BY KIM ZETTER BACKCHANNEL MAY 2, 2023 6:00 AM

The Untold Story of the Boldest Supply-Chain Hack Ever

The attackers were in thousands of corporate and government networks. They might still be there now. Behind the scenes of the SolarWinds investigation.

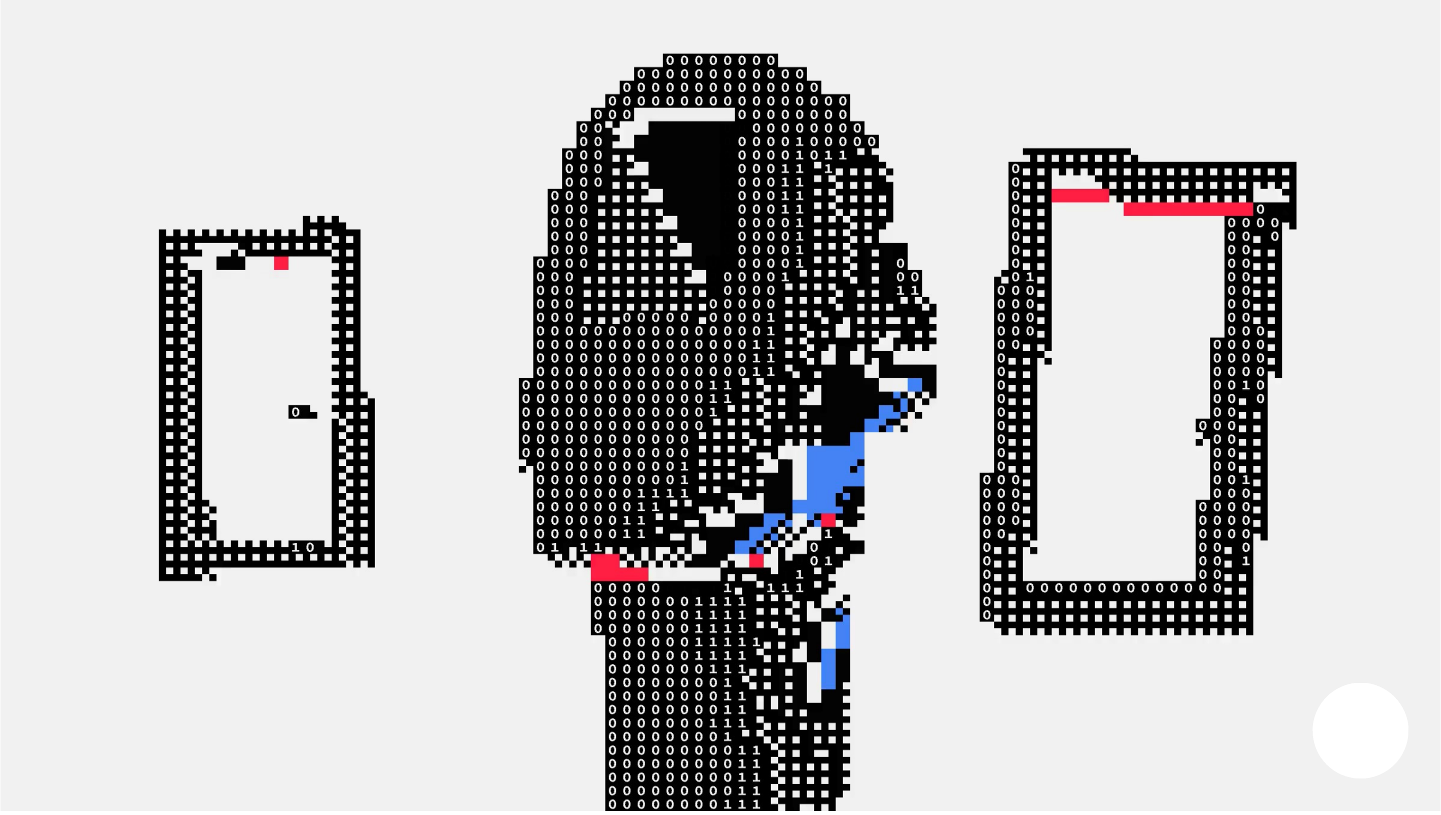

ILLUSTRATION: TAMEEM SANKARI

SAVE

STEVEN ADAIR WASN'T too rattled at first.

It was late 2019, and Adair, the president of the security firm Volexity, was investigating a digital security breach at an American think tank. The intrusion was nothing special. Adair figured he and his team would rout the attackers quickly and be done with the case—until they noticed something strange. A *second* group of hackers was active in the think tank's network. They were going after email, making copies and sending them to an outside server. These intruders were much more skilled, and they were returning to the network several times a week to siphon correspondence from specific executives, policy wonks, and IT staff.

Adair and his colleagues dubbed the second gang of thieves "Dark Halo" and booted them from the network. But soon they were back. As it turned out, the hackers had planted a backdoor on the network three years earlier —malicious code that opened a secret portal, allowing them to enter or communicate with infected machines. Now, for the first time, they were using it. "We shut down one door, and they quickly went to the other," Adair says.

His team spent a week kicking the attackers out again and getting rid of the backdoor. But in late June 2020, the hackers somehow returned. And they were back to grabbing email from the same accounts. The investigators spent days trying to figure out how they had slipped back in. Volexity zeroed in on one of the think tank's servers—a machine running a piece of software that helped the organization's system admins manage their computer network. That software was made by a company that was well known to IT teams around the world, but likely to draw blank stares from pretty much everyone else—an Austin, Texas, firm called SolarWinds.

This article appears in the June 2023 issue. Subscribe to WIRED. PHOTOGRAPH: DAN WINTERS

Adair and his team figured the hackers must have embedded another backdoor on the victim's server. But after considerable sleuthing, they couldn't find one. So they kicked the intruders out again and, to be safe, disconnected the server from the internet. Adair hoped that was the end of it. But the incident nagged at him. For days he woke up around 2 am with a sinking feeling that the team had missed something huge.

They had. And they weren't the only ones. Around the time Adair's team was kicking Dark Halo out of the think tank's network, the US Department of Justice was also wrestling with an intrusion—one involving a server running a trial version of the same SolarWinds software. According to sources with knowledge of the incident, the DOJ discovered suspicious traffic passing from the server to the internet in late May, so they asked one of the foremost security and digital forensics firms in the world—Mandiant—to help them investigate. They also engaged Microsoft, though it's not clear why. (A Justice Department spokesperson confirmed that this incident and investigation took place but declined to say whether Mandiant and Microsoft were involved. Neither company chose to comment on the investigation.)

According to the sources familiar with the incident, investigators suspected the hackers had breached the Justice Department server directly, possibly by exploiting a vulnerability in the SolarWinds software. The Justice Department team contacted the company, even referencing a specific file that they believed might be related to the issue, according to the sources, but SolarWinds' engineers were unable to find a vulnerability in their code. After weeks of back and forth the mystery was still unresolved, and the communication between investigators and SolarWinds stopped. (SolarWinds declined to comment on this episode.) The department, of course, had no idea about Volexity's uncannily similar hack.

As summer turned to fall, behind closed doors, suspicions began to grow among people across government and the security industry that something major was afoot. But the government, which had spent years trying to improve its communication with outside security experts, suddenly wasn't talking. Over the next few months, "people who normally were very chatty were hush-hush," a former government worker says. There was a rising fear among select individuals that a devastating cyber operation was unfolding, he says, and no one had a handle on it.

In fact, the Justice Department and Volexity had stumbled onto one of the most sophisticated cyberespionage campaigns of the decade. The perpetrators had indeed hacked SolarWinds' software. Using techniques that investigators had never seen before, the hackers gained access to thousands of the company's customers. Among the infected were at least eight other federal agencies, including the US Department of Defense, Department of Homeland Security, and the Treasury Department, as well as top tech and security firms, including Intel, Cisco, and Palo Alto Networks—though none of them knew it yet. Even Microsoft and Mandiant were on the victims list.

After the Justice Department incident, the operation remained undiscovered for another six months. When investigators finally cracked it, they were blown away by the hack's complexity and extreme premeditation. Two years on, however, the picture they've assembled—or at least what they've shared publicly—is still incomplete. A full accounting of the campaign's impact on federal systems and what was stolen has never been provided to the public or to lawmakers on Capitol Hill. According to the former government source and others, many of the federal agencies that were affected didn't maintain adequate network logs, and hence may not even know what all was taken. Worse: Some experts believe that SolarWinds was not the only vector—that other software makers were, or might still be, spreading malware. What follows is an account of the investigation that finally exposed the espionage operation—how it happened, and what we know. So far.

The Clue

ON NOVEMBER 10, 2020, an analyst at Mandiant named Henna Parviz responded to a routine security alert—the kind that got triggered anytime an employee enrolled a new phone in the firm's multifactor authentication system. The system sent out one-time access codes to credentialed devices, allowing employees to sign in to the company's virtual private network. But Parviz noticed something unusual about this Samsung device: It had no phone number associated with it.

She looked closely at the phone's activity logs and saw another strange detail. The employee appeared to have used the phone to sign in to his VPN account from an IP address in Florida. But the person didn't live in Florida, and he still had his old iPhone enrolled in the multifactor system. Then she noticed that the Samsung phone had been used to log in from the Florida IP address at the same time the employee had logged in with his iPhone from his home state. Mandiant had a problem.

The security team blocked the Samsung device, then spent a day investigating how the intruder had gotten into the network. They soon realized the issue transcended a single employee's account. The attackers had pulled off a Golden SAML attack—a sophisticated technique for hijacking a company's employee authentication system. They could seize control of a worker's accounts, grant those accounts more privileges, even create new accounts with unlimited access. With this power, there was no telling how deep they had burrowed into the network.

On November 17, Scott Runnels and Eric Scales, senior members of Mandiant's consulting division, quietly pulled together a top-tier investigative team of about 10, grabbing people from other projects without telling managers why, or even when the employees would return. Uncertain what the hunt would uncover, Runnels and Scales needed to control who knew about it. The group quickly realized that the hackers had been active for weeks but had evaded detection by "living off the land"—subverting administration tools already on the network to do their dirty deeds rather than bringing in their own. They also tried to avoid creating the patterns, in activity logs and elsewhere, that investigators usually look for.

> The Mandiant team was facing a textbook example of a supply-chain hack—the nefarious alteration of trusted software at its source.

But in trying to outsmart Mandiant, the thieves inadvertently left behind different fingerprints. Within a few days, investigators picked up the trail and began to understand where the intruders had been and what they had stolen.

On Friday morning, November 20, Kevin Mandia, Mandiant's founder and CEO, clicked out of an all-hands meeting with 3,000 employees and noticed that his assistant had added a new meeting to his calendar. "Security brief" was all it said. Mandia, a 52-year-old former Air Force intelligence officer who still sports taper-cut military hair two decades after leaving service, was planning to get an early start on the weekend, but he dialed into the call anyway. He expected a quick update of some kind. Five minutes into the conversation, he knew his weekend was shot.

RELATED STORIES

IT'S A TRAP!

The Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site

ANDY GREENBERG

SECURITY

Inside the Cyberattack That Shocked the US Government

BRENDAN I. KOERNER

WEAK LINK

The Massive 3CX Supply-Chain Hack Targeted Cryptocurrency Firms

ANDY GREENBERG

Many of the highest-profile hacks of the past two decades have been investigated by Mandia's firm, which he launched in 2004. Acquired by FireEye in 2013, and again last year by Google, the company has threat hunters working on more than 1,000 cases annually, which have included breaches at Google, Sony, Colonial Pipeline, and others. In all that time, Mandiant itself had never suffered a serious hack. Now the hunters were the hunted.

The intruders, Mandia learned, had swiped tools his company uses to find vulnerabilities in its clients' networks. They had also viewed sensitive information identifying its government customers. As his team described how the intruders had concealed their activity, Mandia flashed back to incidents from the early days of his career. From 1995 to 2013, while in the Air Force Office of Special Investigations and in the private sector, he had observed Russian threat actors continuously testing systems, disappearing as soon as investigators got a lock on them. Their persistence and stealth made them the toughest adversaries he'd ever faced. Now, hearing about the activity inside his own network, he "started getting pattern recognition," he later told a conference audience. The day after getting the unsettling news of the breach, he reached out to the National Security Agency (NSA) and other government contacts.

While Mandia conferred with the government, Charles Carmakal, the CTO of Mandiant Consulting, contacted some old friends. Many of the hackers' tactics were unfamiliar, and he wanted to see whether two former Mandiant colleagues, Christopher Glyer and Nick Carr, had seen them before. Glyer and Carr had spent years investigating large, sophisticated campaigns and had tracked the notorious hackers of the SVR—Russia's foreign intelligence agency—extensively. Now the two worked for Microsoft, where they had access to data from many more hacking campaigns than they had at Mandiant.

Carmakal told them the bare minimum—that he wanted help identifying some activity Mandiant was seeing. Employees of the two companies often shared notes on investigations, so Glyer thought nothing of the request. That evening, he spent a few hours digging into the data Carmakal sent him, then tapped Carr to take over. Carr was a night owl, so they often tag-teamed, with Carr passing work back to Glyer in the morning.

The two didn't see any of the familiar tactics of known hacking groups, but as they followed trails they realized whatever Mandiant was tracking was significant. "Every time you pulled on a thread, there was a bigger piece of yarn," Glyer recalls. They could see that multiple victims were communicating with the hackers Carmakal had asked them to trace. For each victim, the attackers set up a dedicated command-and-control server and gave that machine a name that partly mimicked the name a real system on the victim's network might have, so it wouldn't draw suspicion. When Glyer and Carr saw a list of those names, they realized they could use it to identify new victims. And in the process, they unearthed what Carmakal hadn't revealed to them—that Mandiant itself had been hacked.

It was a "holy shit" moment, recalls John Lambert, head of Microsoft Threat Intelligence. The attackers weren't only looking to steal data. They were conducting counterintelligence against one of their biggest foes. “Who do customers speed-dial the most when an incident happens?” he says. “It’s Mandiant.”

As Carr and Glyer connected more dots, they realized they had seen signs of this hack before, in unsolved intrusions from months earlier. More and more, the exceptional skill and care the hackers took to hide their tracks was reminding them of the SVR.

VIDEO: TAMEEM SANKARI

The Hunt

BACK AT MANDIANT, workers were frantically trying to address what to do about the tools the hackers had stolen that were designed to expose weak spots in clients’ defenses. Concerned that the intruders would use those products against Mandiant customers or distribute them on the dark web, Mandiant set one team to work devising a way to detect when they were being used out in the wild. Meanwhile, Runnels’ crew rushed to figure out how the hackers had slipped in undetected.

Because of the pandemic, the team was working from home, so they spent 18 hours a day connected through a conference call while they scoured logs and systems to map every step the hackers took. As days turned to weeks, they became familiar with the cadence of each other’s lives—the voices of children and partners in the background, the lulling sound of a snoring pit bull lying at Runnels’ feet. The work was so consuming that at one point Runnels took a call from a Mandiant executive while in the shower.

Runnels and Scales briefed Mandia daily. Each time the CEO asked the same question: How did the hackers get in? The investigators had no answer.

On December 8, when the detection tools were ready and the company felt it had enough information about the breach to go public, Mandiant broke its silence and released a blockbuster statement revealing that it had been hacked. It was sparse on details: Sophisticated hackers had stolen some of its security tools, but many of these were already public, and there was no evidence the attackers had used them. Carmakal, the CTO, worried that customers would lose confidence in the company. He was also anxious about how his colleagues would react to the news. “Are employees going to feel embarrassed?” he wondered. “Are people not going to want to be part of this team anymore?”

What Mandiant did not reveal was how the intruders got in or how long they had been in the company’s network. The firm says it still didn’t know. Those omissions created the impression that the breach was an isolated event with no other victims, and people wondered whether the company had made basic security errors that got it hacked. “We went out there and said that we got compromised by a top-tier adversary,” Carmakal says—something every victim claims. “We couldn’t show the proof yet.”

Mandiant isn’t clear about exactly when it made the first discovery that led it to the source of the breach. Runnels’ team fired off a barrage of hypotheses and spent weeks running down each one, only to turn up misses. They’d almost given up hope when they found a critical clue buried in traffic logs: Months earlier, a Mandiant server had communicated briefly with a mysterious system on the internet. And that server was running software from SolarWinds.

SolarWinds makes dozens of programs for IT administrators to monitor and manage their networks—helping them configure and patch a lot of systems at once, track performance of servers and applications, and analyze traffic. Mandiant was using one of the Texas company's most popular products, a software suite called Orion. The software should have been communicating with SolarWinds' network only to get occasional updates. Instead it was contacting an unknown system—likely the hackers' command-and-control server.

Back in June, of course, Mandiant had been called in to help the Justice Department investigate an intrusion on a server running SolarWinds software. Why the pattern-matchers at one of the world's preeminent security firms apparently didn't recognize a similarity between the two cases is one of the lingering mysteries of the SolarWinds debacle. It's likely that Runnels' chosen few hadn't worked on the Justice case, and internal secrecy prevented them from discovering the connection. (Mandiant declined to comment.)

Runnels' team suspected the infiltrators had installed a backdoor on the Mandiant server, and they tasked Willi Ballenthin, a technical director on the team, and two others with finding it. The task before him was not a simple one. The Orion software suite consisted of more than 18,000 files and 14 gigabytes of code and data. Finding the rogue component responsible for the suspicious traffic, Ballenthin thought, would be like riffling through *Moby-Dick* for a specific sentence when you'd never read the book.

But they had been at it only 24 hours when they found the passage they'd been looking for: a single file that appeared to be responsible for the rogue traffic. Carmakal believes it was December 11 when they found it.

The file was a .dll, or dynamic-link library—code components shared by other programs. This .dll was large, containing about 46,000 lines of code that performed more than 4,000 legitimate actions, and—as they found after analyzing it for an hour—one illegitimate one.

The main job of the .dll was to tell SolarWinds about a customer's Orion usage. But the hackers had embedded malicious code that made it transmit intelligence about the victim's network to *their* command server instead. Ballenthin dubbed the rogue code "Sunburst"—a play on SolarWinds. They were ecstatic about the discovery. But now they had to figure out how the intruders had snuck it into the Orion .dll.

This was far from trivial. The Orion .dll file was signed with a SolarWinds digital certificate, which was *supposed* to verify that the file was legitimate company code. One possibility was that the attackers had stolen the digital certificate, created a corrupt version of the Orion file, signed the file to make it look authentic, then installed the corrupt .dll on Mandiant's server. Or, more alarmingly, they might have breached SolarWinds' network and altered the legitimate Orion .dll source code *before* SolarWinds compiled it—converting the code into software—and signed it. The second scenario seemed so far-fetched that the Mandiant crew didn't really consider it—until an investigator downloaded an Orion software update from the SolarWinds website. The backdoor was in it.

The implication was staggering. The Orion software suite had about 33,000 customers, some of whom had started receiving the hacked software update in March. That meant some customers might have been compromised for eight months already. The Mandiant team was facing a textbook example of a software-supply-chain attack—the nefarious alteration of trusted software at its source. In a single stroke, attackers can infect thousands, potentially millions, of machines.

In 2017 hackers had sabotaged a software supply chain and delivered malware to more than 2 million users by compromising the computer security cleanup tool CCleaner. That same year, Russia distributed the malicious NotPetya worm in a software update to the Ukrainian equivalent of TurboTax, which then spread around the world. Not long after, Chinese hackers also used a software update to slip a backdoor to thousands of Asus customers. Even at this early stage in the investigation, the Mandiant team could tell that none of those other attacks would rival the SolarWinds campaign.

SolarWinds Joins the Chase

IT WAS A Saturday morning, December 12, when Mandia called SolarWinds' president and CEO on his cell phone. Kevin Thompson, a 14-year veteran of the Texas company, was stepping down as CEO at the end of the month. What he was about to hear from Mandia—that Orion was infected—was a hell of a way to wrap up his tenure. "We're going public with this in 24 hours," Mandia said. He promised to give SolarWinds a chance to publish an announcement first, but the timeline wasn't negotiable. What Mandia didn't mention was that he was under external pressure himself: A reporter had been tipped off about the backdoor and had contacted his company to confirm it. Mandia expected the story to break Sunday evening, and he wanted to get ahead of it.

Thompson started making calls, one of the first to Tim Brown, SolarWinds' head of security architecture. Brown and his staff quickly confirmed the presence of the Sunburst backdoor in Orion software updates and figured out, with alarm, that it had been delivered to as many as 18,000 customers since the spring of 2020. (Not every Orion user had downloaded it.) Thompson and others spent most of Saturday frantically pulling together teams to oversee the technical, legal, and publicity challenges they faced. They also called the company's outside legal counsel, DLA Piper, to oversee the investigation of the breach. Ron Plesco, an attorney at Piper and former prosecutor with forensic expertise, was in his backyard with friends when he got the call at around 10 pm.

Plesco beelined to his home office, arrayed with whiteboards, and started sketching out a plan. He set a timer for 20 hours, annoyed by what he felt was Mandia's arbitrary deadline. A day was nowhere near enough to prepare affected customers. He worried that once SolarWinds went public, the attackers might do something destructive in customers' networks before anyone could boot them out.

> The attackers had infected thousands of networks but only dug deep into a tiny subset of them—about 100. The main goal appeared to be espionage.

The practice of placing legal teams in charge of breach investigations is a controversial one. It puts cases under attorney-client privilege in a manner that can help companies fend off regulatory inquiries and fight discovery requests in lawsuits. Plesco says SolarWinds was, from the start, committed to transparency, publishing everything it could about the incident. (In interviews, the company was mostly forthcoming, but both it and Mandiant withheld some answers on the advice of legal counsel or per government request —Mandiant more so than SolarWinds. Also, SolarWinds recently settled a class action with shareholders over the breach but still faces a possible enforcement action from the Securities and Exchange Commission, making it less open than it might otherwise be about events.)

In addition to DLA Piper, SolarWinds brought on the security firm CrowdStrike, and as soon as Plesco learned this, he knew he wanted his old friend, Adam Meyers, on the case. The two had known each other for decades, ever since they'd worked on incident response for a defense contractor. Meyers was now the head of CrowdStrike's threat intelligence team and rarely worked investigations. But when Plesco texted him at 1 am to say "I need your help," he was all in.

Later that Sunday morning, Meyers jumped on a briefing call with Mandiant. On the call was a Microsoft employee, who told the group that in some cases, the hackers were systematically compromising Microsoft Office 365 email accounts and Azure cloud accounts. The hackers were also able to bypass multifactor authentication protocols. With every detail Meyers heard, the scope and complexity of the breach grew. Like others, he also suspected the SVR.

After the call, Meyers sat down in his living room. Mandiant had sent him the Sunburst code—the segment of the .dll file that contained the backdoor—so now he bent over his laptop and began picking it apart. He would remain in this huddled position for most of the next six weeks.

A Second Backdoor

AT SOLARWINDS, SHOCK, disbelief, and "controlled chaos" ruled those first days, says Tim Brown, the head of security architecture. Dozens of workers poured into the Austin office they hadn't visited in months to set up war rooms. The hackers had compromised 71 SolarWinds email accounts —likely to monitor correspondence for any indication they'd been detected— so for the first few days, the teams communicated only by phone and outside accounts, until CrowdStrike cleared them to use their corporate email again.

Brown and his staff had to figure out how they had failed to prevent or detect the hack. Brown knew that whatever they found could cost him his job.

One of the team's first tasks was to collect data and logs that might reveal the hackers' activity. They quickly discovered that some logs they needed didn't exist—SolarWinds didn't track everything, and some logs had been wiped by the attackers or overwritten with new data as time passed. They also scrambled to see whether any of the company's nearly 100 other products were compromised. (They only found evidence that Orion was hit.)

Around midmorning on Sunday, news of the hack began to leak. Reuters reported that whoever had struck Mandiant had also breached the Treasury Department. Then around 5 pm Eastern time, *Washington Post* reporter Ellen Nakashima tweeted that SolarWinds' software was believed to be the source of the Mandiant breach. She added that the Commerce Department had also been hit. The severity of the campaign was growing by the minute, but SolarWinds was still several hours from publishing its announcement. The company was obsessing over every detail—a required filing to the Securities and Exchange Commission got so heavily lawyered that Thompson, the CEO, quipped at one point that adding a single comma would cost $20,000.

Around 8:30 that night, the company finally published a blog post announcing the compromise of its Orion software—and emailed customers with a preliminary fix. Mandiant and Microsoft followed with their own reports on the backdoor and the activity of the hackers once inside infected networks. Oddly, Mandiant didn't identify itself as an Orion victim, nor did it explain how it discovered the backdoor in the first place. Reading Mandiant's write-up, one would never know that the Orion compromise had anything to do with the announcement of its own breach five days earlier.

Monday morning, calls started cascading in to SolarWinds from journalists, federal lawmakers, customers, and government agencies in and outside the US, including president-elect Joe Biden's transition team. Employees from across the company were pulled in to answer them, but the queue grew to more than 19,000 calls.

The US Cybersecurity and Infrastructure Security Agency wanted to know whether any research labs developing Covid vaccines had been hit. Foreign governments wanted lists of victims inside their borders. Industry groups for power and energy wanted to know whether nuclear facilities were breached.

As agencies scrambled to learn whether their networks used Orion software—many weren't sure—CISA issued an emergency directive to federal agencies to disconnect their SolarWinds servers from the internet and hold off on installing any patch aimed at disabling the backdoor until the security agency approved it. The agency noted that it was up against a "patient, well-resourced, and focused adversary" and that removing them from networks would be "highly complex and challenging." Adding to their problems, many of the federal agencies that had been compromised were lax about logging their network activity, which effectively gave cover to the hackers, according to the source familiar with the government's response. The government "couldn't tell how they got in and how far across the network they had gone," the source says. It was also "really difficult to tell what they had taken."

It should be noted that the Sunburst backdoor was useless to the hackers if a victim's Orion server wasn't connected to the internet. Luckily, for security reasons, most customers did not connect them—only 20 to 30 percent of all Orion servers were online, SolarWinds estimated. One reason to connect them was to send analytics to SolarWinds or to obtain software updates. According to standard practice, customers should have configured the servers to only communicate with SolarWinds, but many victims had failed to do this, including Mandiant and Microsoft. The Department of Homeland Security and other government agencies didn't even put them behind firewalls, according to Chris Krebs, who at the time of the intrusions was in charge of CISA. Brown, SolarWinds' security chief, notes that the hackers likely knew in advance whose servers were misconfigured.

But it soon became clear that although the attackers had infected thousands of servers, they had dug deep into only a tiny subset of those networks—about 100. The main goal appeared to be espionage.

The hackers handled their targets carefully. Once the Sunburst backdoor infected a victim's Orion server, it remained inactive for 12 to 14 days to evade detection. Only then did it begin sending information about an infected system to the attackers' command server. If the hackers decided the infected victim wasn't of interest, they could disable Sunburst and move on. But if they liked what they saw, they installed a second backdoor, which came to be known as Teardrop. From then on, they used Teardrop instead of Sunburst. The breach of SolarWinds' software was precious to the hackers—the technique they had employed to embed their backdoor in the code was unique, and they might have wanted to use it again in the future. But the more they used Sunburst, the more they risked exposing how they had compromised SolarWinds.

Through Teardrop, the hackers stole account credentials to get access to more sensitive systems and email. Many of the 100 victims that got Teardrop were technology companies—places such as Mimecast, a cloud-based service for securing email systems, or the antivirus firm Malwarebytes. Others were government agencies, defense contractors, and think tanks working on national security issues. The intruders even accessed Microsoft's source code, though the company says they didn't alter it.

In the Hot Seat

VICTIMS MIGHT HAVE made some missteps, but no one forgot where the breaches began. Anger against SolarWinds mounted quickly. A former employee claimed to reporters that he had warned SolarWinds executives in 2017 that their inattention to security made a breach inevitable. A researcher revealed that in 2018 someone had recklessly posted, in a public GitHub account, a password for an internal web page where SolarWinds software updates were temporarily stored. A bad actor could have used the password to upload malicious files to the update page, the researcher said (though this would not have allowed the Orion software itself to be compromised, and SolarWinds says that this password error was not a true threat). Far worse, two of the company's primary investors—firms that owned about 75 percent of SolarWinds and held six board seats—sold $315 million in stock on December 7, six days before news of the hack broke, prompting an SEC investigation into whether they had known about the breach.

Government officials threatened to cancel their contracts with SolarWinds; lawmakers were talking about calling its executives into a hearing. The company hired Chris Krebs, CISA's former head, who weeks earlier had been fired by President Donald Trump, to help navigate interactions with the government.

Meanwhile, Brown and his security team faced a mountain of work. The tainted Orion software was signed with the company's digital certificate, which they now had to invalidate. But the same certificate had been used to sign many of the company's other software products too. So the engineers had to recompile the source code for every affected product and sign those new programs with new certificates.

But they still didn't know where the rogue code in Orion had come from. Malicious code could be lurking on their servers, which could embed a backdoor in any of the programs being compiled. So they ditched their old compilation process for a new one that allowed them to check the finished program for any unauthorized code. Brown says they were under so much stress to get the recompiled programs out to customers that he lost 25 pounds in three weeks.

While Brown's team rebuilt the company's products and CrowdStrike tried to figure out how the hackers got into SolarWinds' network, SolarWinds brought on KPMG, an accounting firm with a computer forensics arm, to solve the mystery of how the hackers had slipped Sunburst into the Orion .dll file. David Cowen, who had more than 20 years of experience in digital forensics, led the KPMG team.

The infrastructure SolarWinds used to build its software was vast, and Cowen and his team worked with SolarWinds engineers through the holidays to solve the riddle. Finally, on January 5, he called Plesco, the DLA Piper attorney. A SolarWinds engineer had spotted something big: artifacts of an old virtual machine that had been active about a year earlier. That virtual machine—a set of software applications that takes the place of a physical computer—had been used to build the Orion software back in 2020. It was the critical puzzle piece they needed.

Forensic investigations are often a game of chance. If too much time has passed since a breach began, traces of a hacker's activity can disappear. But sometimes the forensic gods are on your side and evidence that should be gone remains.

To build the Orion program, SolarWinds had used a software build-management tool called TeamCity, which acts like an orchestra conductor to turn source code into software. TeamCity spins up virtual machines—in this case about 100—to do its work. Ordinarily, the virtual machines are ephemeral and exist only as long as it takes to compile software. But if part of the build process fails for some reason, TeamCity creates a “memory dump”—a kind of snapshot—of the virtual machine where the failure occurred. The snapshot contains all of the virtual machine’s contents at the time of failure. That’s exactly what occurred during the February 2020 build. Ordinarily, SolarWinds engineers would delete these snapshots during post-build cleanup. But for some reason, they didn’t erase this one. If it hadn’t been for its improbable existence, Cowen says, “we would have nothing.”

In the snapshot, they found a malicious file that had been on the virtual machine. Investigators dubbed it “Sunspot.” The file had only 3,500 lines of code, but those lines turned out to be the key to understanding everything.

It was around 9 pm on January 5 when Cowen sent the file to Meyers at CrowdStrike. The CrowdStrike team got on a Zoom call with Cowen and Plesco, and Meyers put the Sunspot file into a decompiler, then shared his screen. Everyone grew quiet as the code scrolled down, its mysteries slowly revealed. This tiny little file, which should have disappeared, was responsible for injecting the backdoor into the Orion code and allowing the hackers to slip past the defenses of some of the most well-protected networks in the country.

Now the investigators could trace any activity related to Sunspot. They saw that the hackers had planted it on the build server on February 19 or 20. It lurked there until March, when SolarWinds developers began building an Orion software update through TeamCity, which created a fleet of virtual machines. Not knowing which virtual machine would compile the Orion .dll code, the hackers designed a tool that deployed Sunspot into each one.

At this point, the beauty and simplicity of the hack truly revealed itself. Once the .dll appeared on a virtual machine, Sunspot quickly and automatically renamed that legitimate file and gave its original name to the hackers' rogue doppelgänger .dll. The latter was almost an exact replica of the legitimate file, except it contained Sunburst. The build system then grabbed the hackers' .dll file and compiled it into the Orion software update. The operation was done in a matter of seconds.

Once the rogue .dll file was compiled, Sunspot restored the original name to the legitimate Orion file, then deleted itself from all of the virtual machines. It remained on the build server for months, however, to repeat the process the next two times Orion got built. But on June 4, the hackers abruptly shut down this part of their operation—removing Sunspot from the build server and erasing many of their tracks.

Cowen, Meyers, and the others couldn't help but pause to admire the tradecraft. They'd never before seen a build process get compromised. "Sheer elegance," Plesco called it. But then they realized something else: Nearly every other software maker in the world was vulnerable. Few had built-in defenses to prevent this type of attack. For all they knew, the hackers might have already infiltrated other popular software products. "It was this moment of fear among all of us," Plesco says.

In the Government

THE NEXT DAY, January 6—the same day as the insurrection on Capitol Hill—Plesco and Cowen hopped on a conference call with the FBI to brief them on their gut-churning discovery. The reaction, Plesco says, was palpable. "If you can sense a virtual jaw drop, I think that's what occurred."

A day later they briefed the NSA. At first there were just two people from the agency on the video call—faceless phone numbers with identities obscured. But as the investigators relayed how Sunspot compromised the Orion build, Plesco says, more than a dozen phone numbers popped up onscreen, as word of what they'd found "rippled through the NSA."

But the NSA was about to get another shock. Days later, members of the agency joined a conference call with 50 to 100 staffers from the Homeland Security and Justice Departments to discuss the SolarWinds hack. The people on the call were stumped by one thing: Why, when things had been going so well for them, had the attackers suddenly removed Sunspot from the build environment on June 4?

The response from an FBI participant stunned everyone.

The man revealed matter-of-factly that, back in the spring of 2020, people at the agency had discovered some rogue traffic emanating from a server running Orion and contacted SolarWinds to discuss it. The man conjectured that the attackers, who were monitoring SolarWinds' email accounts at the time, must have gotten spooked and deleted Sunspot out of fear that the company was about to find it.

Callers from the NSA and CISA were suddenly livid, according to a person on the line—because for the first time, they were learning that Justice had detected the hackers months earlier. The FBI guy "phrased it like it was no big deal," the attendee recalls. The Justice Department told WIRED it had informed CISA of its incident, but at least some CISA people on the call were responding as if it was news to them that Justice had been close to discovering the attack—half a year before anyone else. An NSA official told WIRED that the agency was indeed "frustrated" to learn about the incident on the January call. For the attendee and others on the call who hadn't been aware of the DOJ breach, it was especially surprising, because, the source notes, in the months after the intrusion, people had been "freaking out" behind closed doors, sensing that a significant foreign spy operation was underway; better communication among agencies might have helped uncover it sooner.

Instead, says the person with knowledge of the Justice investigation, that agency, as well as Microsoft and Mandiant, surmised that the attackers must have infected the DOJ server in an isolated attack. While investigating it in June and July, Mandiant had unknowingly downloaded and installed tainted versions of the Orion software to its own network. (CISA declined to comment on the matter.)

The SVR Hackers

THE DISCOVERY OF the Sunspot code in January 2021 blew the investigation open. Knowing when the hackers deposited Sunspot on the build server allowed Meyers and his team to track their activity backward and forward from that time and reinforced their hunch that the SVR was behind the operation.

The SVR is a civilian intelligence agency, like the CIA, that conducts espionage outside the Russian Federation. Along with Russia's military intelligence agency, the GRU, it hacked the US Democratic National Committee in 2015. But where the GRU tends to be noisy and aggressive—it publicly leaked information stolen from the DNC and Hilary Clinton's presidential campaign—SVR hackers are more deft and quiet. Given various names by different security firms (APT29, Cozy Bear, the Dukes), SVR hackers are noted for their ability to remain undetected in networks for months or years. The group was very active between 2014 and 2016, Glyer says, but then seemed to go dark. Now he understood that they'd used that time to restrategize and develop new techniques, some of which they used in the SolarWinds campaign.

Investigators found that the intruders had first used an employee's VPN account on January 30, 2019, a full *year* before the Orion code was compromised. The next day, they returned to siphon 129 source code repositories for various SolarWinds software products and grabbed customer information—presumably to see who used which products. They "knew where they were going, knew what they were doing," Plesco says.

The hackers likely studied the source code and customer data to select their target. Orion was the perfect choice. The crown jewel of SolarWinds' products, it accounted for about 45 percent of the company's revenue and occupied a privileged place in customer networks—it connected to and communicated with a lot of other servers. The hackers could hijack those connections to jump to other systems without arousing suspicion.

Once they had the source code, the hackers disappeared from the SolarWinds network until March 12, when they returned and accessed the build environment. Then they went dark for six months. During that time they may have constructed a replica of the build environment to design and practice their attack, because when they returned on September 4, 2019, their movements showed expertise. The build environment was so complex that a newly hired engineer could take months to become proficient in it, but the hackers navigated it with agility. They also knew the Orion code so well that the doppelgänger .dll they created was stylistically indistinguishable from the legitimate SolarWinds file. They even improved on its code, making it cleaner and more efficient. Their work was so exceptional that investigators wondered whether an insider had helped the hackers, though they never found evidence of that.

Not long after the hackers returned, they dropped benign test code into an Orion software update, meant simply to see whether they could pull off their operation and escape notice. Then they sat back and waited. (SolarWinds wasn't scheduled to release its next Orion software update for about five months.) During this time, they watched the email accounts of key executives and security staff for any sign their presence had been detected. Then, in February 2020, they dropped Sunspot into place.

On November 26, the intruders logged in to the SolarWinds VPN for the last time—while Mandiant was deep into its investigation. The hackers continued to monitor SolarWinds email accounts until December 12, the day Kevin Mandia called Kevin Thompson to report the backdoor. Nearly two years had passed since they had compromised SolarWinds.

ILLUSTRATION: TAMEEM SANKARI

The Legacy of the Hack

STEVEN ADAIR, THE Volexity CEO, says it was pure luck that, back in 2019, his team had stumbled on the attackers in a think tank's network. They felt proud when their suspicion that SolarWinds was the source of the intrusion was finally confirmed. But Adair can't help but rue his missed chance to halt the campaign earlier. "We were so close," he says.

Mandiant's Carmakal believes that if the hackers hadn't compromised his employer, the operation might have gone undetected for much longer. Ultimately, he calls the SolarWinds hacking campaign "a hell of an expensive operation for very little yield"—at least in the case of its impact on Mandiant. "I believe we caught the attackers far earlier than they ever anticipated," he says. "They were clearly shocked that we uncovered this … and then discovered SolarWinds' supply chain attack."

But given how little is still known publicly about the wider campaign, any conclusions about the success of the operation may be premature.

The US government has been fairly tight-lipped about what the hackers did inside its networks. News reports revealed that the hackers stole email, but how much correspondence was lost or what it contained has never been disclosed. And the hackers likely made off with more than email. From targeting the Departments of Homeland Security, Energy, and Justice, they could plausibly have accessed highly sensitive information—perhaps details on planned sanctions against Russia, US nuclear facilities and weapons stockpiles, the security of election systems, and other critical infrastructure. From the federal court's electronic case-files system, they could have siphoned off sealed documents, including indictments, wiretap orders, and other nonpublic material. Given the logging deficiencies on government computers noted by one source, it's possible the government still doesn't have a full view of what was taken. From technology companies and security firms, they could have nabbed intelligence about software vulnerabilities.

More concerning: Among the 100 or so entities that the hackers focused on were other makers of widely used software products. Any one of those could potentially have become a vehicle for another supply chain attack of similar scale, targeting the customers of those companies. But few of those other companies have revealed what, if anything, the hackers did inside their networks. Why haven't they gone public, as Mandiant and SolarWinds did? Is it to protect their reputations, or did the government ask them to keep quiet for national security reasons or to protect an investigation? Carmakal feels strongly that the SolarWinds hackers intended to compromise other software, and he said recently in a call with the press that his team had seen the hackers "poking around in source code and build environments for a number of other technology companies."

What's more, Microsoft's John Lambert says that judging by the attackers' tradecraft, he suspects the SolarWinds operation wasn't their first supply chain hack. Some have even wondered whether SolarWinds itself got breached through a different company's infected software. SolarWinds still doesn't know how the hackers first got into its network or whether January 2019 was their first time—the company's logs don't go back far enough to determine.

Krebs, the former head of CISA, condemns the lack of transparency. “This was not a one-off attack by the SVR. This is a broader global-listening infrastructure and framework,” he says, “and the Orion platform was just one piece of that. There were absolutely other companies involved.” He says, however, that he doesn’t know specifics.

Krebs takes responsibility for the breach of government networks that happened on his watch. “I was the leader of CISA while this happened,” he says. “There were many people in positions of authority and responsibility that share the weight here of not detecting this.” He faults the Department of Homeland Security and other agencies for not putting their Orion servers behind firewalls. But as for detecting and halting the broader campaign, he notes that “CISA is really the last line of defense … and many other layers failed.”

The government has tried to address the risks of another Orion-style attack —through presidential directives, guidelines, initiatives, and other security-boosting actions. But it may take years for any of these measures to have impact. In 2021, President Biden issued an executive order calling on the Department of Homeland Security to set up a Cyber Safety Review Board to thoroughly assess “cyber incidents” that threaten national security. Its first priority: to investigate the SolarWinds campaign. But in 2022 the board focused on a different topic, and its second investigation will also not be about SolarWinds. Some have suggested the government wants to avoid a deep assessment of the campaign because it could expose industry and government failures in preventing the attack or detecting it earlier.

“SolarWinds was the largest intrusion into the federal government in the history of the US, and yet there was not so much as a report of what went wrong from the federal government,” says US representative Ritchie Torres, who in 2021 was vice-chair of the House Committee on Homeland Security.

"It's as inexcusable as it is inexplicable."

At a recent conference, CISA and the US's Cyber National Mission Force, a division of Cyber Command, revealed new details about their response to the campaign. They said that after investigators identified Mandiant's Orion server as the source of that firm's breach, they gleaned details from Mandiant's server that allowed them to hunt down the attackers. The two government teams implied that they even penetrated a system belonging to the hackers. The investigators were able to collect 18 samples of malware belonging to the attackers—useful for hunting for their presence in infected networks.

Speaking to conference attendees, Eric Goldstein, the leader for cybersecurity at CISA, said the teams were confident that they had fully booted these intruders from US government networks.

But the source familiar with the government's response to the campaign says it would have been very difficult to have such certainty. The source also said that around the time of Russia's invasion of Ukraine last year, the prevailing fear was that the Russians might still be lurking in those networks, waiting to use that access to undermine the US and further their military efforts.

Meanwhile, software-supply-chain hacks are only getting more ominous. A recent report found that in the past three years, such attacks increased more than 700 percent.

This article appears in the June 2023 issue. Subscribe now.

Let us know what you think about this article. Submit a letter to the editor at mail@wired.com.

Get More From WIRED

- 📩 Don’t miss our biggest stories, delivered to your inbox every day
- 🎧 Our new podcast wants you to *Have a Nice Future*
- The night 17 million military records went up in smoke
- The AI protest group campaigning against human extinction
- How your new car tracks you
- A grid collapse would make a heat wave far deadlier
- WIRED’s favorite “buy it for life” gear
- 🌲 Our Gear team has branched out with a new guide to the best sleeping pads and fresh picks for the best coolers and binoculars

Kim Zetter writes about cybersecurity and national security and is the author of *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon*.

TOPICS LONGREADS SECURITY CYBERSECURITY HACKING GOVERNMENT HACKS MAGAZINE-31.06

MORE FROM WIRED

The Night 17 Million Precious Military Records Went Up in Smoke

Fifty years ago, a fire ripped through the National Personnel Records Center. It set off a massive project to save crucial pieces of American history—including, I hoped, my grandfather's.

MEGAN GREENWELL

Boots Riley Says a ‘Gentler Capitalism’ Won’t Save Society

The *I’m a Virgo* creator loves contradictions, like trying to launch a radical labor movement with a show on Amazon Prime.

JASON PARHAM

The Dark Secrets Buried at Red Cloud Boarding School

How much truth and healing can forensic tech really bring? On the sites of Native American tragedies, Marsha Small has made it her life’s mission to find out.

ROWAN MOORE GERETY

How Christopher Nolan Learned to Stop Worrying and Love AI

The *Oppenheimer* director says AI is not the bomb. His new movie might still scare you shitless.

MARIA STRESHINSKY

Meet the Psychedelic Boom's First Responders

With more tripping will come more psychic terror. A new movement of volunteers will guide you through your brain melt.

CHRIS COLIN