# FireEye's Mandia: 'Severity-Zero Alert' Led to Discovery of SolarWinds Attack

By Kelly Jackson Higgins

Published: 2021-01-07 · Archived: 2026-04-05 18:47:55 UTC

FireEye CEO Kevin Mandia today shared some insight on the cyberattack on the security firm that was the first clue to a massive and wide-ranging attack campaign against several major US government and commercial networks.

In a panel today hosted by the Aspen Institute, Mandia described how his company first recognized the serious attack it had suffered, describing how a newly registered phone using a FireEye user account was the first indication of malicious activity. "In this particular case, the event that got briefed to me and got us to escalate and declare this a full-blown incident was somebody was accessing our network just like we do, but they were doing it with a second registered device," he explained. The FireEye user whose account was associated with the flagged access was contacted and asked if he had registered a new phone, but he had not.

"Even though this was a severity-zero alert" at first, Mandia said, it was evidence of a major security event. "We had somebody bypassing our two-factor authentication by registering a new device and accessing our network just like our employees do, but it actually wasn't our employee" doing it, he said.

Details about the illicit phone used in the attack was first reported by Yahoo News last month, in an interview with Charles Carmakal, senior vice president and CTO of FireEye. "They had to provide credentials to authenticate [their device] to the [multifactor authentication system] in order to authenticate to the FireEye VPN," Carmakal told Yahoo News. "It was the process the attacker followed to enroll in the MFA solution, which is what generated the alert. But at this point, the attacker already had the employee's username and password."

Mandia said that method of attack was a big red flag. "The minute we saw that, we recognized that's the kind of tradecraft advanced groups would do," Mandia noted. No malware, and under the guise of a legitimate user, "doing exactly what your employees do when they go to work every day."

"There's no magical wand that ... finds backdoors in software that we all purchase and trust," he said. "What led us to do that [decompiling] work was, in fact, all of the forensics" we conducted beforehand, he says.FireEye had investigated packet captures and forensic software logs on its endpoints and found one common thread: "It kept backing into, the earliest evidence of compromise for us was the system that harbored the SolarWinds product," he said. So, the company went to work decompiling code and found 4,000 lines of malicious code.

The attackers planted malware in legitimate updates to SolarWinds' Orion network management software that was sent to some 18,000 public and private sector customers of the software. According to US intelligence assessments, a very small number of those organizations actually were targeted and compromised.

The Attack on FireEye

Stage one of the attack planted the backdoor onto FireEye's network via the SolarWinds platform, Mandia said. Stage two used the backdoor to access domain credentials, he said, such as user accounts and passphrases. "Stage three was to get the token signing-certs to access O365, likely for specific email accounts," Mandia said. The final stage of the FireEye attack was the theft of its red-team tools.

Mandia said he had not seen many ".com" breaches for this type of espionage, so the attack group behind this "smells different."

While the US intelligence community as well as several government officials and security experts have cited Russia as the perpetrator, FireEye has not done so. The company has attributed the attack to an unknown or unclassified group or nation-state. "We have not made any attribution beyond assigning this activity to UNC 2452. An UNC group, short for unclassified, is a cluster of cyber-intrusion activity — which includes observable artifacts such as adversary infrastructure, tools, and tradecraft — that we are not yet ready to give a classification such as APT or FIN," a FireEye spokesperson said. "As we collect additional intelligence, UNC group activity can be assigned to an existing group, graduated to a new group, or simply remain unclassified."

## About the Author

Editor-in-Chief, Dark Reading

Kelly Jackson Higgins is the Editor-in-Chief of Dark Reading and VP, cybersecurity editorial at Informa TechTarget, where she leads editorial strategy for the company's three cybersecurity media brands: Dark Reading, SearchSecurity and Cybersecurity Dive. She is an award-winning veteran technology and business journalist with three decades of experience in reporting and editing for various technology and business publications and major media properties. Jackson Higgins was selected three consecutive times as one of the Top 10 Cybersecurity Journalists in the U.S., and was named as one of Folio's 2019 Top Women in Media. She has been with Dark Reading since its launch in 2006.