Exclusive: FBI probes Russian-linked postcard sent to FireEye CEO after cybersecurity firm uncovered hack - sources

reuters.com/article/us-global-cyber-fireeye/exclusive-fbi-probes-russian-linked-postcard-sent-to-fireeye-ceo-after-cybersecurity-firm-uncovered-hack-sources-idUSKBN29G2IG

Christopher Bing

Cyber Risk
Updated

By Christopher Bing

4 Min Read

(Reuters) - The FBI is investigating a mysterious postcard sent to the home of cybersecurity firm FireEye's chief executive days after it found initial evidence of a suspected Russian hacking operation on dozens of U.S. government agencies and private American companies.

Slideshow (2 images)

U.S. officials familiar with the postcard are investigating whether it was sent by people associated with a Russian intelligence service due its timing and content, which suggests internal knowledge of last year's hack well before it was publicly disclosed in December.

Moscow has denied involvement in the hack, which U.S. intelligence agencies publicly attributed here to Russian state actors.

The postcard carries FireEye's logo, is addressed to CEO Kevin Mandia, and calls into question the ability of the Milpitas, California-based firm to accurately attribute cyber operations to the Russian government.

People familiar with Mandia's postcard summarized its content to Reuters. It shows a cartoon with the text: "Hey look Russians" and "Putin did it!"

The opaque message itself did not help FireEye find the breach, but rather arrived in the early stages of its investigation. This has led people familiar with the matter to believe the sender was attempting to "troll" or push the company off the trail by intimidating a senior executive.

Reuters could not determine who sent the postcard. U.S. law enforcement and intelligence agencies are spearheading the probe into its origin, the sources familiar said.

The FBI did not provide comment. A FireEye representative declined to discuss the postcard.

A disinformation researcher from the Rand Corporation, Todd Helmus, received a similar postcard in 2019, based on an image of it Helmus posted to Twitter. Helmus, who studies digital propaganda, said he received the postcard after testifying to Congress about Russian disinformation tactics.

FireEye discovered the Russian hacking campaign - now known as "Solorigate" for how it leveraged supply chain vulnerabilities in network management firm Solarwinds - because of an anomalous device login from within FireEye's network. The odd login triggered a security alert and subsequent investigation, which led to the discovery of the operation.

FireEye worked closely with Microsoft to determine that the infiltration at FireEye in fact represented a hacking campaign that struck at least eight federal agencies including the Treasury, State and Commerce Departments.

When the postcard was sent, FireEye had not yet determined who was behind the cyberattack. A person familiar with the postcard investigation said "this is not typically the Russian SVR's playbook" but "times are rapidly changing." SVR is an acronym for the Foreign Intelligence Service of Russia.

A former U.S. intelligence official said the postcard reminded him of a now public mission by U.S. Cyber Command where they sent private messages to Russian hackers ahead of the 2018 congressional elections in the United States.

“The message then from the U.S. was ‘watch your back, we see you’ similar to here,” the former official said.

The extent of the damages tied to the U.S. government hack remains unclear. Emails belonging to senior officials were stolen from an unclassified network at the Treasury and Commerce Departments.

Reporting by Christopher Bing; editing by Grant McCool

Our Standards: The Thomson Reuters Trust Principles.