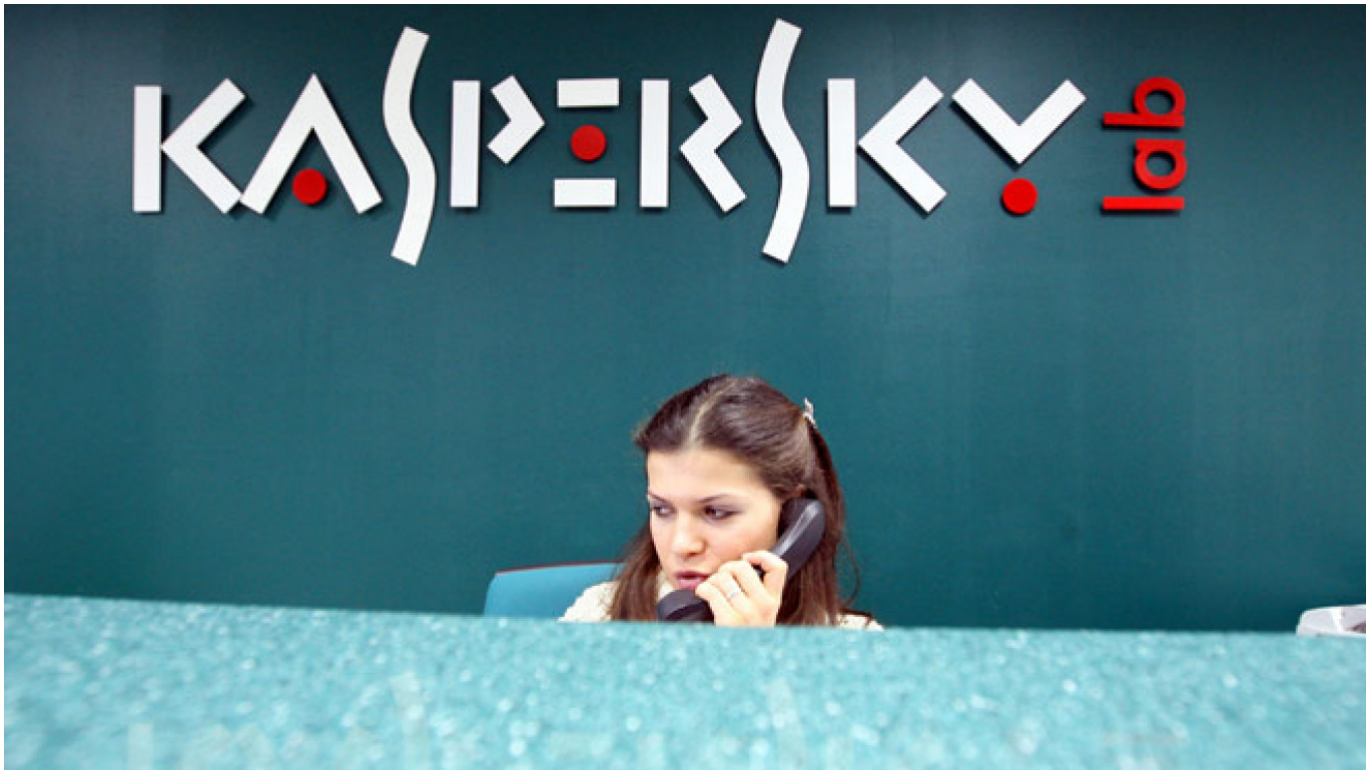
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russia's Kaspersky Threatened to 'Rub Out' Rival, E-mail Shows

August 30, 2015



In 2002, Kaspersky Lab had been struggling to gain traction in the massive Chinese market, where piracy was rampant in the software industry, according to former employees.

In 2009, Eugene Kaspersky, co-founder of one of the world's top security companies, told some of his lieutenants that they should attack rival antivirus software maker AVG Technologies N.V. by "rubbing them out in the outhouse," one of several previously undisclosed e-mails shows.

He was quoting from President Vladimir Putin's famous threat a decade earlier to pursue Chechen rebels wherever they were: "If we catch them in the toilet, then we will rub them out in the outhouse."

Former employees say that the reprisal Kaspersky was pushing for was to trick AVG's antivirus software into producing false positives — that is, misclassifying clean computer files as infected.

The plan involved creating fake virus samples and malware identifications to fool competitors

into disabling or deleting important files, thereby creating problems for their customers.

“More and more I get the desire to smack them with their falses,” Kaspersky wrote in Russian in one e-mail seen by Reuters, dated July 23, 2009. He accused AVG of poaching staff from his company. “AVG is carrying out an HR attack on the company, mostly the managers.”

The e-mails shed fresh light on the allegations of two former Kaspersky Lab employees that the Moscow-based company had sought to sabotage rivals to gain market share and retaliate against competitors it believed were mimicking its malware detections instead of relying on their own research.

Kaspersky Lab has strongly denied the allegations. On Friday, it said the e-mails “may not be legitimate and were obtained from anonymous sources that have a hidden agenda.”

“Kaspersky Lab has never conducted any secret campaign to trick competitors into generating false positives to damage their market standing. Such actions are unethical, dishonest and illegal,” the company said in a statement.

The ex-employees told Reuters that AVG, Microsoft Corp and Avast Software were among the companies targeted by Kaspersky Lab in campaigns between 2009 and 2013 to spread false positives through threat information-sharing programs.

“To be honest, I’ll feel pretty bad when AVG goes public and earns a billion. They won’t say thanks to you or me — don’t even hope,” Kaspersky wrote in another e-mail seen by Reuters, dated Oct. 8, 2009.

“‘Rubbing out’ — is one of the methods, which we will DEFINITELY use in combination with other methods.”

A day earlier, Kaspersky had urged his team in another e-mail to consider “rubbing them out in the outhouse,” noting that his European chief was “very positive about falses.” The e-mails do not confirm that an attack was launched against AVG or say how effective it might have been.

AVG’s former chief technology officer, Yuval Ben-Itzhak, previously told Reuters the company was hit with waves of doctored virus samples from 2009 to 2013.

AVG, Microsoft and Avast have all declined to comment on who might have been behind the sophisticated assaults. AVG did not immediately respond to a request for comment on the e-mails.

In the e-mails, Eugene Kaspersky did not give specifics on the “rubbing out” method that he envisioned using against AVG. But he said it was a trick that the company had used against a competitor in China years ago. He did not identify the company in the e-mail.

“We’ve already had an experience ‘rubbing out’ — in China. In year 2002-2003. And we did end up moving one of the then-market leaders,” Kaspersky wrote.

A former Kaspersky Lab employee said the Chinese target was Beijing Jiangmin New Science & Technology Co, one of the biggest antivirus companies in the country at the time. Jiangmin

General Manager Guo Changsheng declined to comment.

In 2002, Kaspersky Lab had been struggling to gain traction in the massive Chinese market, where piracy was rampant in the software industry, according to former employees.

Jiangmin did well in part because it copied Kaspersky Lab's identifications of malicious software files, said two former software engineers at Jiangmin, and a Chinese expert who had worked with both companies. The three sources spoke on condition of anonymity.

After repeated threats and attempts to reach a licensing deal with Jiangmin failed, the Chinese expert said, Kaspersky Lab began to fake some of its malware detections in China in order to cause problems on Jiangmin's customer machines when the Chinese company copied them.

Kaspersky Lab did this to protect itself from more piracy, the Chinese expert said, adding that the campaign worked. "All of a sudden, customers came to Kaspersky."

Jiangmin's general manager declined to comment on the allegations that the company copied Kaspersky Lab's detections. He also declined to comment on whether Jiangmin had suffered from false detections during the period in question.

Kaspersky Lab has previously said that it too had been hit with fake virus samples. It declined to provide copies of the samples or give other details.

It is not known how much business Kaspersky Lab may have gained in China or elsewhere as a result of these alleged attacks.

In one of the e-mails, Eugene Kaspersky said the China attack, which he called a "rubber bomb," was a success. The term "rubber bomb" comes from a Russian joke about an explosive that keeps bouncing and inflicting more damage.

"Something tells me that without that 'rubber bomb,' things wouldn't be so rosy for us in China," Kaspersky wrote in the Oct. 8, 2009 e-mail.

Original url:
https://www.themoscowtimes.com/2015/08/30/russias-kaspersky-threatened-to-rub-out-rival-e-mail-shows-a49231