Exclusive: Kaspersky Software Lingers On Sensitive Government Systems 2 Years After U.S. Ban

Thomas Brewster
Forbes, Aug 8, 2019

Removing Kaspersky Lab's antivirus software has proved a challenge for U.S government agencies.

In September 2017, the U.S. government said it was going to outlaw the use of security software from Russian company Kaspersky Lab. Government departments had 90 days to start to remove the antivirus software, deemed an intelligence risk because of fears the Kremlin had influence over the Moscow-based company, something Kaspersky has always denied.

But nearly two years on, the U.S. still can't shift Kaspersky software from even military networks, according to an ex-CIA analyst, whose company has been on the lookout for the Russian tech. Tim Junio, co-founder of Expanse, gave *Forbes* exclusive research from his team, who claimed Kaspersky was, at a minimum, sitting on two U.S. government military networks. Kaspersky was also detected within eight government non-military networks and 14 defense contractors. Such contractors were prohibited from using Kaspersky in any work with U.S. agencies from October last year.

Critical private industry companies were also not immune: Expanse, which has received Department of Defense backing since founding in 2016, found 19 financial services companies and 17 healthcare businesses, all in the Fortune 100, were still running Kaspersky.

The bottom line, Junio told *Forbes*, was that even "the most elite, highest cybersecurity spend organizations in the world are still dealing with the Kaspersky problem."

U.S. Senator Jeanne Shaheen, who led the charge in crafting legislation to rid the Russian security tools from American government computers, said "rooting out Kaspersky software from federal computers and networks has always been a tall order but one that's absolutely vital to national security.

"It's disappointing that some government computers still have Kaspersky products installed and I hope that the Trump administration will redouble their efforts to finish the job. As long as Kaspersky is present on federal systems they are vulnerable to foreign intrusion," she told *Forbes*.

A Kaspersky spokesperson said: "The company maintains that no public evidence of any wrongdoing has been presented by the U.S. Government, including any technical evidence that its products present risks materially greater than other similar anti-virus products.

"Kaspersky continues to demonstrate its ongoing commitment to assuring the integrity and trustworthiness of its products and the protection of its users' data through its Global Transparency Initiative." Kaspersky unsuccessfully sued the Trump administration over the ruling and announced plans in 2018 to build new data centres in Switzerland as a part of this "transparency" initiative.

American companies shipping Russian tools

Junio's researchers were looking at traffic between customer networks and servers that Kaspersky controls.

Though there may be some cases of employees bringing in Kaspersky software and using it on government networks, Junio told *Forbes* his team believe the Russian software is deeply embedded in other products purchased by the U.S. government. This forms part of a "whitelabelling" problem where Kaspersky tools are being used in hardware like security appliances from other companies, some of them trusted American suppliers.

Matt Kraning, CTO at Expanse, said that at the core of the issue is the complexity of large organization computing infrastructure. "Everyone is still fighting fires because everything is so complex," Kraning said.

The government, meanwhile, is convinced it has fixed the Kaspersky problem despite the evidence from Expanse. A spokesperson at the Department of Homeland Security told *Forbes* that by April 9 2018, all federal agencies had confirmed that either they didn't have Kaspersky on their networks or had taken action to remove the software. Government departments had also claimed to have removed Kaspersky from third-party tech too.

Rooting out Chinese tech

It's not just Kaspersky that the U.S. government is going to have trouble removing. The National Defense Authorization Act (NDAA) bans government departments from using technology from Chinese firms Huawei, HikVision, ZTE and Dahua, over similar concerns that they pose a national security risk. From August 13, government departments have to outline just how they're removing those manufacturers' technologies.

Data provided to *Forbes* from Forescout Technologies showed just how prevalent those technologies are. Looking specifically at Chinese surveillance camera makers, Forescout said there were 1,162 HikVision devices and 822 Dahua systems on government networks as of July 11.

As with Kaspersky, pinning down exactly where those technologies are is a work in progress. "We're hearing from customers they're still on networks and they're actively trying to locate them," said Katherine Gronberg, vice president at government affairs for Forescout. "These are really complex supply chains. I'm not sure anyone is going to be able to trace to the second, third, fourth degree, where your hardware and software components are coming from.