giving governments ideas on how to sabotage their political opponents . After Die Hard 4 was released , he said the idea was now public . He hired the researcher that identified the Stuxnet worm , which is believed to be the first instance of state @-@ sponsored cyberweapon . Afterwards , the company exposed the Flame virus at the request of the International Telecommunication Union . The virus was believed to have been used for cyber @-@ espionage in Middle @-@ Eastern countries .

Kaspersky Lab developed a reputation for discovering cybersecurity threats . In 2015 Kaspersky and Kaspersky Lab discovered a group of hackers known as Carbanak that were stealing money from banks . They also exposed Equation Group , which developed advanced spyware for monitoring desktop activity and was believed to be affiliated with National Security Agency in the U.S. According to The Economist , it was these discoveries , Kaspersky 's " relentless salesmanship " and the company 's anti @-@ virus product that made Kaspersky Lab uncommon as an internationally recognized Russian company .

= = = CEO = = =

Kaspersky became CEO of Kaspersky Lab in 2007 . According to a 2008 article in USA Today , he traveled to 20 to 30 countries per year promoting Kaspersky Lab products . In early 2009 , CRN said his personality contributed to the company 's growth from " relative obscurity to now nipping at the heels of its larger , better @-@ known rivals . " At the time , Kaspersky Lab was the fourth largest endpoint security company . It introduced new products for the enterprise market and expanded its channel programs .

In 2011 , Kaspersky made a decision against taking the company public , saying it would make decision @-@ making slow and prevent long @-@ term R & D investments . This led to a series of high @-@ level departures from the company , including his ex @-@ wife and co @-@ founder . Another series of departures occurred in 2014 due to disagreements over how to run the company .

Kaspersky Lab has defended itself against allegedly frivolous patent claims more aggressively than most IT companies . In 2012 , it was the only one of 35 firms named in a suit by patent troll Information Protection and Authentication (IPAC) to take the case to court , rather than pay a fee . The case was ruled in Kaspersky 's favor . Also in 2012 , another company , Lodsys , sued Kaspersky and 54 other companies for patent infringement , and that case also resulted in the claimant dropping the case against Kaspersky . According to an article in TechWorld , the company 's aversion to settling these claims is most likely because Eugene " just hates " patent trolls . In his blog he called them " parasites " and " IT racketeers . " Kaspersky himself is the co @-@ author of several patents , including one for a constraint @-@ and @-@ attribute @-@ based security system for controlling software component interaction .

As of 2015 , Kaspersky Lab now employs more than 2 @,@ 800 people . As of 2012 , Kaspersky

has been working on developing software to protect critical infrastructure , like power plants , from cyberwarfare . He throws a New Years party each year with about 1 @,@ 500 guests and hosts Kaspersky conferences in exotic locations .

= = Controversies = =

= = = Alleged affiliations with Russia = = =

Eugene Kaspersky 's prior work for the Russian military and his education at a KGB @-@ sponsored technical college has led to controversy about whether he uses his position to advance Russian government interests and intelligence efforts . According to Kaspersky , allegations of dubious connections with Russian agencies began after he got his first clients in America . He spends much of his working life trying to get governments and organizations to trust him and his software in spite of the allegations .

Wired said Kaspersky 's critics accuse him of using the company to spy on users for Russian intelligence . Russian telecommunications companies for example are required by federal law in Russia to cooperate with the government 's military and spy operations if asked . Kaspersky said his company has never been asked to tamper with its software for espionage and called the accusations " cold war paranoia . " According to Wired , Kaspersky staffers argue " not unconvincingly " that spying on users would hurt its business and its relationship with the Russian FSB is limited . According to Gartner , " There 's no evidence that they have any back doors in their software or any ties to the Russian mafia or state ... but there is still a concern that you can ? t operate in Russia without being controlled by the ruling party . ? Computing mocked some of the more extreme accusations of espionage , but said it would be unlikely for a Russian business to grow to the size of Kaspersky Lab without relationships within the Russian government . NPR journalists also said it was unlikely Kaspersky was using its software for espionage , because it would be risky for the company 's business , but said Kaspersky showed an unusual disinterest in Russia @-@ based cybercrime .

Bloomberg and The New York Times also said Kaspersky was less aggressive about identifying cyberattacks originating from Russia than from other countries , allegations Kaspersky refutes . For example , he allegedly ignored or downplayed a series of denial @-@ of @-@ service attacks in December 2011 that were made to disrupt online discussion criticizing Russian politicians . Kaspersky also allegedly ignored a Russian @-@ based spyware called Sofacy , which is believed to have been used by Russia against NATO and Eastern Europe . On the other hand , Kaspersky also published information on the Russia @-@ based Crouching Yeti cyberattacks two days before Bloomberg accused him of ignoring Russia @-@ based cyberattacks . At the time , the company had published eleven reports on malicious Russian programs . Competitor FireEye said it is awkward even in the U.S. to investigate cybercrimes performed by your own government .

A March 2015 article in Bloomberg said an increasing number of executive staff at Kaspersky Lab previously worked for Russian military and intelligence agencies . According to News & Observer , Kaspersky " published a mammoth response , tearing down Bloomberg 's accusations and accusing them of throwing facts out the window for the sake of a juicy anti @-@ Russian narrative . " Competitor FireEye said many U.S. IT companies also have executives that formerly worked for government military and intelligence agencies . NPR reported that Kaspersky has been doing an increasing amount of business with Russian cybersecurity agencies to catch cybercriminals . Kaspersky confirms that Russian agencies are among its government customers .

= = = Alleged anti @-@ virus spoofing = = =

In August 2015 , two former Kaspersky employees alleged that the company introduced modified files into the VirusTotal community anti @-@ virus database to trick its rivals ' programs into triggering false positives . The result of the false positives was that important uninfected files would

be disabled or deleted . The allegations also claimed that Kaspersky himself had ordered some of the actions , specifically targeting competitors , including Chinese companies he felt were copying his software . Emails dated 2009 , two years after Kaspersky became CEO , were allegedly leaked to Reuters , one of which allegedly had Kaspersky threatening to go after competitors by " rubbing them out in the outhouse , " using a phrase popularized by Vladimir Putin . The company denied the allegations .

= = Personal life = =

Eugene Kaspersky lives in Moscow , Russia with his wife and kids . He and his first wife were divorced in 1998 . On 21 April 2011 , his son , Ivan , then 20 , was kidnapped for a $ 4 @.@ 4 million ransom . Kaspersky worked with a friend at the FSB and Russian police to trace the ransomer 's phone call . They set up a trap for the ransomers , where they rescued his son and arrested many of the kidnappers . The incident had an influence on Kaspersky 's sense of personal security . He now travels with a bodyguard and security detail .

Kaspersky is one of the richest people in Russia . His net worth is about $ 1 billion . According to Wired , he has " cultivated the image of a wild man with cash to burn . " He has an interest in racing and drives his sports cars on race tracks as a hobby . He sponsors various " quirky or scientific projects " such as Ferrari Formula One racing team . Kaspersky himself owns a BMW M3 . Kaspersky describes himself as an " adrenaline junky . " He has gone hiking on volcanoes in Russia and reserved a trip to space on the Virgin Galactic . He travels often and writes about his experiences in his personal blog . He also enjoys photography as a hobby .

Kaspersky is known for shunning formal attire , typically dressing in jeans and a shirt . He supports university projects and competitions in the IT security field .

= = Views = =

Eugene Kaspersky is influential among politicians and security experts . He has been active in promoting warnings about the possibility of cyberwarfare that targets critical infrastructure . He regularly speaks at conferences advocating for an international cyberwarfare treaty , that would ban government @-@ sponsored cyberattacks .

After the Stuxnet attack , Kaspersky proposed that the internet needed more regulation and policing . One idea was to have some parts of the internet anonymous , while more secure areas require user identification . He argued that anonymity mostly benefited cybercriminals and hackers . For example , accessing a network operated by a nuclear power plant could require a verified identity through a digital passport .

Kaspersky said anonymity on the internet could be protected by using a proxy , whereby a responsible international body maintains a record of which online identities correspond to which real @-@ world ones . For example , a browser 's identity would be revealed in cases of malicious activity . Some security experts believe that a centralized database of the real @-@ world identities of internet users would be " a privacy disaster and a highly attractive target for thieves . " The Age said it " sounds a little too close for comfort to a Big Brother scenario " and Wired said Kaspersky 's views were highly aligned with the Russian government 's agenda .

Many organizations have been considering reducing privacy to improve security as a result of Kaspersky 's arguments . In a more recent Slashdot interview Kaspersky said the internet should be divided into three zones : a red zone for voting , online banking , and other " critical transactions " that would require an internet ID ; a grey zone that may only require verification of age to access the site , but not identity ; and a green zone for blogs , news , and " everything related to your freedom of speech . " He proposes " special proxies " for red zone websites that allow disclosure of the user 's identity only in the case of suspected malfeasance .