Kaspersky: We uploaded US documents but quickly deleted them

October 25 2017, by Raphael Satter

In this July 1, 2017, file photo, Eugene Kaspersky, Russian antivirus programs developer and chief executive of Russia's Kaspersky Lab, poses for a photo on a balcony at his company's headquarters in Moscow, Russia. The founder of Russian anti-virus firm Kaspersky tells The Associated Press his company did upload classified U.S. documents a couple of years ago, only to delete them immediately after realizing what had happened. Kaspersky's acknowledgement is the first on-the-record confirmation of an incident described earlier this month in three U.S. newspapers.(AP Photo/Pavel Golovkin, File)

Sometime in 2014, a group of analysts walked into the office of Eugene Kaspersky, the ebullient founder of Russian cybersecurity firm Kaspersky Lab, to deliver some sobering news.

Kaspersky's anti-virus software had automatically scraped powerful digital surveillance tools off a computer in the United States and the analysts were worried: The data's headers clearly identified the files as classified.

"They immediately came to my office," Kaspersky recalled, "and they told me that they have a problem."

He said there was no hesitation about what to do with the cache.

"It must be deleted," Kaspersky says he told them.

The incident, recounted by Kaspersky during a brief telephone interview on Tuesday and supplemented by a timeline and other information provided by company officials, could not immediately be corroborated. But it's the first public acknowledgement of a story that has been building for the past three weeks—that Kaspersky's popular anti-virus program uploaded powerful digital espionage tools belonging to the National Security Agency from a computer in the United States and sent them to servers in Moscow.

The account provides new perspective on the U.S. government's recent move to blacklist Kaspersky from federal computer networks, even if it still leaves important questions unanswered.

To hear Kaspersky tell it, the incident was an accident borne of carelessness.

Analysts at his company were already on the trail of the Equation

Group—a powerful group of hackers later exposed as an arm of the NSA—when a computer in the United States was flagged for further investigation. The machine's owner, identified in media reports as an NSA worker, had run anti-virus scans on their home computer after it was infected by a pirated copy of Microsoft Office, according to a Kaspersky timeline released Wednesday.

The scan didn't just treat the infection. It also triggered an alert for Equation Group files the worker had left in a compressed archive which was then spirited to Moscow for analysis.

Kaspersky's story at least partially matches accounts published in The New York Times, The Washington Post and The Wall Street Journal. All three publications recently reported that someone at the NSA's elite hacking unit lost control of some of the agency's powerful surveillance tools after they brought their work home with them, leaving what should have been closely guarded code on a personal computer running Kaspersky's anti-virus software.

But information security experts puzzling over the hints dropped by anonymous government officials are still wondering at whether Kaspersky is suspected of deliberately hunting for confidential data or was merely doing its job by sniffing out suspicious files.

Much of the ambiguity is down to the nature of modern anti-virus software, which routinely submits rogue files back to company servers for analysis. The software can easily be quietly tweaked to scoop up other files, too: perhaps classified documents belonging to a foreign rival's government, for example.

Concerns have been fanned by increasingly explicit warnings from U.S. government officials after tensions with Russia escalated in the wake of the 2016 presidential election.

Kaspersky denies any inappropriate link to the Russian government, and said in his interview that any classified documents inadvertently swept up by his software would be destroyed on discovery.

"If we see confidential or classified information, it will be immediately deleted and that was exactly (what happened in) this case," he said, adding that the order had since been written into company policy.

An AP request for a copy of that policy wasn't immediately granted.

Kaspersky's account still has some gaps. For example, why not alert American authorities to what happened? The newspaper reports alleged that the U.S. learned that Kaspersky had acquired the NSA's tools via an Israeli spying operation.

Kaspersky declined to say whether he had ever alerted U.S. authorities to the incident.

"Do you really think that I want to see in the news that I tried to contact the NSA to report this case?" he said at one point. "Definitely I don't want to see that in the news."

So did he alert the NSA to the incident or not?

"I'm afraid I can't answer the question," he said.

Even if some questions linger, Kaspersky's explanation sounds plausible, said Jake Williams, a former NSA analyst and the founder of Augusta, Georgia-based Rendition InfoSec. He noted that Kaspersky was pitching itself at the time to government clients in the United States and may not have wanted the risk of having classified documents on its network.

"It makes sense that they pulled those up and looked at the classification

marking and then deleted them," said Williams. "I can see where it's so toxic you may not want it on your systems."

As for the insinuation that someone at the NSA not only walked highly classified software out of the building but put it on a computer running a bootleg version of Office, Williams called it "absolutely wild."

"It's hard to imagine a worse PR nightmare for the NSA," he said.