What you need to know about the FireEye hack: Cybersecurity attack against US government

usatoday.com/story/tech/2020/12/14/fireeye-solarwinds-hack-breach-cybersecurity-attack/6538645002

TECH

A devastating cybersecurity attack targeting major branches of the U.S. government has put an untold number of Americans, agencies and government secrets at risk of compromise.

The attackers, which may have been tied to the Russian government, penetrated federal computer systems through a popular piece of server software offered through a company called SolarWinds.

The threat apparently came from the same cyberespionage campaign that has afflicted cybersecurity firm FireEye, foreign governments and major corporations, and the FBI was investigating.

The system is used by hundreds of thousands of organizations globally, including most Fortune 500 companies and multiple U.S. federal agencies, which will now be scrambling to patch up their networks.

The attackers planted malware in computer networks after using what FireEye CEO Kevin Mandia called “a novel combination of techniques not witnessed by us or our partners in the past.”

The sophisticated attack breached the Treasury and Commerce departments and potentially other agencies. The Commerce Department said in a statement that it asked the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency and the FBI to investigate.

The Department of Homeland Security is also reviewing a possible breach at the agency, spokesman Alexei Woltornist said Monday.

Cyber attack under investigation: When a top cybersecurity firm gets hacked, what is the takeaway for the average netizen?

US government agencies hacked: Russia a possible culprit

But the full extent of the damage is not yet clear.

“Think of it like a health virus that manages to get into your body,” said Mathieu Gorge, a cybersecurity expert and author of the forthcoming book “The Cyber Elephant in the Boardroom.” “Once it’s in your body, it multiplies, using all of the organs and all of the arteries and all the liquids in your body. Everything is interconnected.”

Here’s what you need to know so far.

What information was potentially taken?

It’s too early to say since the attack was only recently discovered but appears to have exploited what SolarWinds called a “potential vulnerability” related to updates released between March and June for Orion, which helps monitor networks for problems.

But early indications suggest the attackers were seeking information on American hacking capabilities and defenses. Call it the latest phase in what could be a cyber-era cold war.

“It appears the attackers may have taken our own tools for finding vulnerabilities in foreign networks,” said Matthew Schmidt, a professor in the national security department of the University of New Haven’s Henry C. Lee College of Criminal Justice and Forensic Sciences. “They hacked our hacking capability. It's very early, but the level of immediate reaction suggests a very, very serious intrusion.”

National Security Council spokesman John Ullyot said authorities are working with cyber units at DHS and FBI to "coordinate a swift and effective, whole-of-government recovery and response to the recent compromise."

Could your personal information be at risk?

Yes. The federal agencies targeted in the attack have a storehouse of personal information about Americans, of course. But comprehensive details on the motivations of the attackers remain unclear.

“The initial sense is that the attack left the updating system for many key security systems open to exploitation, meaning it's possible they could have attained root access to many agency's systems,” Schmidt said in an email interview. “If that's true, and we don't know yet, it could mean the most important systems are compromised – personnel data, including foreign agents, planning, operations, etc. If anything near the worst is true, it will mean months of work to determine whether it's safe to use these systems.”

What can you do to protect yourself?

Americans, just like the agencies targeted in the attack, should take a consistent approach to protecting themselves.

Use complex and different passwords for your digital accounts. Monitor your finances closely. Use two-factor authentication for critical accounts like email and social media. Don’t click on links from any source that you haven’t authenticated as legitimate.

“People need to change any passwords they've used on (U.S. government) sites like Social Security, IRS, Small Business Administration,” Schmidt said.

Unfortunately, there may be little people can do to protect themselves when the governments, companies and organizations that have their personal information fall prey to attacks.

“The challenge is that the criminals only need to get it right once, whereas the government and companies need to get right all the time,” Gorge said.

Gorge urged Americans to look out for notifications from government agencies or corporations that their information has been compromised. In many previous cyber breaches, affected consumers are offered identity theft monitoring services for free.

What does the government need to do?

The government's first focus should be on ousting the intruders, Gorge said.

"You need to be in the mode that allows you to contain the hack as much as possible as you investigate," he said.

The attackers likely breached other agencies or organizations in addition to those already identified, which simply makes it more urgent to root out the infiltrators. FireEye's Mandia said the attacks appears to have started in the spring.

"This might be a domino effect," Gorge said. "It's a coordinated attack. It's a sophisticated attack and I don't think we've seen the end of it."

The government is organizing its response to the intrusion without its top cybersecurity protection official. Last month, President Donald Trump fired Christopher Krebs, director of DHS' CISA, after he declared that the election was the most secure in American history.

Was this inevitable?

When it comes to cybersecurity attacks, there's a degree of inevitability in the air, despite everyone's best attempts to protect themselves – particularly when a motivated and sophisticated nation-state poses a threat.

"There's a saying in the industry that there are only two types of companies – those that have been breached and those that don't know they've been breached," Gorge said. "Everybody has security incidents. How they deal with the breach will decide whether the public trusts them or not."

Ilia Sotnikov, vice president of product management at cybersecurity software provider Netwrix, said companies' cybersecurity teams should "immediately take advantage of countermeasures offered by FireEye" and be on the alert for additional security updates.

"This attack is another evidence that a motivated hacker will be able to compromise any organization, no matter how well it is protected," Sotnikov said. "Our new normal right now is to be open about a data breach and own the message as FireEye did."

Gorge agreed that FireEye has taken the right steps by providing regular updates to the public and is widely respected in the cybersecurity industry.

“FireEye extremely good at what they’re doing and they are pioneers,” he said. “They are ahead of the pack.”

Contributing: Mike Snider, and Associated Press

Follow USA TODAY reporter Nathan Bomey on Twitter @ NathanBomey.