Cybersecurity firm FireEye says was hacked by nation state

December 9 2020, by Frank Bajak and Matt O'brien

This Wednesday, Feb. 11, 2015 photo shows FireEye offices in Milpitas, Calif. The cybersecurity firm said Tuesday, Dec. 8, 2020 it was hacked by what it believes was a national government. The attacker targeted and stole assessment tools that FireEye uses to test its customers' security and which mimic the methods used by hackers, the company said. (AP Photo/Ben Margot)

Prominent U.S. cybersecurity firm FireEye said Tuesday that foreign government hackers with "world-class capabilities" broke into its network and stole offensive tools it uses to probe the defenses of its thousands of customers, who include federal, state and local governments and major global corporations.

The hackers "primarily sought information related to certain government customers," FireEye CEO Kevin Mandia said in a such as Facebook of malicious campaigns.

FireEye said it is investigating the attack in coordination with the FBI and other partners such as Microsoft, which has its own cybersecurity team. Mandia said the hackers used "a novel combination of techniques not witnessed by us or our partners in the past."

Matt Gorham, assistant director of the FBI's cyber division, concurred that the hackers' "high level of sophistication (was) consistent with a nation state." He said the government is "focused on imposing risk and consequences on malicious cyber actors, so they think twice before attempting an intrusion in the first place."

That has included what the U.S. Cyber Command terms "defending forward" operations, which include penetrating networks of adversaries, including Russia.

The nation's Cybersecurity and Infrastructure Security Agency said Tuesday warned that "unauthorized third-party users could abuse" the stolen red-team hacking tools that FireEye uses to try to penetrate its customers' defenses.

U.S. Sen. Mark Warner, a Virginia Democrat on the Senate's intelligence committee, applauded FireEye for quickly disclosing the intrusion and said the case "shows the difficulty of stopping determined nation-state

hackers."

Cybersecurity expert Dmitri Alperovitch said he was not surprised by the announcement because companies like FireEye are top targets. In the past, breached security companies have included such big names as Kaspersky and Symantec, he noted.

"Every security company is being targeted by nation-state actors. This has been going on got over a decade now," said Alperovitch, the co-founder and former chief technical officer of Crowdstrike, which investigated the 2016 Russian hack of the Democratic National Committee and Hillary Clinton's campaign.

He said the release of the "red-team" tools, while a serious concern, was "not the end of the world because threat actors always create new tools."

"This could have been much worse if their customer data had been hacked and exfiltrated. So far there is no evidence of that," Alperovitch said.

He said from what is currently known, the hack is not as serious as the hacks of two other cybersecurity companies—RSA Security in 2011 and Bit9 two years later—because they contributed to the compromise of customer data.

Founded in 2004, FireEye went public in 2013 and months later acquired Virginia-based Mandiant Corp., the firm that linked years of cyberattacks against U.S. companies to a secret Chinese military unit. It had about 3,400 employees and $889.2 million in revenue last year, though with a net loss of $257.4 million. It has reported operating losses each year since its inception, according to its financial filings.

The company's 8,800 customers last year included more than half of the

Forbes Global 2000, companies in telecommunications, technology, financial services, healthcare, electric grid operators, pharmaceutical companies and the oil-and-gas industry.

Its stock fell more than 7% in after-hours trading Tuesday following news of the hack.