UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, DC 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 or 15(d) of
The Securities Exchange Act of 1934

Date of Report (Date of earliest event reported): December 8, 2020

FireEye, Inc.
(Exact name of registrant as specified in its charter)

Delaware	**001-36067**	**20-1548921**
(State or other jurisdiction of incorporation)	**(Commission File Number)**	**(IRS Employer Identification No.)**

601 McCarthy Blvd.
Milpitas, CA 95035
(Address of principal executive offices, including zip code)

(408) 321-6300
(Registrant's telephone number, including area code)

Not Applicable
(Former name or former address, if changed since last report.)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions (see General Instruction A.2. below):

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Common Stock, par value $0.0001 per share	**FEYE**	**The NASDAQ Global Select Market**

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter).

Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Item 8.01 Other Events.

On December 8, 2020, concurrently with the filing of this Current Report on Form 8-K, FireEye, Inc. ("FireEye", “we”, “our” or “us”) is announcing on our corporate blog that FireEye recently was attacked by a highly sophisticated cyber threat actor, one whose discipline, operational security, and techniques lead us to believe it was a state-sponsored attack. Based on his 25 years in cyber security and responding to incidents, Kevin Mandia, our Chief Executive Officer, concluded we are witnessing an attack by a nation with top-tier offensive capabilities. This attack is different from the tens of thousands of incidents we have responded to throughout the years. The attackers tailored their world-class capabilities specifically to target and attack FireEye. They are highly trained in operational security and executed with discipline and focus. They operated clandestinely, using methods that counter security tools and forensic examination. They used a novel combination of techniques not witnessed by us or our partners in the past. We are actively investigating in coordination with the Federal Bureau of Investigation and other key partners, including Microsoft. Their initial analysis supports our conclusion that this was the work of a highly sophisticated state-sponsored attacker utilizing novel techniques.

During our investigation to date, we have found that the attacker targeted and accessed certain Red Team assessment tools that we use to test our customers’ security. These tools mimic the behavior of many cyber threat actors and enable FireEye to provide essential diagnostic security services to our customers. None of the tools contain zero-day exploits. Consistent with our goal to protect the community, we are proactively releasing methods and means to detect the use of our stolen Red Team tools. We are not sure if the attacker intends to use our Red Team tools or to publicly disclose them. Nevertheless, out of an abundance of caution, we have developed more than 300 countermeasures for our customers, and the community at large, to use in order to minimize the potential impact of the theft of these tools. We have seen no evidence to date that any attacker has used the stolen Red Team tools. We, as well as others in the security community, will continue to monitor for any such activity. At this time, we want to ensure that the entire security community is both aware and protected against the attempted use of these Red Team tools.

Consistent with a nation-state cyber-espionage effort, the attacker primarily sought information related to certain government customers. While the attacker was able to access some of our internal systems, at this point in our investigation, we have seen no evidence that the attacker exfiltrated data from our primary systems that store customer information from our incident response or consulting engagements or the metadata collected by our products in our dynamic threat intelligence systems. If we discover that customer information was taken, we will contact them directly.

For additional information, please see FireEye's corporate blog at fireeye.com/blog. We currently intend that any further announcements regarding the security incident will be disclosed on our corporate blog at fireeye.com/blog or social media (twitter.com/fireeye; twitter.com/mandiant; facebook.com/FireEye/; and/or linkedin.com/company/fireeye).

Forward Looking Statements

Certain statements contained in this Current Report on Form 8-K constitute “forward-looking statements” within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended. These forward-looking statements are based on our current beliefs, understanding and expectations and may relate to, among other things, statements regarding our current beliefs and understanding regarding the impact and scale of the disclosed event and our understanding of what occurred. Forward-looking statements are based on currently available information and our current beliefs, expectations and understanding, which may change as the investigation proceeds and more is learned, including what was targeted and accessed by the attacker. These statements are subject to future events, risks and uncertainties – many of which are beyond our control or are currently unknown to FireEye. These risks and uncertainties include but are not limited to our ongoing investigation, including the potential discovery of new information related to the incident.

Forward-looking statements speak only as of the date they are made, and while we intend to provide additional information regarding the attack, FireEye does not undertake to update these statements other than as required by law and specifically disclaims any duty to do so.

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

FIREEYE, INC.

Date: December 8, 2020

By: /s/ Alexa King

Alexa King
Executive Vice President, General Counsel and Secretary