***<https://www.wsj.com/amp/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402>***

**SolarWinds Hack Victims: From Tech Companies to a Hospital and University**

A Wall Street Journal analysis identified at least 24 organizations that installed software laced with malicious code by Russian hackers

**SolarWinds said it traced activity from the hackers back to at least October 2019.**

**Kevin Poulsen , Robert McMillan and Dustin Vol, *WSJ*, Dec. 21, 2020**

The suspected Russian hackers behind breaches at U.S. government agencies **also gained access to major U.S. technology and accounting companies, at least one hospital and a university**, a Wall Street Journal analysis of internet records found.

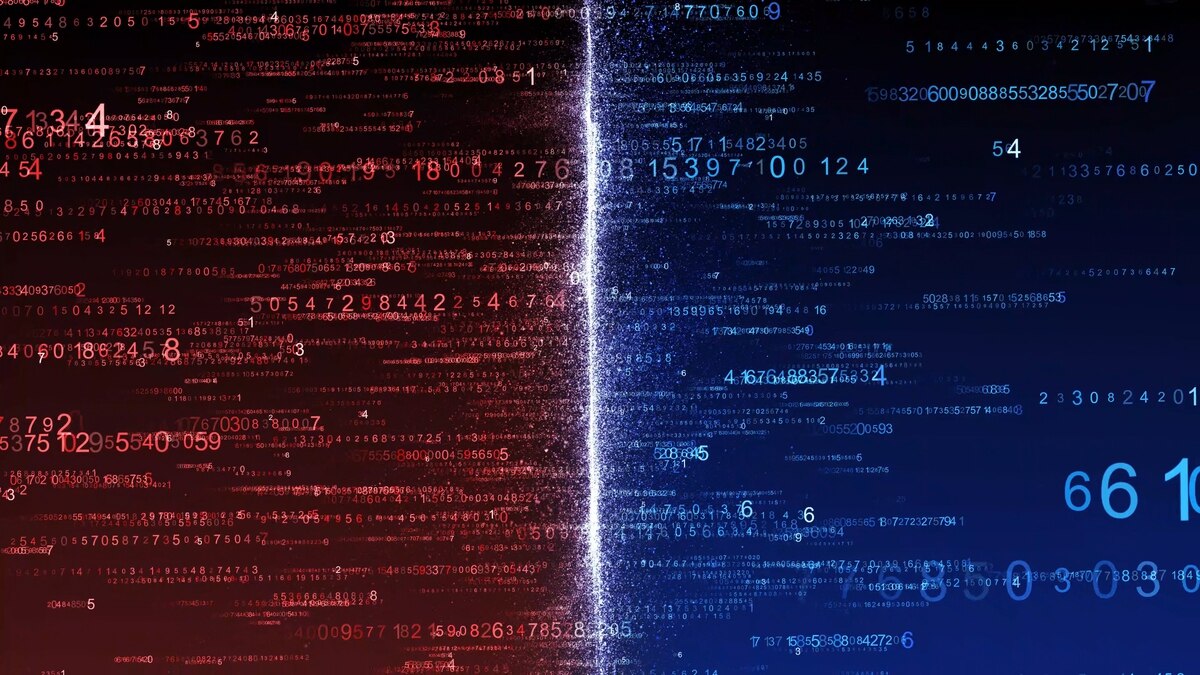
The Journal identified infected computers at two dozen organizations that installed tainted network monitoring software called SolarWinds Orion that allowed the hackers in via a covertly inserted backdoor. **It gave them potential access to much sensitive corporate and personal data.**

=======================================================

[***https://www.c4isrnet.com/battlefield-tech/it-networks/2020/12/27/very-difficult-to-defend-what-happens-if-hackers-are-inside-the-pentagons-networks/***](https://www.c4isrnet.com/battlefield-tech/it-networks/2020/12/27/very-difficult-to-defend-what-happens-if-hackers-are-inside-the-pentagons-networks/)

**‘Very difficult to defend’: What happens if hackers are inside the Pentagon’s networks?**

**Andrew Eversden , Joe Gould , and Mark Pomerleau, C4ISRNET, December 24, 2020**

**The U.S. Department of Defense faces a tough challenge assessing its networks after suspected Russian hackers may have had access for months. (Aislan13/Getty Images**)

**WASHINGTON** — If Russian hackers suspected of a vast cybersecurity breach slipped into the Pentagon or military’s computer systems, the strength of protective network blockades is key to keeping them from burrowing in to try to access increasing amounts of information.

Those protections — in the form of secure network connections — have to stand up to meddling to keep hackers from hopping from network to network to potentially reach sensitive communications or even weapon systems, where they could steal or alter data or cause damage, experts say. However, observers point out that this breach appears so far to be a classic espionage campaign, though with some of the most sophisticated methods seen yet.

“We certainly have a high degree of activity around that right now,” Navy CIO Aaron Weis told C4ISRNET. “We have teams who have acted upon the direct orders from Cyber Command and have executed those things. We continue to engage around that. There are internal meetings that are ongoing where we’re ensuring that we’ve put the right things in place. Absolutely it’s got our full attention.”

**Overall, the Pentagon has been largely silent about the breach publicly as it works through the** [**long process to assess fallout from the intrusion**](https://www.c4isrnet.com/cyber/2020/12/17/its-going-to-take-a-lot-of-digging-the-pentagons-long-search-to-see-if-anyones-hiding-in-its-networks/)**, saying early on that no breach had been detected yet, despite media reports that said the agency was among government offices compromised through widely used software from SolarWinds, a network management company.**

President-elect Joe Biden has criticized the Pentagon for not briefing him and his transition team fully, challenging President Donald Trump’s assertion that the situation is under control. The Pentagon disputed the idea that it is withholding information from Biden, saying briefings will continue in early January after a break over the holidays.

**According to cybersecurity company FireEye, which uncovered the breach, the access that hackers achieved has allowed the malicious actor to move further into computer networks.**

Several former government cybersecurity officials told C4ISRNET that lateral movement allowing the suspected Russian hackers to dig deeper posed a worst-case scenario with a myriad of possible outcomes spiraling from there. The challenge is that the DoD’s web of systems includes legacy and modernized networks that connect to weapons systems and control systems.

**“If an adversary had gotten in and moved laterally, then all the network connection points — any place you have connections between networks and those trust relationships — that becomes very difficult to defend,” said retired Rear Adm. Danelle Barrett, former deputy Navy CIO and cybersecurity division director.**

**Know all the coolest acronyms**

Sign up for the C4ISRNET newsletter about future battlefield technologies.

Top of Form

Bottom of Form

Top of Form

Bottom of Form

“Wherever you have those trust relationships, you have to always be really careful about what is going on back and forth across that tunnel,” Barrett said.

There are potentially two worst-case dimensions to this situation, said Jan Tighe, former commander of 10th Fleet/Fleet Cyber Command and deputy chief of naval operations for information warfare.

First, cyber threat hunters must find out whether the intruder persists on the network. Job No. 1 for response teams is to cut off any existing access the trespassers might have, Tighe said. If the intrusion was an espionage campaign, DoD will have to do a damage assessment of what information was affected. If the agency can’t be sure what data and communications were accessed, leaders have to make assumptions about what the hackers may have reached, she said.

**The second, more troubling question is whether hackers altered data in any way, which Tighe said could be more problematic than destroying data.**

“You have data, but you don’t know if it’s really the right data in your network. Depending on what aspect of the DoD you’re in, that could be very damaging,” she explained.

Once inside, the access would depend on what system the malicious code went to through updates to the SolarWinds software. For example, an upload to an agency’s central administration systems could be damaging, allowing access to information such as user logs and system locations, said Frank Downs, former NSA analyst and director of proactive services at cybersecurity firm BlueVoyant.

If the actor entered into a central network through the SolarWinds vulnerability and found lax security on connected systems, that could cause serious problems for the department.

“It all depends on what’s on the network and the permissions on the network, but they could hop from one node to another node to another node,” Downs said. “If you have security in depth, the chances are a lot lower that they’ll be able to get much greater access, but if you are just sitting on a perimeter baseline, it’s not looking good.”

If those systems administrator privileges are vulnerable, experts said accounts could be manipulated and privileges elevated to continually allow increased access.

“They’re going get in and build all sorts of backdoors that you’re not going to be able to figure out,” Barrett said. “They’re going to be able to manipulate accounts and do things and hide their tracks**. You’re not going to catch them, and they’re probably still there now.”**

Communication is likely disrupted during a survey of potential network damage. Specifically, officials shouldn’t send and receive emails on the network if investigators are searching for potential compromises, Tighe said, noting that one of the first things the Cybersecurity and Infrastructure Security Agency did was tell agencies to have a different way of communicating as they coordinate the response.

There’s also more risk through [the software supply chain](https://www.c4isrnet.com/2020/12/23/wide-reaching-hack-has-defense-firms-on-their-toes/). Another concerning scenario is if the attackers find their way into an update for a hacked company’s software, infecting still more users through those software products or even the firmware on chips or other hardware, said Greg Conti, founder at cybersecurity firm Kopidion and former chief of the U.S. Army Cyber Institute.

“This could have second, third or fourth order effects as it propagates that we’ll never know,” said Conti. “This thing could attack, spread outward, companies could remediate, and then it could loop back in through another product that was compromised.”

Authorities believe that hackers had extensive access to some government or business networks for as long as nine months. With that time, could the hackers have figured out how to jump the air gap meant to block computer system users from accessing classified systems?

“I’m speculating, but people have done amazing things where they turn a RAM in a computer into a radio transmitter [to bridge into air-gapped networks],” Conti said. “There are hundreds of counterintuitive and crazy things people have done. This is a huge thing, and there’s a nonzero chance the attackers pulled out their super-secret best capability.”

Agencies could face another problem if they use the same credentials for users on unclassified and classified portions of network, allowing hackers to steal unclassified credentials and migrate to more protected areas, Tighe pointed out. While administrators work to have different credentials for each, rare cases where they are the same are worrying.

In another scenario, subtle, hard-to-detect data manipulations could be introduced into the software of a weapon system so that it malfunctions.

However, Jamil Jaffer, founder and executive director of the National Security Institute at George Mason University, cautioned that there is no evidence that the Russians have taken that step, and it is unlikely because of the strong reaction it would likely provoke. He also noted that if the Russians were to even threaten such action, that would raise concerns.

“I’m not sure they’d even want to do that, because I think they realize if we found out they’d engaged in data manipulation or destruction, they’d be crossing a red line that would provoke a stiff response, but they might try to hold us at risk, and if they do, that’s a major problem also and might force us to get more aggressive sooner,” Jaffer said.

===================================

**U.S. cyber agency says SolarWinds hackers are 'impacting' state, local governments**

**By** [**Raphael Satter**](https://www.reuters.com/journalists/raphael-satter)**., *Reuters,* December 2020**

**WASHINGTON (Reuters)** - The U.S. cybersecurity agency said on Wednesday that a sprawling cyber espionage campaign made public earlier this month is affecting state and local governments, although it released few additional details.

The hacking campaign, which used U.S. tech company SolarWinds as a springboard to penetrate federal government networks**, was “impacting enterprise networks across federal, state, and local governments, as well as critical infrastructure entities and other private sector organizations,”** the Cybersecurity and Infrastructure Security Agency (CISA) said in a statement posted to its website.

The CISA said last week that U.S. government agencies, critical infrastructure entities, and private groups were among those affected, but did not specifically mention state or local bodies. So far only a handful of federal government agencies have officially confirmed having been affected, including the U.S. Treasury Department, the Commerce Department, and the Department of Energy.

CISA did not identify the state or local agencies affected and did not immediately return an email seeking additional detail on the notice.

Reuters has previously reported that Pima County, Arizona was among the victims of the wave of intrusions.

The county did not immediately return a message seeking comment late Wednesday. The county’s chief information officer previously told Reuters his team had taken its SolarWinds software offline immediately after the hack became public and that investigators had not found any evidence of a further compromise.

Senior U.S. officials and lawmakers have alleged that Russia is to blame for the hacking spree, a charge the Kremlin denies.

Reporting by Raphael Satter; Editing by Christian Schmollinger and Raju Gopalakrishnan

===========================================

**Danger from Russian hack may persist and spread, experts say**

**By: Gopal Ratnam for THE HILL // 23 December 2020**

The widespread breach of SolarWinds, the network management software company that supplies so many U.S. government agencies and Fortune 500 companies, likely allowed Russian hackers to access the top echelons of those institutions and cannot simply be dismissed as routine espionage by a strategic rival, former cybersecurity officials said this week.

 Moreover, they warned that the attackers may be burrowed deep into government and corporate networks and from there could launch other damaging attacks at a time of their choosing.  The cybersecurity experts who served in the George W. Bush and Obama administrations said that the attackers, who breached the SolarWinds operating software to gain access to the company’s clients between March and June, by now may have used that access to slip deeper into the networks, making it harder to find them.

President-elect Joe Biden on Tuesday said the cyberattack, likely launched by the Russian intelligence service known as SVR, happened “on Donald Trump’s watch, when he wasn’t watching.” **Biden said the attack “constitutes a grave risk to our national security.** It was carefully planned and carefully orchestrated.” Although most knowledgeable observers say the attack was likely carried out by Russia, President Donald Trump has tweeted that it could have been carried out by China or others, contradicting statements by Secretary of State Mike Pompeo and outgoing Attorney General William Barr, both of whom have said the attack was likely carried out by Moscow.

The attack has exposed 18,000 SolarWinds clients after they downloaded and installed a tainted software update that was infected with malware. The breach wasn’t discovered until cybersecurity research firm FireEye, which was attacked separately, revealed the SolarWinds breach this month.  Federal departments such as Commerce, Treasury, Energy, and Homeland Security have been exposed, as well as large corporations like Microsoft, Ford Motor Co. and others.

On Monday, Oregon Sen. [Ron Wyden](https://www.rollcall.com/members/406?utm_source=memberLinks&utm_medium=memberlinks&personid=406), the top Democrat on the Senate Finance Committee, said the Treasury Department “suffered a serious breach, beginning in July, the full depth of which isn’t known,” based on briefings the committee received from the agency, and contradicting Treasury Secretary Steven Mnuchin, who earlier said the breach was “under control.”  Wyden said the hackers had broken into systems that are home to the department’s highest-ranking officials and that the agency remained in the dark about “all of the actions taken by the hackers, or precisely what information was stolen.”

**Attack not over**

The attackers “still have the ability in the networks in which they have maintained some persistent control to do the proverbial bomb drop, if they really wanted to go that route,” said Tom Bossert, who was a White House adviser for homeland security and cybersecurity in the Trump administration until April 2018.  The attackers also could use information they have gleaned from their presence in government and corporate networks to “conduct a misinformation or disinformation campaign” in the coming months and even years, Bossert said.

Bossert appeared on a panel discussion with Michael Daniel, the Obama administration cybersecurity adviser; Melissa Hathaway, who advised Presidents Barack Obama and George W. Bush on cyber matters; and Chris Inglis, the former deputy director of the National Security Agency. The event was organized by the McCrary Institute for Cyber and Critical Infrastructure Security at Auburn University.

Unlike the Japanese attack on Pearl Harbor or al-Qaida’s attack on 9/11, it’s likely that the wide-open breach that has allowed Russian hackers to hide inside government networks could enable Moscow to spread out its attack in a diffused manner “over time and space,” Inglis said.  The U.S. government must shift its approach to cybersecurity from “detect and react strategy” after each major attack, because “it’s a fool’s errand,” Inglis said. “We appear to be defending technology as opposed to the operations that are dependent upon that technology.”

Hathaway said a handful of private companies with weak security systems have exposed thousands of others and the U.S. government to risk. In addition to SolarWinds, “Microsoft is part of this problem,” she said, because the company’s Office 365 and cloud services enabled the attack.  The exposure means that “we will have lost trust in all of these enterprises,” Hathaway said, adding that the path of attack could also leave the country’s energy and utilities infrastructure — electricity, gas, water — vulnerable.

**Paying a price**

The experts said Russia must pay a price for its indiscriminate breaching of U.S. government networks.  The attack in its “scope and scale is clearly unacceptable,” Inglis said. “It’s brazen, it’s impactful, and it’s indiscriminate.”  The American response cannot simply be a computer network attack or a physical attack by armed forces, which are “not completely appropriate,” but the U.S. government must craft an adequate response, Inglis said.

Hathaway and Daniel said the response could be a series of steps ranging from economic sanctions, an oil embargo or moves expelling Russian diplomats, and working with U.S. allies to step up pressure steadily on Moscow.  Those steps executed in a sequence could also deter and forestall any long-term damage Moscow might be contemplating from the network access its spies have gained, Hathaway and Daniel said.

==========================================

**Energy Department says it was hacked in suspected Russian campaign**

The massive breach has left the U.S. government scrambling to find out what was infected and how much information was stolen.

The Energy Department was hacked as part of a massive, ongoing campaign against the U.S. government, a spokesperson said Thursday, making it the latest confirmed agency to have been breached by Russian spies.

A number of federal agencies have been hit by a massive monthslong breach, which officials believe is the work of Russian intelligence, leaving the government scrambling to find out what was infected and how much information was stolen.

"The investigation is ongoing and the response to this incident is happening in real time," Energy Department spokeswoman Shaylyn Hynes said in a statement.

"At this point, the investigation has found that the malware has been isolated to business networks only, and has not impacted the mission essential national security functions of the Department, including the National Nuclear Security Administration," she said.

Much of the campaign came after the hacking of SolarWinds, an Austin, Texas-based company that counts many government agencies and a number of major U.S. companies as customers. The hackers planted malicious code into software updates, which bypassed the federal cybersecurity scans.

The campaign, which is believed to have started in early March at the latest, was made public Dec. 8 when the cybersecurity company FireEye, which also does work for federal agencies, [said it had been hacked](https://www.nbcnews.com/tech/security/fireeye-top-u-s-cybersecurity-company-says-it-was-hacked-n1250449). On Sunday, the U.S. Cybersecurity and Infrastructure Security Agency, or CISA, released [an emergency directive](https://cyber.dhs.gov/ed/21-01/) to uninstall the compromised version of SolarWinds' software.

CISA notified the Energy Department on Sunday and immediately disconnected its systems, said a federal official with knowledge of the situation. Teams are now working round the clock to assess what, if anything, was exfiltrated, which may take weeks.

It was "one of the most sophisticated hacks" they have ever seen, said the official, who said the fact that the government learned of the breach only after a private company was hacked and after it had been going on for months was "truly breathtaking."

Hynes said in the department's statement that "immediate action was taken to mitigate the risk, and all software identified as being vulnerable to this attack was disconnected from the DOE network."

Only one other federal agency, the Commerce Department, has formally acknowledged that it was hacked as part of the SolarWinds campaign, but a number of other agencies, including the [Homeland Security](https://www.reuters.com/article/global-cyber/u-s-homeland-security-thousands-of-businesses-scramble-after-suspected-russian-hack-idUSKBN28O1Z3) and [Treasury](https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html) departments, are reported to have also been breached.

On Wednesday, a [joint statement](https://www.cisa.gov/news/2020/12/16/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure) from CISA, the FBI and the office of the director of national intelligence said the campaign was "significant and ongoing."

===============================================

[**POLITICO**](https://www.politico.com/)

**Nuclear weapons agency breached amid massive cyber onslaught**

**By** [**NATASHA BERTRAND**](https://www.politico.com/staff/natasha-bertrand) **and** [**ERIC WOLFF**](https://www.politico.com/staff/eric-wolff)**, 12/17/2020 03:29 PM EST**

**The Energy Department and National Nuclear Security Administration, (NNSA)which maintains the U.S. nuclear weapons stockpile, have evidence that hackers accessed their networks as part of an extensive espionage operation that has affected at least half a dozen federal agencies, officials directly familiar with the matter said.**

On Thursday, DOE and NNSA officials began coordinating notifications about the breach to their congressional oversight bodies after being briefed by Rocky Campione, the chief information officer at DOE.

**They found suspicious activity in networks belonging to the Federal Energy Regulatory Commission (FERC), Sandia and Los Alamos national laboratories in New Mexico and Washington, the Office of Secure Transportation at NNSA, and the Richland Field Office of the DOE.**

**The hackers have been able to do more damage at FERC than the other agencies, and officials there have evidence of highly malicious activity, the officials said, but did not elaborate.**

The officials said that the Cybersecurity and Infrastructure Security Agency, which has been helping to manage the federal response to the broad hacking campaign, indicated to FERC this week that CISA was overwhelmed and might not be able to allocate the necessary resources to respond. DOE will therefore be allocating extra resources to FERC to help investigate the hack, even though FERC is a semi-autonomous agency, the officials said.

Several top officials from CISA, including its former director Christopher Krebs, have either been pushed out by the Trump administration or resigned in recent weeks.

Federal investigators have been combing through networks in recent days to determine what hackers had been able to access and/or steal, and officials at DOE still don’t know whether the attackers were able to access anything, the people said, noting that the investigation is ongoing and they may not know the full extent of the damage “for weeks.”

Shaylyn Hynes, a DOE spokesperson, said that an ongoing investigation into the hack has found that the perpetrators did not get into critical defense systems.

"At this point, the investigation has found that the malware has been isolated to business networks only, and has not impacted the mission essential national security functions of the department, including the National Nuclear Security Administration," Hynes said in a statement. "When DOE identified vulnerable software, immediate action was taken to mitigate the risk, and all software identified as being vulnerable to this attack was disconnected from the DOE network.”

**The attack on DOE is the clearest sign yet that the hackers were able to access the networks belonging to a core part of the U.S. national security enterprise.** The hackers are believed to have gained access to the federal agencies’ networks by compromising the software company SolarWinds, which sells IT management products to hundreds of government and private-sector clients.

DOE officials were planning on Thursday to notify the House and Senate Energy committees, House and Senate Energy and Water Development subcommittees, House and Senate Armed Services committees, and the New Mexico and Washington State delegations of the breach, the officials said.

CISA, the FBI and the Office of the Director of National Intelligence acknowledged the “ongoing” cybersecurity campaign [in a joint statement](https://www.cisa.gov/news/2020/12/16/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure) released on Wednesday, saying that they had only become aware of the incident in recent days.

“This is a developing situation, and while we continue to work to understand the full extent of this campaign, we know this compromise has affected networks within the federal government,” the statement read. The U.S. government has not blamed any particular actor for the hacks yet, but cybersecurity experts have said the activity bears the hallmarks of Russia’s intelligence services.

**NNSA is responsible for managing the nation's nuclear weapons,** and while it gets the least attention, it takes up the vast majority of DOE's budget. Similarly, the Sandia and Los Alamos National Labs conduct atomic research related to both civil nuclear power and nuclear weapons. The Office of Secure Transportation is tasked with moving enriched uranium and other materials critical for maintaining the nuclear stockpile.

Hackers may have been casting too wide a net when they targeted DOE's Richland Field Office, whose primary responsibility is overseeing the cleanup of the Hanford nuclear waste site in Washington state. During World War II and the Cold War, the U.S. produced two- thirds of its plutonium there, but the site hasn't been active since 1971.

The attack on the Federal Energy Regulatory Commission may have been an effort to disrupt the nation's bulk electric grid. FERC doesn't directly manage any power flows, but it does store sensitive data on the grid that could be used to identify the most disruptive locations for future attacks.

=================================

**Massive data breach may have been discovered due to 'unforced error' by suspected Russian hackers**

**By** [**Zachary Cohen**](https://www.cnn.com/profiles/zachary-cohen-profile) **and** [**Jeremy Herb**](https://www.cnn.com/profiles/jeremy-herb)**, *CNN*, Wed December 23, 2020**

*(****CNN****)* US officials and private sector experts investigating the [massive data breach](https://www.cnn.com/2020/12/18/politics/us-government-hack-early-signs/index.html) that has rocked Washington increasingly believe the attackers were ultimately discovered because they took a more aggressive "calculated risk" that led to a possible "unforced error" as they tried to expand their access within the network they had penetrated months earlier without detection, according to a US official and two sources familiar with the situation.

Investigators still haven't confirmed the motives of the attackers as they work both to uncover the full scope of the attack and assign blame for the campaign that impacted at least half a dozen government agencies and potentially hundreds of private companies. The incursion was first uncovered by the cybersecurity firm FireEye after its own network was breached.

FireEye was tipped off to the hackers' presence when they attempt to move laterally within the firm's network, according to the sources, a move that suggested the hackers were targeting sensitive data beyond emails addresses or business records. Whether that exposure was the result of a mistake by the attackers or because they took a calculated risk remains unclear, the sources said.

"At some point, you have to risk some level of exposure when you're going laterally to get after the things that you really want to get. And you're going to take calculated risks as an attacker," one source familiar with the investigation said.

**Multiple entry points**

Last week, FireEye acknowledged in a statement that the breach "occurred when the hackers, who already had an employee's credentials, used those to register their own device to FireEye's multi-factor authentication system so they could receive the employee's unique access codes."

FireEye has declined to provide additional details about how the hackers were ultimately discovered after evading detection for months, citing an ongoing investigation into the matter. The Cybersecurity and Infrastructure Security Agency also declined to comment. US officials and experts warn the hackers used multiple entry points to breach these networks, some of which have not yet been identified.

Now, the hackers are attempting to salvage what access they can as the US government and private sector are "burning it all down," sources said, referring to their complete overhaul of networks, which will force the attackers to find new ways of getting the information they seek.

Meanwhile, US officials continue to grapple with the fallout and assess just how successful the operation was, the US official said, noting that it is clear the nation-state responsible invested significant time and resources into the effort.

[[](https://www.cnn.com/2020/12/21/politics/treasury-solarwinds-hack-ron-wyden/index.html)](https://www.cnn.com/2020/12/21/politics/treasury-solarwinds-hack-ron-wyden/index.html)

[**Treasury Department email accounts compromised in suspected Russian hack, top Senate Democrat says**](https://www.cnn.com/2020/12/21/politics/treasury-solarwinds-hack-ron-wyden/index.html)

While the scope of the hacking campaign remains unclear, government agencies that have disclosed they were impacted have said there is no evidence to date that classified data was compromised.

But the way the hackers were discovered suggests the operation was intended to steal sensitive information beyond what was available on unclassified networks and sought to establish long-standing access to various targeted networks, the sources said.

The fact that FireEye -- not the federal government -- discovered the breach has also raised questions about why the attack went undetected at US government agencies.

[Speaking to reporters](https://www.cnn.com/2020/12/22/politics/biden-key-lines-christmas-address/index.html) Tuesday, President-elect Joe Biden knocked President Donald Trump's administration over hack, charging that "the Trump administration failed to prioritize cybersecurity."

"This assault happened on Donald Trump's watch when he wasn't watching," Biden said. "It is a grave risk, and it continues. I see no evidence that it's under control. I've seen none."

Biden also charged that the Pentagon is failing to brief his transition team on the extent of the hack. On Wednesday, a senior defense official denied that was the case.

**'Damage done'**

"The question of the damage done remains to be determined," Biden said Tuesday. "We have to look at very closely the nature of the breaches, how extensive they are and what damage has been done."

When Biden takes office next month, the hack will pose an immediate challenge, as it's expected to take weeks or months to truly understand the extent of the damage to US agencies. Biden is also likely to have to decide how to respond if the federal government formally attributes the hack to Russia, which members of Trump's administration and lawmakers have said is likely.

"I believe that when I learn the extent of the damage, and in fact who's formally responsible, they can be assured that we will respond," Biden said Tuesday. "We'll probably respond in kind. We have many options, which I will not discuss now."

Lawmakers on the relevant committees are also pushing to learn more about the extent of the hack, why it took so long to be discovered, and why it was a private company that ultimately unearthed the breach. Congressional committees have been briefed both by US officials from the intelligence community and other agencies, as well as by FireEyes, a sign of the company's importance to understanding the data breach, lawmakers and aides say.

[[](https://www.cnn.com/2020/12/19/politics/pompeo-us-government-hack-russia/index.html)](https://www.cnn.com/2020/12/19/politics/pompeo-us-government-hack-russia/index.html)

[***Trump downplays massive cyber hack on government after Pompeo links attack to Russia***](https://www.cnn.com/2020/12/19/politics/pompeo-us-government-hack-russia/index.html)

"If the public reporting is accurate that it was the private sector that discovered this, that's another big question that our agencies are going to have to answer, which is, why didn't you catch this?" House Intelligence Chairman Adam Schiff said on MSNBC.

While a private company spotted the breach, a private sector contractor, SolarWinds, was at least one of the entry points hackers used to break into government networks. The software that the suspected malware was delivered with, SolarWinds Orion, has as many as 18,000 global customers, including government agencies and Fortune 500 companies.

"The government itself may have pretty good protections, but when you have a software firm you're contracting with and they send you a patch and you install it, turns out to not really be a patch but a back door for the Russians or Chinese or whoever wants to do something like this," said Sen. Angus King, a Maine Independent who co-chaired a congressional commission, the Cyberspace Solarium Commission, to improve US cyber defenses.

Much of the federal government only learned of one of the country's worst-ever cybersecurity incidents from public reporting and disclosures from private firms. Lawmakers predict there will be efforts next year both to strengthen the US defenses and improve government partnerships with the private sector.

**Complicated**

But that remains a complicated proposition.

"It's very clear from this that we're going to need to set up more partnerships between government and private companies," Rep. Jim Himes, a Connecticut Democrat on the House Intelligence Committee, told CNN. "We're going to need to have a tough conversation about whether we want to make it easier for the government to look at private companies' networks and products. That's a very tough conversation because there's civil liberties in the mix there."

Sen. Mark Warner of Virginia, the top Senate Intelligence Committee Democrat, told CNN's Poppy Harlow on Tuesday there should be a reexamination of reporting requirements after data breaches for both private companies and government agencies.

"If you are a public company, you have to report at the end of the quarter, but there is no immediate requirement to report" for government entities, Warner said. "These are all things that leave us much more vulnerable."