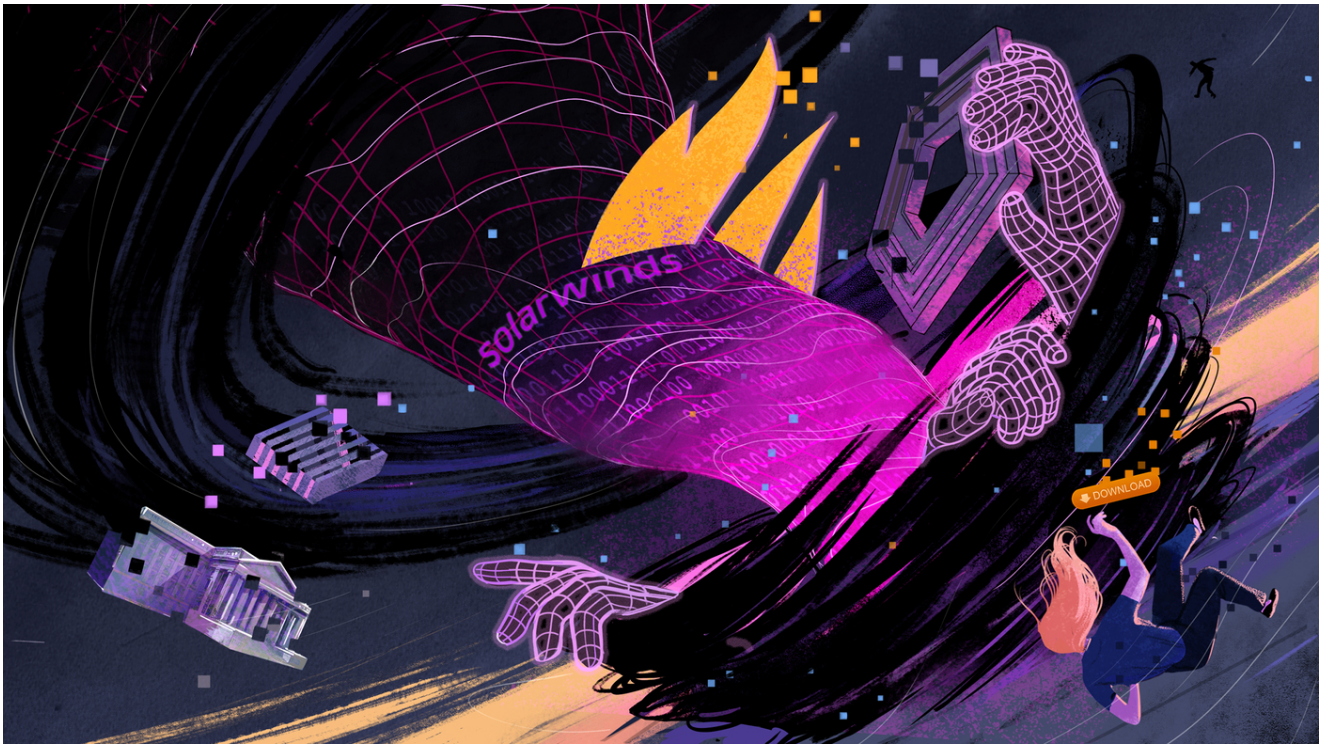
A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack

npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack



Special Series

Untangling Disinformation

April 16, 202110:05 AM ET

Heard on All Things Considered
Dina Temple-Raston

A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack

Listen · 12:08 12:08

- **Download**

- `<iframe src="https://www.npr.org/player/embed/985439655/988837603" width="100%" height="290" frameborder="0" scrolling="no" title="NPR embedded audio player">`
- **Transcript**

Enlarge this image

An NPR investigation into the SolarWinds attack reveals a hack unlike any other, launched by a sophisticated adversary intent on exploiting the soft underbelly of our digital lives. **Zoë van Dijk for NPR hide caption**

toggle caption

Zoë van Dijk for NPR

An NPR investigation into the SolarWinds attack reveals a hack unlike any other, launched by a sophisticated adversary intent on exploiting the soft underbelly of our digital lives.

Zoë van Dijk for NPR

"This release includes bug fixes, increased stability and performance improvements."

The routine software update may be one of the most familiar and least understood parts of our digital lives. A pop-up window announces its arrival and all that is required of us is to plug everything in before bed. The next morning, rather like the shoemaker and the elves, our software is magically transformed.

Last spring, a Texas-based company called SolarWinds made one such software update available to its customers. It was supposed to provide the regular fare — bug fixes, performance enhancements — to the company's popular network management system, a software program called Orion that keeps a watchful eye on all the various components in a company's network. Customers simply had to log into the company's software development website, type a password and then wait for the update to land seamlessly onto their servers.

The routine update, it turns out, is no longer so routine.

Hackers believed to be directed by the Russian intelligence service, the SVR, used that routine software update to slip malicious code into Orion's software and then used it as a vehicle for a massive cyberattack against America.

"Eighteen thousand [customers] was our best estimate of who may have downloaded the code between March and June of 2020," Sudhakar Ramakrishna, SolarWinds president and CEO, told NPR. "If you then take 18,000 and start sifting through it, the actual number of impacted customers is far less. We don't know the exact numbers. We are still conducting the investigation."

On Thursday, the Biden administration announced a roster of tough sanctions against Russia as part of what it characterized as the "seen and unseen" response to the SolarWinds breach.

NPR's months-long examination of that landmark attack — based on interviews with dozens of players from company officials to victims to cyber forensics experts who investigated, and intelligence officials who are in the process of calibrating the Biden administration's response — reveals a hack unlike any other, launched by a sophisticated adversary who took aim at a soft underbelly of digital life: the routine software update.

By design, the hack appeared to work only under very specific circumstances. Its victims had to download the tainted update and then actually deploy it. That was the first condition. The second was that their compromised networks needed to be connected to the Internet, so the hackers could communicate with their servers.

For that reason, Ramakrishna figures the Russians successfully compromised about 100 companies and about a dozen government agencies. The companies included Microsoft, Intel and Cisco; the list of federal agencies so far includes the Treasury, Justice and Energy departments and the Pentagon.

Enlarge this image

SolarWinds CEO and President Sudhakar Ramakrishna inherited the attack. He was hired shortly before the breach was discovered and stepped into the job just as the full extent of the hack became clear. **Demetrius Freeman/Pool/AFP via Getty Images hide caption**

toggle caption

Demetrius Freeman/Pool/AFP via Getty Images

SolarWinds CEO and President Sudhakar Ramakrishna inherited the attack. He was hired shortly before the breach was discovered and stepped into the job just as the full extent of the hack became clear.

Demetrius Freeman/Pool/AFP via Getty Images

The hackers also found their way, rather embarrassingly, into the Cybersecurity and Infrastructure Security Agency, or CISA — the office at the Department of Homeland Security whose job it is to protect federal computer networks from cyberattacks.

The concern is that the same access that gives the Russians the ability to steal data could also allow them to alter or destroy it. "The speed with which an actor can move from espionage to degrading or disrupting a network is at the blink of an eye," one senior administration said during a background briefing from the White House on Thursday. "And a defender cannot move at that speed. And given the history of Russia's malicious activity in cyberspace and their reckless behavior in cyberspace, that was a key concern."

"The tradecraft was phenomenal"

Network monitoring software is a key part of the backroom operations we never see. Programs like Orion allow information technology departments to look on one screen and check their whole network: servers or firewalls, or that printer on the fifth floor that keeps going offline. By its very nature, it touches everything — which is why hacking it was genius.

"It's really your worst nightmare," Tim Brown, vice president of security at SolarWinds, said recently. "You feel a kind of horror. This had the potential to affect thousands of customers; this had the potential to do a great deal of harm."

When cybersecurity experts talk about harm, they're thinking about something like what happened in 2017, when the Russian military launched a ransomware attack known as NotPetya. It, too, began with tainted software, but in that case the hackers were bent on destruction. They planted ransomware that paralyzed multinational companies and permanently locked people around the world out of tens of thousands of computers. Even this much later, it is considered the most destructive and costly cyberattack in history.

Intelligence officials worry that SolarWinds might presage something on that scale. Certainly, the hackers had time to do damage. They roamed around American computer networks for nine months, and it is unclear whether they were just reading emails and doing the things spies typically do, or whether they were planting something more destructive for use in the future.

"When there's cyber-espionage conducted by nations, FireEye is on the target list," Kevin Mandia, CEO of the cybersecurity firm FireEye, told NPR, but he believes there are other less obvious targets that now might need more protecting. "I think utilities might be on that list. I think health care might be on that list. And you don't necessarily want to be on the list of fair game for the most capable offense to target you."

Enlarge this image

Kevin Mandia, CEO of the cybersecurity firm FireEye, said the Russians didn't just attack SolarWinds, they took aim at trust. **Demetrius Freeman/Pool/Getty Images hide caption**

toggle caption

Demetrius Freeman/Pool/Getty Images

Kevin Mandia, CEO of the cybersecurity firm FireEye, said the Russians didn't just attack SolarWinds, they took aim at trust.

Demetrius Freeman/Pool/Getty Images

The SolarWinds attackers ran a master class in novel hacking techniques. They modified sealed software code, created a system that used domain names to select targets and mimicked the Orion software communication protocols so they could hide in plain sight. And then, they did what any good operative would do: They cleaned the crime scene so thoroughly investigators can't prove definitively who was behind it. The White House has said unequivocally that Russian intelligence was behind the hack. Russia, for its part, has denied any involvement.

"The tradecraft was phenomenal," said Adam Meyers, who led the cyber forensics team that pawed through that tainted update on behalf of SolarWinds, providing details for the first time about what they found. The code was elegant and innovative, he said, and then added, "This was the craziest f***ing thing I'd ever seen."

Like razor blades in peanut butter cups

Meyers is the vice president for threat intelligence at the cybersecurity firm CrowdStrike, and he's seen epic attacks up close. He worked on the 2014 Sony hack, when North Korea cracked into the company's servers and released emails and first-run movies. A year later, he was on the front lines when a suspected Kremlin-backed hacking team known as "Cozy Bear" stole, among other things, a trove of emails from the Democratic National Committee. WikiLeaks then released them in the runup to the 2016 election.

"We're involved in all kinds of incidents around the globe every day," Meyers said. Typically he directs teams, he doesn't run them. But SolarWinds was different: "When I started getting briefed up, I realized [this] was actually quite a big deal."

The attack began with a tiny strip of code. Meyers traced it back to Sept. 12, 2019. "This little snippet of code doesn't do anything," Meyers said. "It's literally just checking to see which processor is running on the computer, if it is a 32- or 64-bit processor and if it is one or the other, it returns either a zero or a one."

National Security

U.S. Slaps New Sanctions On Russia Over Cyberattack, Election Meddling

Investigations

Why Russia May Have Stepped Up Its Hacking Game

The code fragment, it turns out, was a proof of concept — a little trial balloon to see if it was possible to modify SolarWinds' signed-and-sealed software code, get it published and then later see it in a downloaded version. And they realized they could. "So at this point, they know that they can pull off a supply chain attack," Meyers said. "They know that they have that capability."

After that initial success, the hackers disappeared for five months. When they returned in February 2020, Meyers said, they came armed with an amazing new implant that delivered a backdoor that went into the software itself before it was published.

To understand why that was remarkable, you need to know that finished software code has a kind of digital factory seal. If you break that seal, someone can see it and know that the code might have been tampered with. Meyers said the hackers essentially found a way to get under that factory seal.

They began by implanting code that told them any time someone on the SolarWinds development team was getting ready to build new software. They understood that the process of creating software or an update typically begins with something routine such as checking a code out of a digital repository, sort of like checking a book out of the library.

Under normal circumstances, developers take the code out of the repository, make changes and then check it back in. Once they finish tinkering, they initiate something called the build process, which essentially translates the code a human can read to the code a computer does. At that point, the code is clean and tested. What the hackers did after that was the trick.

They would create a temporary update file with the malicious code inside while the SolarWinds code was compiling. The hackers' malicious code told the machine to swap in their temporary file instead of the SolarWinds version. "I think a lot of people probably assume that it is the source code that's been modified," Meyers said, but instead the hackers used a kind of bait-and-switch.

Enlarge this image

Adam Meyers, vice president for threat intelligence at CrowdStrike, said when he became familiar with the SolarWinds attack, he knew it was a big deal. **Oscar Zagal Studio hide caption**

toggle caption
Oscar Zagal Studio

Adam Meyers, vice president for threat intelligence at CrowdStrike, said when he became familiar with the SolarWinds attack, he knew it was a big deal.

Oscar Zagal Studio
But this, Meyers said, was interesting, too. The hackers understood that companies such as SolarWinds typically audit code before they start building an update, just to make sure everything is as it should be. So they made sure that the switch to the temporary file happened at the last possible second, when the updates went from source code (readable by people) to executable code (which the computer reads) to the software that goes out to customers.

The technique reminded Meyers of old fears around trick-or-treating. For decades, there had been an urban myth that kids couldn't eat any Halloween candy before checking the wrapper seal because bad people might have put razor blades inside. What the hackers did with the code, Meyers said, was a little like that.

"Imagine those Reese's Peanut Butter Cups going into the package and just before the machine comes down and seals the package, some other thing comes in and slides a razor blade into your Reese's Peanut Butter Cup," he said. Instead of a razor blade, the hackers swapped the files so "the package gets sealed and it goes out the door to the store."

The update that went out to SolarWinds' customers was the dangerous peanut butter cup — the malicious version of the software included code that would give the hackers unfettered, undetected access to any Orion user who downloaded and deployed the update and was connected to the Internet.

But there was something else about that code that bothered Meyers: It wasn't just for SolarWinds. "When we looked at [it], it could have been reconfigured for any number of software products," Meyers said. In other words, any number of other software developers using the same compiler may also be on the receiving end of a cyberattack, he said, and they just don't know it yet.

Picking and choosing targets

Meyers said it's hard not to admire just how much thought the hackers put into this operation. Consider the way they identified targets. The downside of breaking into so many customer networks all at once is that it is hard to decide what to exploit first. So the hackers created a

passive domain name server system that sent little messages with not just an IP address, which is just a series of numbers, but also with a thumbnail profile of a potential target.

"So they could then say, 'OK, we're going to go after this dot gov target or whatever,' " Meyers said. "I think later it became clear that there were a lot of government technology companies being targeted."

The hackers also reverse-engineered the way Orion communicated with servers and built their own coding instructions mimicking Orion's syntax and formats. What that did is allow the hackers to look like they were "speaking" Orion, so their message traffic looked like a natural extension of the software.

"So once they determined that a target was of interest, they could say, 'OK, let's go active, let's manipulate files, let's change something,' " Meyers said, and then they would slip in unnoticed through the backdoor they had created. "And there is one other thing I should mention: This backdoor would wait up to two weeks before it actually went active on the host. This was a very patient adversary."

None of the tripwires put in place by private companies or the government seems to have seen the attack coming. Christopher Krebs, who had been in charge of the office that protected government networks at DHS during the Trump administration, told NPR that DHS' current system, something known (without irony) as Einstein, only catches known threats. The SolarWinds breach, he said, was just "too novel."

Enlarge this image

Christopher Krebs, who was in charge of protecting government networks during the Trump administration, said the SolarWinds breach used techniques that were "too novel" for the current system to catch. **Drew Angerer/Getty Images hide caption**

toggle caption

Drew Angerer/Getty Images

Christopher Krebs, who was in charge of protecting government networks during the Trump administration, said the SolarWinds breach used techniques that were "too novel" for the current system to catch.

Drew Angerer/Getty Images

"Upwards of 90[%] to 95% of threats are based on known techniques, known cyberactivity," Krebs explained. "And that's not just criminal actors, that's state actors, too, including the Russian intelligence agencies and the Russian military. This was a previously unidentified technique."

And there is something else that Einstein doesn't do: It doesn't scan software updates. So even if the hackers had used code that Einstein would have recognized as bad, the system might not have seen it because it was delivered in one of those routine software updates.

The National Security Agency and the military's U.S. Cyber Command were also caught flat-footed. Broadly speaking, their cyber operators sit in foreign networks looking for signs of cyberattacks before they happen. They can see suspicious activity in much the same way a satellite might see troops amassing on the border. Critics said they should have seen the hackers from the Russian intelligence service, the SVR, preparing this attack.

"The SVR has a pretty good understanding that the NSA is looking out," Krebs said. "What the SVR was able to do was make the transition from wherever they were operating from into the U.S. networks. They move like ghosts. They are very hard to track."

The hackers didn't do anything fancy to give them the domestic footprint, officials confirmed. In fact, they just rented servers from Amazon and GoDaddy.

Early warnings

There were some indications, elsewhere, though, that something was wrong.

In early July, Steven Adair, the founder of a Washington, D.C.-based cybersecurity company called Volexity, saw some suspicious activity on a client's computers. "We traced it back, and we thought it might be related to a bad update with SolarWinds," Adair told NPR. "We addressed the problem, made sure no one was in our customers' systems, and we left it at that."

Adair said he didn't feel he had enough detail to report the problem to SolarWinds or the U.S. government. "We thought we didn't have enough evidence to reach out," he said.

That was the first missed sign.

The second came three months later when a California-based cybersecurity company called Palo Alto Networks discovered a malicious backdoor that seemed to emanate from the Orion software.

They move like ghosts. They are very hard to track.

Christopher Krebs, former director of the Cybersecurity and Infrastructure Security Agency

In that case, according to SolarWinds' Ramakrishna, the security teams at SolarWinds and Palo Alto worked together for three months to try to pick up the thread of the problem and walk it back. "None of us could pinpoint a supply chain attack at that point," Ramakrishna told NPR. "The ticket got closed as a result of that. If we had the benefit of hindsight, we could have traced it back" to the hack.

Palo Alto Networks had agreed to speak to NPR about the incident last month and then canceled the interview just an hour before it was supposed to take place. A spokesperson declined to say why and sent a few blog posts and wrote: "I'm afraid this is all we have to help at this time."

"Just 3,500 lines long"

It was the cybersecurity firm FireEye that finally discovered the intrusion. Mandia, the company's CEO, used to be in the U.S. Air Force Office of Special Investigations, so his specialty was criminal cases and counterintelligence. In the intervening years, the kinds of patterns he learned to recognize in special investigations kept appearing in his cyber security work.

The first indication that hackers had found their way into FireEye's networks came in an innocuous way. Someone on the FireEye security team had noticed that an employee appeared to have two phones registered on his network, so she called him. "And that phone call is when we realized, hey, this isn't our employee registering that second phone, it was somebody else," Mandia said.

Mandia had a security briefing a short time later and everything he heard reminded him of his previous work in the military. "There was a lot of pattern recognition from me," he told NPR. "I spent from 1996 to 1998 responding to what I would equate to the Russian Foreign Intelligence Service, and there were some indicators in the first briefing that were consistent with my experience in the Air Force."

He called a board meeting the same day. "It just felt like the breach that I was always worried about."

What his team discovered over the course of several weeks was that not only was there an intruder in its network, but someone had stolen the arsenal of hacking tools FireEye uses to test the security of its own clients' networks. FireEye called the FBI, put together a detailed report, and once it had determined the Orion software was the source of the problem, it called SolarWinds.

Brown, vice president of security at SolarWinds, took the Saturday morning phone call. "He said, 'Essentially, we've decompiled your code. We found malicious code,' " Brown said. FireEye was sure SolarWinds "had shipped tainted code."

The tainted code had allowed hackers into FireEye's network, and there were bound to be others who were compromised, too. "We were hearing that different reporters had the scoop already," Mandia said. "My phone actually rang from a reporter and that person knew and I went, OK, we're in a race."

Mandia thought they had about a day before the story would break.

After that, events seemed to speed up. SolarWinds' chief security officer, Brown, called Ron Plesco, a lawyer at the firm DLA Piper, and told him what had happened. One of the first things companies tend to do after cyberattacks is hire lawyers, and they put them in charge of the investigation. They do this for a specific reason — it means everything they find is protected by attorney-client privilege and typically is not discoverable in court.

Enlarge this image

Ron Plesco, a lawyer with the firm DLA Piper, has made cybercrimes a specialty of his practice. "I've been in situations where, while you're in there doing the investigation, [hackers are] watching your email, they're compromising your phone calls or your Zooms," he said.
Kriston Jae Bethel for NPR hide caption

toggle caption
Kriston Jae Bethel for NPR

Ron Plesco, a lawyer with the firm DLA Piper, has made cybercrimes a specialty of his practice. "I've been in situations where, while you're in there doing the investigation, [hackers are] watching your email, they're compromising your phone calls or your Zooms," he said.

Kriston Jae Bethel for NPR
Plesco, who has made cybercrimes a specialty of his practice, knew that once the story broke it would be saying "to the world that, ready, set, go, come after it," Plesco said. "So that puts you on an accelerated timeline on two fronts: Figure out what happened if you can and get a fix out as soon as possible."

The company worked with DHS to craft a statement that went out on Dec. 13.

To investigate a hack, you have to secure a digital crime scene. Just as detectives in the physical world have to bag the evidence and dust for prints for the investigation later, SolarWinds had to pull together computer logs, make copies of files, ensure there was a

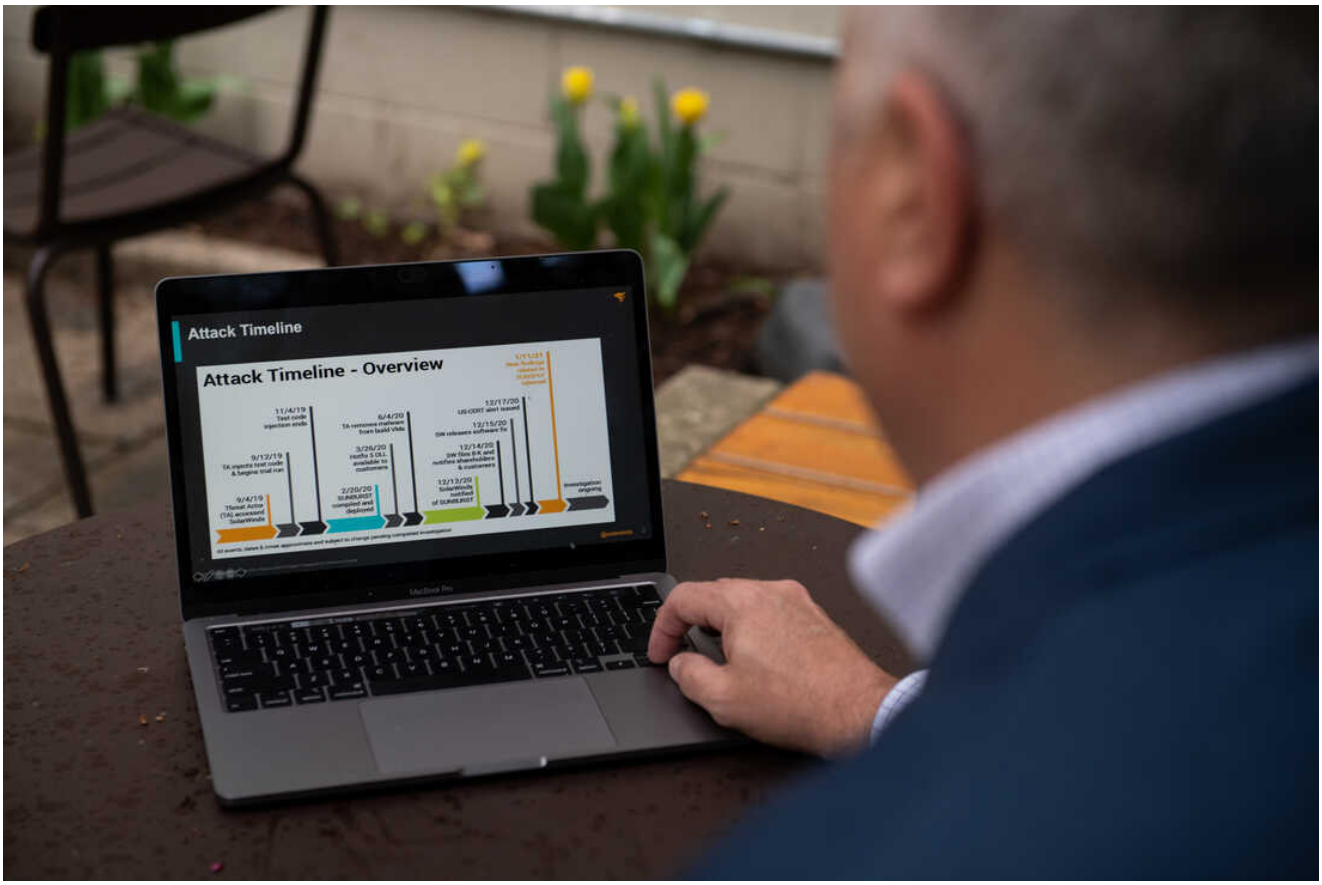
recorded chain of custody, all while trying to ensure the hackers weren't inside its system watching everything they did.

"I've been in situations where, while you're in there doing the investigation, they're watching your email, they're compromising your phone calls or your Zooms," Plesco said. "So they're literally listening in on how you're going to try to get rid of them."

By mid-January, Meyers and the CrowdStrike team had isolated what they thought was the attack's tiny beating heart. It was an elegant, encrypted little blob of code "just 3,500 lines long," he said. The best code is short and to the point, like a well-written sentence. This little encrypted strip, Meyers thought, might help them figure out who was behind the attack.

Little blobs of clues

Think of forensic cyber teams as digital detectives looking for patterns. Coding tics can sometimes help identify perpetrators or sometimes forensic teams find small cultural artifacts — such as Persian script, or Korean hangul. When an elite Russian hacking team took over the electrical grid in Ukraine in 2015, it had more literary aspirations: It sprinkled its malicious code with references to Frank Herbert's *Dune* novels. That's why CrowdStrike found that little blob of malicious code so intriguing.



Enlarge this image

Plesco shows a timeline of the SolarWinds hack on his computer. **Kriston Jae Bethel for NPR hide caption**

toggle caption
Kriston Jae Bethel for NPR

Plesco shows a timeline of the SolarWinds hack on his computer.

Kriston Jae Bethel for NPR
After weeks of working with the code, Meyers convened a Zoom call with leaders at SolarWinds and members of his team from around the world. He shared his screen so everyone could all watch the encryption fall away in real time. He began walking the spectators through the code as it was revealed, like a play-by-play analysis of a game. Meyers kept watching for the big reveal. "We're hoping it's going to have, you know, variable names or maybe some comments in Cyrillic or Mandarin to give us some clue who wrote this thing," he said.

But as CrowdStrike's decryption program chewed its way through the zeroes and ones, Meyers' heart sank. The crime scene was a bust. It had been wiped down. "They'd washed the code," Meyers said. "They'd cleaned it of any human artifact or tool mark. And that was kind of mind-blowing that [they] had the wherewithal to hide anything that a human might have inadvertently left behind as a clue."

Holy s***, he thought to himself, who does that?

Just type "solarwinds123"

Against such a sophisticated hack, it is easy to suggest this could have happened to just about any software company. But there were some troubling signs at SolarWinds that may have made it a target.

Consider its online marketing website. It contained a list of clients, including specific companies and government agencies, that ran its Orion software. While a lot of companies do that, the SolarWinds site was very specific. It was, two cybersecurity analysts told NPR, like a shopping list for adversaries.

Ramakrishna pushed back on the criticism. "Lots of companies do it. That is their badge of honor, saying all these customers rely on my technology," he said. "I wouldn't say that was the reason for why we were targeted." Ramakrishna said the hackers were "a lot more sophisticated" than that. Shortly after the attack, though, that particular page on the marketing website was taken down.

There was another unsettling report about passwords. A security researcher in Bangalore, India, named Vinoth Kumar told NPR that he had found the password to a server with SolarWinds apps and tools on a public message board and the password was: "solarwinds123." Kumar said he sent a message to SolarWinds in November and got an automated response back thanking him for his help and saying the problem had been fixed.

When NPR asked SolarWinds' vice president of security, Brown, about this, he said that the password "had nothing to do with this event at all, it was a password to a FTP site." An FTP site is what you use to transfer files over the Internet. He said the password was shared by an intern and it was "not an account that was linked to our active directory."

Ramakrishna said it was a password for a third-party site where some of SolarWinds' tools and apps were available for download. Ramakrishna admitted, though, that while the matter was unconnected to the breach, it was a problem to have that kind of password on a site that contained something someone might download thinking it was a SolarWinds product.

Enlarge this image

The SolarWinds attackers were masters in novel hacking techniques. The White House has said Russian intelligence was behind the hack. Russia has denied any involvement. **Bronte Wittpenn/Bloomberg via Getty Images hide caption**

toggle caption

Bronte Wittpenn/Bloomberg via Getty Images

The SolarWinds attackers were masters in novel hacking techniques. The White House has said Russian intelligence was behind the hack. Russia has denied any involvement.

Bronte Wittpenn/Bloomberg via Getty Images

"We used that as another opportunity to reeducate everybody on password policies," he said. "I do not want to minimize it or be casual about it, but I want to highlight that it had nothing to do" with the attack on Orion.

Ramakrishna inherited this attack. He was hired as the SolarWinds CEO shortly before the breach was discovered and stepped into the top job just as the full extent of the hack became clear. In a way, that has given him an incredible freedom. He can't be blamed for something that happened before he got there, and the changes he's making could be seen in the context of a new man in charge instead of a response to the attack.

Shortly after he arrived, he published a long blog post providing what was essentially an 11-point plan to improve company security. "Armed with what we have learned of this attack, we are also reflecting on our own security practices," he wrote in the blog post, adding that his goal was to put in place an "immediate improvement of critical business and product development systems."

Ramakrishna said he planned to transform SolarWinds into a truly "secure by design" organization with more robust threat protection and detection tools across its network, with a particular focus on where it developed and built software — the places that the SVR hackers used to break in.

He said he would establish privileged accounts and all accounts used by anybody who had anything to do with Orion and the company would enforce multifactor authentication, or MFA, across the board.

"If I come up with an 11-point plan to improve my company's security, one interpretation of that could be that we have learned a valuable lesson from what the hack was," said Ian Thornton-Trump, chief information security officer at Cyjax, a threat intelligence company. "The other interpretation could be, is that there were at least 11 material deficiencies in the actual security we had. I see that the 11-point plan is actually an admission that things were not good in this security house."

Thornton-Trump used to work at SolarWinds and was on the security team. Thornton-Trump left the company in 2017 because, by his own account, SolarWinds' management (Kevin Thompson was CEO at the time. Ramakrishna wouldn't arrive for another three years.) didn't want to spend enough on security.

Thornton-Trump concedes that the hackers who broke into the company were so sophisticated it would have been hard for anyone to defend against them. "But if you're driving drunk, rolling down the road, and it was raining and you smash up your car," he said, "why are we focused so much on the damage to the car, instead of what actually led up to the series of events that led to the great undoing?"

In other words, does the overhaul of SolarWinds' security practices add up to an admission that something was wrong, or is it simply a responsible upgrade?

Ramakrishna said it was both. "Oftentimes what happens is people conduct investigations, identify learnings and then implement something like this," he said. "Can we do things better? Absolutely. And honestly, even after implementing these 11 things, I'll be looking for the next 11 things to work on because the adversaries are becoming smarter and smarter every single day."

Ramakrishna said he wonders why, of all the software companies it had to choose from, the Russian intelligence service ended up targeting SolarWinds.

"I've thought about this quite a bit as to why us, why not somebody else," he said. "And that goes on through any investigation. As you think about this, we are deployed in more than 300,000 customers today. And so we are fairly broadly deployed software and where we enjoy administrative privileges in customer environments. So in a supply chain attack like this, the goal will be to try to get a broad swath of deployment and then you pick and choose what you want to do from there."

Whatever the reason SolarWinds ended up in the crosshairs, the attack revealed the U.S. cyber community's spectacular inability to connect the dots. Not just the early warnings from Volexity or the investigation with Palo Alto Networks, but a simple discovery from a lone cyber researcher in Bangalore suggests that something is not right in our digital world.

Bigger attacks

"It's one of the most effective cyber-espionage campaigns of all time," said Alex Stamos, director of the Internet Observatory at Stanford University and the former head of security at Facebook. "In doing so, they demonstrated not just technical acumen, but the way they did this demonstrated that they understand how tech companies operate, how software companies operate. ... This certainly is going to change the way that large enterprises think about the software they install and think about how they handle updates."

The adversaries are becoming smarter and smarter every single day.

Sudhakar Ramakrishna, SolarWinds CEO and president

Intelligence analysts, already years ahead of the rest of us, are paid to imagine the darkest of scenarios. What if the hackers planted the seeds of future attacks during that nine months they explored SolarWinds' customer networks — did they hide code for backdoors that will allow them to come and go as they please at a time of their choosing? When hackers shut down the Ukraine's power grid in 2015 and disabled a Saudi refinery with computer code a year later, they showed it was possible to jump from a corporate network to system controls. Will we find out later that the SolarWinds hack set the stage for something more sinister?

Even if this was just an espionage operation, FireEye's Mandia said, the attack on SolarWinds is an inflection point. "We ... kind of mapped out the evolution of threats and cyber," he said. "And we would have landed at this day sooner or later, that at some point in time, software that many companies depend on is going to get targeted and it's going to lead to exactly what it led to," Mandia said. "But to see it happen, that's where you have a little bit of shock and surprise. OK, it's here now, nations are targeting [the] private sector, there's no magic wand you can shake. ... It's a real complex issue to solve."

The Biden administration is working on a second executive order — beyond the sanctions — that is supposed to address some of the issues SolarWinds has put in stark relief.

Anne Neuberger, the deputy national security adviser for cyber and emerging technology in charge of the SolarWinds attack response, is preparing an order that would, among other things, require companies that work with the U.S. government to meet certain software standards, and federal agencies would be required to adopt basic security practices such as encrypting data in their systems.

In addition, software companies such as SolarWinds could be required to have their so-called build systems — the place where they assemble their software — air-gapped, which means they would not be connected to the Internet. Those elements are all still under discussion as part of the executive order, NPR has learned.

Enlarge this image

Anne Neuberger, deputy national security adviser for cyber and emerging technology, is in charge of the SolarWinds attack response. She is preparing an order that would require companies that work with the U.S. to meet certain software standards, and federal agencies would be required to adopt certain basic security practices. **Drew Angerer/Getty Images hide caption**

toggle caption

Drew Angerer/Getty Images

Anne Neuberger, deputy national security adviser for cyber and emerging technology, is in charge of the SolarWinds attack response. She is preparing an order that would require companies that work with the U.S. to meet certain software standards, and federal agencies would be required to adopt certain basic security practices.

Drew Angerer/Getty Images

Another idea starting to gain traction is to create a kind of National Transportation Safety Board, or NTSB, to investigate cyberattacks in a more formal way.

"When the Boeing 737 Maxes started crashing, there was a government agency whose entire job it was to gather up the facts of all those different crashes and then come up with a theory of what needed to be fixed and then oversaw the fixes that went into that," Stamos said. "We need the same kind of function in the U.S. government."

The FBI could do its investigation of the cybercrime and some sort of federal agency would look at the root causes of a cyberattack and make the appropriate changes to the way we do things. Mandia said something like that probably needs to exist.

"When you think about the conflict, you have air, land and sea and space and now cyber," he said. "But in cyber, the private sector is front and center. Any conflict in cyberspace, whether motivated by a criminal element or motivated by geopolitical conditions, it's going to involve both the government and the private sector. And that response, because it impacts both, you almost need a triage that both sides, both private and public sector, benefit from similar to the NTSB."

Mandia envisions a review board for significant incidents where intelligence is gathered and the nation finds a way to defend itself appropriately. Right now, the onus is on private companies to do all the investigations.

A Biden administration official told reporters during a background briefing Thursday that one reason the White House responded so strongly to the SolarWinds attack is because these kinds of hacks put an undue burden on private companies.

It's one of the most effective cyber-espionage campaigns of all time.

Alex Stamos, director of the Internet Observatory at Stanford University and former head of security at Facebook

A federal review might help with one of the issues that has plagued cyberspace up to now: how to ensure software and hardware vendors disclose hacks when they discover them. Could a review board take the sting out of the reputation damage of admitting publicly you've been hacked? Would it give companies such as Volexity and Palo Alto Networks somewhere to go when they see a problem?

Ultimately, the goal is to connect the dots and respond in a way that makes us safer. And the impetus for all of this might be that tainted routine update. That's one of the key reasons SolarWinds decided to go public, Ramakrishna said.

"We went out and published the entire source code because what we wanted people to do, no matter the vendor, whether it could be a competitor of ours or not, is to check your software, make sure you don't have a situation like this, and if there is, clean it up," he said. "So while it was unfortunate that we were the subject of this attack, my hope is, by us learning from it, we can also help the broader community."

Even so, there are parts of this story that may sound familiar: missed opportunities, hints of a problem that were ignored, the failure of U.S. intelligence officials to connect the dots. Who would have thought a routine software update could launch a cyberattack of epic proportions?

"This was an intelligence collection operation meant to steal information, and it's not the last time that's going to happen," CrowdStrike's Meyers warned. "This is going to happen every day. ... And I think there's a lot that we all need to do to work together to stop this from happening."

NPR's Monika Evstatieva contributed to this report.

Special Series

Untangling Disinformation