How A Cybersecurity Firm Uncovered The Massive Computer Hack

npr.org/2020/12/21/948843356/how-a-cybersecurity-firm-uncovered-the-massive-computer-hack

Greg Myre

National Security

Enlarge this image

Kevin Mandia, CEO of the cybersecurity firm FireEye, testifies before the Senate Intelligence Committee in 2017. Mandia's company was the first to sound the alarm about the massive hack of government agencies and private companies on Dec. 8. **Susan Walsh/AP hide caption**

toggle caption
Susan Walsh/AP

Kevin Mandia, CEO of the cybersecurity firm FireEye, testifies before the Senate Intelligence Committee in 2017. Mandia's company was the first to sound the alarm about the massive hack of government agencies and private companies on Dec. 8.

Susan Walsh/AP

The first word that hackers had carried out a highly sophisticated intrusion into U.S. computer networks came on Dec. 8, when the cybersecurity firm FireEye announced it had been breached and some of its most valuable tools had been stolen.

"We escalated very quickly from the moment I got the first briefing that, 'Hey, we have a security incident of some magnitude,' " FireEye CEO Kevin Mandia told *All Things Considered* co-host Mary Louise Kelly. "My gut was telling me it was something we needed to put people on right away."

Mandia was right. Within days, the scope of the hack began to emerge.

Multiple U.S. agencies were successfully targeted, including the departments of State, Treasury, Commerce, Energy and Homeland Security as well as the National Institutes of Health.

The hackers attached their malware to a software update from Austin, Texas-based company SolarWinds, which makes software used by many federal agencies and thousands of private companies to monitor their computer networks.

The SVR, Russia's foreign intelligence agency, is considered the most likely culprit, according to Secretary of State Mike Pompeo and some members of Congress who have been briefed by the U.S. intelligence community. But the Trump administration has not formally attributed blame.

"What I've seen is 2020 has been about the hardest year, period, to be an information security officer," Mandia said. "It's time this nation comes up with some doctrine on what we expect nations' rules of engagement to be, and what will our policy, or proportional response, be to folks who violate that doctrine. Because right now there's absolutely an escalation in cyberspace."

Here are excerpts from Mandia's interview:

What was that moment like when you're figuring out it's your cybersecurity company that has been hacked?

If you wrote down the reasons why another nation might want to compromise FireEye, you can come up with some reasons. What we do is we track attackers and quite frankly, we out them. We try to figure out — here's their fingerprints, let's share those fingerprints with everybody so they can't get away with what they're doing.

[Early on] there was enough operational security by the attacker that I knew it was professional. This wasn't the first rodeo for these attackers. In fact, they followed a tradecraft that the more I learned, the more this was a unit that's been operational for a decade or more. They knew what they were doing, they had novel techniques. So we knew we would have to do the full-court press on our investigation. And we did.

Who is behind this attack?

For me, it's definitely a nation. In regards to the supply chain compromise at SolarWinds, they did an innocuous addition of code in October 2019 inside the supply chain, saw that it was provisioned and deployed — so they knew that their techniques on offense to hack the supply chain were efficient and effective. They went live with actual malicious code inside of the SolarWinds in March through June of this year.

So this is somebody who is patient, professional, and what made this interesting to me is I felt they were more interested in staying surreptitious and clandestine than they were about accomplishing their mission.

What nations have this kind of capability?

Not a lot. It's very consistent with what Russia could do. There might be a group out of China that might be able to do it. And that's probably it.

Is there any signature to this attack that would be consistent with other hacks you've seen?

There's probably about six to eight technical details that made me realize this is a nation, and most likely a foreign intelligence service doing this breach. One of them is this: They used an infrastructure to attack FireEye. The IP addresses or systems they use to attack FireEye were not used in any other incident we're aware of.

In other words, the attackers set up an infrastructure to attack FireEye that was wholly unique to attacking FireEye. That takes a lot of maintenance. That takes a lot of coordination. That's an operation — not just a hack. Most threat groups, when they attack, will use shared infrastructure to attack many companies. This group does not do that. That in and of itself made me realize it was an operation.

What should we take from the fact that it was FireEye, a private cybersecurity firm, that alerted the U.S. government — and not the other way around?

We're all in this together, period. And there's different visibility at different places. When the attacks were happening against FireEye, all the IP addresses used to attack us [were] all inside the United States. And I'm pretty aware that the [National Security Agency] does not do collections within the United States. So we were the ones, kind of on our own, to be able to see this and detect it.

So you're saying you were able to see things that the NSA, despite all of its vast resources, have firewalls against being able to see, domestically?

Well, I wouldn't call it firewalls necessarily. It's just legal remit. You know, when you look at what these attackers do, they're attacking U.S. companies from the United States. That doesn't necessarily mean the attackers are sitting in the United States — but the infrastructure they're setting up to attack companies like FireEye are all in the United States. So the malicious intent may not be visible outside the United States and may only be visible inside.

We have thousands and thousands of computers that we inspected for evidence that they were compromised, and we couldn't get anything earlier in the time frame than a SolarWinds system. We sat there looking at the SolarWinds system saying, "We can't find anything bad on it right now, but it's our earliest evidence of compromise. Something's wrong."

So we then had to turn it over to our reverse engineers. This is something most companies can't do. We went through 14 gig of information, over 18,000 files in the update that we got from SolarWinds, over 4,000 executable files. We decompiled them into millions of lines. And then with real malware analysts, we found the needle in the haystack.

Do we know whether the NSA itself was hacked?

I don't have any idea.

So what now? There's a statement from the FBI and the director of national intelligence and the cybersecurity arm of Homeland Security that says this breach is ongoing.

I think as folks are being notified or learning that they're compromised, they're going to have a lot of work to do. All these organizations are both going to have to investigate what happened and figure out the scale and scope of it, and then they're going to have to eradicate the attackers from their network if they're still active.

Even if they're not active, you're going to flex your muscle a little bit to do a lot of remediation. That's going to take months.

But one thing that's definitely clear to me: The attackers have no idea what is the envelope of behavior, what are the rules of engagement.

We're a nation losing billions of dollars to ransomware. And we are a nation that just had potentially one of the most successful cyberespionage campaigns ever done on it.

- FireEye hack
- Russia