Blacklisted Kaspersky tipped NSA on security breach: media

January 10 2019

Kaspersky Lab's headquarters in Moscow

The computer security firm Kaspersky Labs helped the US NSA spy agency uncover one of its worst-ever security breaches—one year before the US banned the company's products for government use, US media has reported.

Politico and the Washington Post said the Moscow-based maker of anti-malware products told the National Security Agency that one of its contractors, Harold Martin, had contacted it via cryptic messages on Twitter.

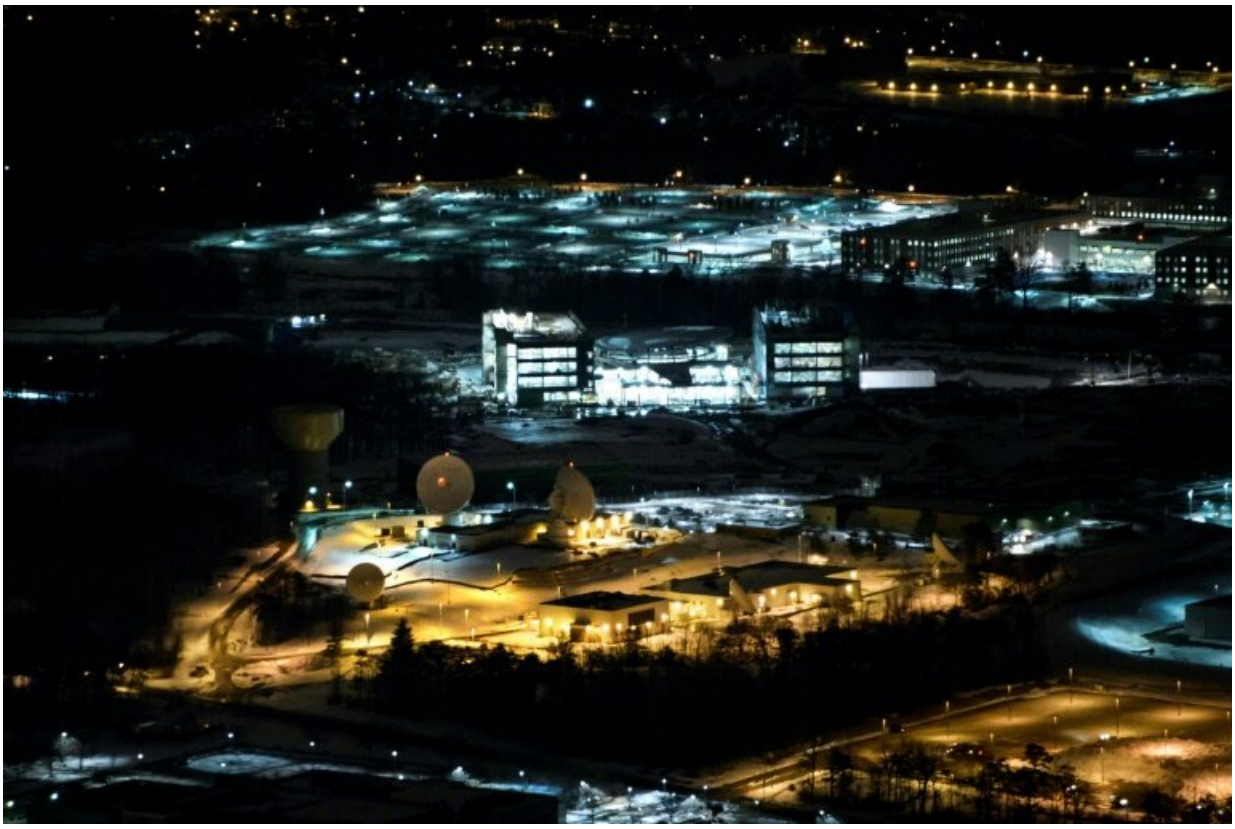
The messages arrived at Kaspersky shortly before unknown hackers known as the "Shadow Brokers" made available on the internet an assembly of advanced hacking tools that the ultra-secret signals intelligence body used to spy on the communications and computers of foreign governments and officials.

After the Shadow Brokers release, Kaspersky researchers thought there was a connection with Martin's messages and reached out with the information to the NSA.

Weeks later, in August 2016, federal agents arrested the contractor, Harold Martin, discovering that he had stockpiled in his home a massive amount of sensitive NSA data, computer code and programs—some 50 terabytes worth—over two decades.

It was considered the largest-ever breach of classified data in US history.

According to the reports, the Twitter messages were used to justify the warrant issued to investigators to search Martin's home.



The National Security Agency, the US government's premier signals intelligence agency, has its headquarters in Fort Meade, Maryland

The Kaspersky assistance "indicates that the government's own internal monitoring systems and investigators had little to do with catching Martin," Politico wrote, citing two unnamed sources familiar with the Martin investigation.

But within months, the NSA decided that Kaspersky itself could have been instrumental in another leak of its hacking tools, and in September 2017 officially banned the use of Kaspersky software from computers involved in any government operations.

US intelligence officials—including then-NSA chief Michael

Rogers—suggested Kaspersky had intimate ties to Russian intelligence.

"The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates US national security," acting secretary of Homeland Security Elaine Duke said at the time.

Kaspersky strenuously denied the allegation. But it took a heavy toll on Kaspersky's two-decade-old business that saw its anti-virus software installed on hundreds of millions of computers around the world.

Both the NSA and Kaspersky declined to comment, with the NSA citing the ongoing litigation regarding Martin.

Martin has been charged with theft of and illegal retention of classified data in his Maryland home.

But he has not been charged with leaking the materials to the Shadow Brokers or any others.