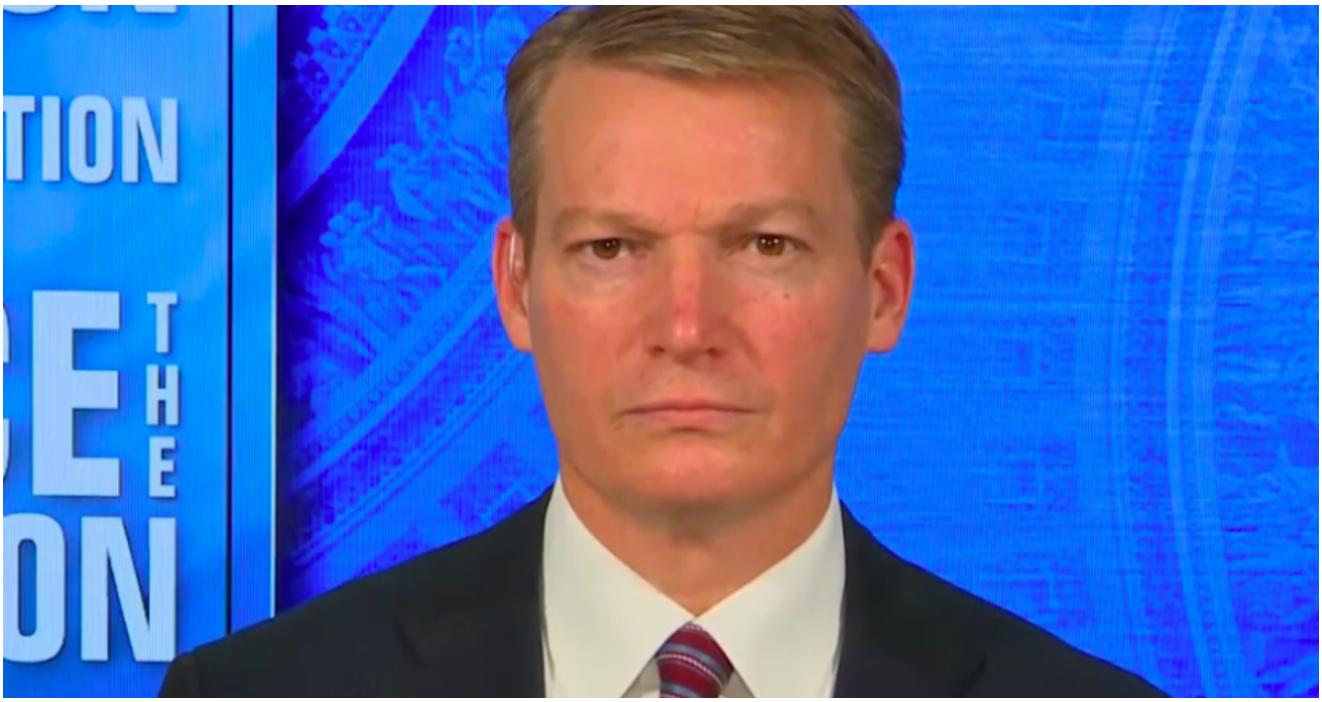
Transcript: Kevin Mandia on "Face the Nation," December 20, 2020

cbsnews.com/news/transcript-kevin-mandia-on-face-the-nation-december-20-2020/



FireEye CEO: Hack was "totally unique," "utterly clandestine"

FireEye CEO says massive hack was "totally unique" and "utterly clandestine" 06:49

The following is a transcript of an interview with Kevin Mandia, FireEye CEO, that aired Sunday, December 20, 2020, on "Face the Nation."

MARGARET BRENNAN: And we are learning more about what may be the worst cyber attack in history. It's affected many organizations, including federal agencies. Kevin Mandia is the CEO of FireEye, a cybersecurity company that protects clients against malicious software and investigates hacks. His company was the first one to discover that this massive breach happened. Good morning to you.

FIREEYE CHIEF EXECUTIVE OFFICER KEVIN MANDIA: MARGARET, good morning to you.

MARGARET BRENNAN: The Trump administration has described this as an ongoing attack and poses grave risk to the federal government, to state governments, to private institutions, critical infrastructure. It went undetected for nearly nine months. How should the public understand this? How significant is it?

MANDIA: Right, well, there's a lot of ways to look at this intrusion, and first and foremost, it's different than other ones that we commonly respond to. We respond to over a thousand breaches a year. And what separates this is who did it, how they did it and what they did when they got in. And I'll get to the who probably last. But when you look at the how, MARGARET, that's what makes this totally unique. This was not a drive by shooting on the information highway. This was a sniper round from somebody a mile away from your house. This was special operations. And it was going to take special operations to detect this breach. So, the how they did it was in a way that was utterly clandestine, very difficult to tell. And quite frankly, it was a backdoor into the American supply chain that separates this from thousands of other cases that we've worked throughout our careers.

MARGARET BRENNAN: Does it go back further than March? How long have hackers been inside the system?

MANDIA: Well, so right now, what we've observed with this latest campaign, first, I think this threat actor wasn't a one and done. What I mean by that is I think these are folks that we've responded to in the '90s, in the early 2000s. It's a continuing game in cyberspace. You know, there's a time in our lives where the domains that we had espionage in or the domains that we had combat in or differences in were land, sea, air, then space. And now we have cyber. This is just one campaign in a long battle in cyberspace. But this campaign specifically has the earliest evidences of being designed. In October of 2019 when code was changed in the SolarWinds Orion platform, but it was innocuous code. It was not a backdoor. Then sometime in March, the operators behind this attack did put malicious code into the supply chain, injected it in there and that is the- the backdoor that impacted everybody. I think, MARGARET, it's important to note everybody says this is potentially the biggest intrusion in our history. The reality is the blast radius for this, I kind of explain it with a funnel. It's true that over 300,000 companies use SolarWinds, but you come down from that total number down to about 18,000 or so companies that actually had--

MARGARET BRENNAN: Yeah.

MANDIA: --the backdoor or malicious code in a network. And then you come down to the next part. It's probably only about 50 organizations or companies, somewhere in that zone--

MARGARET BRENNAN: Right.

MANDIA: --that's genuinely impacted by the threat actor.

MARGARET BRENNAN: I want to come back to that in a moment, but attribution. Secretary of state said it's Russia.

MANDIA: Sure.

MARGARET BRENNAN: A Republican senator who heads the Senate Intelligence Committee said it's increasingly clear that this was Russian intelligence. Do you agree that this was Russia? And what evidence do you base that on?

MANDIA: Well, I think that is definitely a nation behind this. You just heard me say the attack started with a dry run in October of 2019. This wasn't a ransomware attack, not a drive by shooting where somebody breaks in--

MARGARET BRENNAN: Right.

MANDIA: --and it's kind of like a brick through your window. And it's pretty obvious, hey, they broke in with a brick through the window and then they stole your jewels. This is more like a case where somebody came in through a trapdoor in your basement that you never knew about, put on an invisibility cloak and you just got the sense there in your networks, but you weren't even sure how. You were like, there's something different--

MARGARET BRENNAN: Right.

MANDIA: --right now. Something's been moved. And it took--

MARGARET BRENNAN: But you know better than anyone--

MANDIA: Yeah.

MARGARET BRRENNAN: --that there are only a very few number of nation states capable of what you are describing in terms of skill. Russian intelligence--

MANDIA: Right.

MARGARET BRENNAN: --specifically the SVR, has repeatedly been pointed to by officials. Is that who you believe did this right?

MANDIA: Right. I think this is an attack very consistent with that, I also believe this, we're going to get attribution right. The amount of resources inside the government, inside the private sector and the reach that we have, we can speculate it or we can do some more work and put a neon sign on the building of the folks that did this. And I'm very confident as we continue the investigation, as it gets broader, as more people learn the tools, tactics and procedures of this attack, we're going to bring it back and we're going to get attribution.

MARGARET BRENNAN: Yeah.

MANDIA: Not 92% right, not consistent with, but 100%. Let's just get it right--

MARGARET BRENNAN: Right.

MANDIA: --so that we can proportionately respond, period.

MARGARET BRENNAN: Right. And- and it may take time to do that. But, I- I press you on attribution because obviously, if- if you want to stop it from happening again, you actually have to identify who did it in the first place. And the president kind of muddied those--

MANDIA: Right, absolutely.

MARGARET BRENNAN: --muddied those waters yesterday when he said it may be China, the media's overplaying it, downplayed the idea it was Russia. I'm not asking you to weigh in on politics, but how do you stop this from happening again and was it--

MANDIA: Right. Well, clearly--

MARGARET BRENNAN: Do you have to specifically target one country? How do you do this?

MANDIA: Well, I think you have doctrine. That's why we have doctrine for things like the use of chemical weapons. You saw what happened when somebody used chemical weapons in Syria. There was retaliation. Folks have to know the rules of the game. And the problem in cyber is we're not doing the work to come up with the doctrine. If you publish your doctrine- we're uniquely vulnerable in cyberspace. We're the ones in the glass house. These attacks will continue to escalate, and get worse if we do nothing. So, you know, just as a cybersecurity professional, I recognize if you don't communicate the rules of the game, here's the doctrine and here's the penalty when you violate it. We're going to see the borders continue to be pushed outward in cyber attacks to the point where, when do we finally do the work--

MARGARET BRENNAN: Yeah.

MANDIA: --when it's already intolerable, when it already got so bad that we have no choice but to respond.

MARGARET BRENNAN: Right.

MANDIA: But like you said, it starts with doctrine. With doctrine, you have to get attribution right.

MARGARET BRENNAN: Yeah.

MANDIA: And with attribution, then you have to do a proportional response to whoever the actors were.

MARGARET BRENNAN: All right. Kevin Mandia, thank you very much for your insight. We'll be back in a moment with a look at the economy.

Thanks for reading CBS NEWS.

Create your free account or log in
for more features.

Please enter email address to continue

Please enter valid email address to continue