www.propublica.org /article/microsoft-solarwinds-golden-saml-data-breach-russian-hackers

Whistleblower Says Microsoft Dismissed Warnings About a Security Flaw That Russians Later Used to Hack U.S. Government

by Renee Dudley, with research by Doris Burke ⋮ 39-50 minutes

Microsoft hired Andrew Harris for his extraordinary skill in keeping hackers out of the nation's most sensitive computer networks. In 2016, Harris was hard at work on a mystifying incident in which intruders had somehow penetrated a major U.S. tech company.

The breach troubled Harris for two reasons. First, it involved the company's cloud — a virtual storehouse typically containing an organization's most sensitive data. Second, the attackers had pulled it off in a way that left little trace.

He retreated to his home office to "war game" possible scenarios, stress-testing the various software products that could have been compromised.

Early on, he focused on a Microsoft application that ensured users had permission to log on to cloud-based programs, the cyber equivalent of an officer checking passports at a border. It was there, after months of research, that he found something seriously wrong.

The product, which was used by millions of people to log on to their work computers, contained a flaw that could allow attackers to masquerade as legitimate employees and rummage through victims' "crown jewels" — national security secrets, corporate intellectual property, embarrassing personal emails — all without tripping alarms.

To Harris, who had previously spent nearly seven years working for the Defense Department, it was a security nightmare. Anyone using the software was exposed, regardless of whether they used Microsoft or another cloud provider such as Amazon. But Harris was most concerned about the federal government and the implications of his discovery for national security. He flagged the issue to his colleagues.

They saw it differently, Harris said. The federal government was preparing to make a massive investment in cloud computing, and Microsoft wanted the business. Acknowledging this security flaw could jeopardize the company's chances, Harris recalled one product leader telling him. The financial consequences were enormous. Not only could Microsoft lose a multibillion-dollar deal, but it could also lose the race to dominate the market for cloud computing.

Harris said he pleaded with the company for several years to address the flaw in the product, a ProPublica investigation has found. But at every turn, Microsoft dismissed his warnings, telling him they would work on a long-term alternative — leaving cloud services around the globe vulnerable to attack in the meantime.

Harris was certain someone would figure out how to exploit the weakness. He'd come up with a temporary solution, but it required customers to turn off one of Microsoft's most convenient and popular features: the ability to access nearly every program used at work with a single logon.

He scrambled to alert some of the company's most sensitive customers about the threat and personally oversaw the fix for the New York Police Department. Frustrated by Microsoft's inaction, he left the company in August 2020.

Andrew Harris shared his Microsoft employee badge on his LinkedIn page when he announced his departure from the company in 2020. Credit: Screenshot by ProPublica

Within months, his fears became reality. U.S. officials confirmed reports that a state-sponsored team of Russian hackers had carried out SolarWinds, one of the largest cyberattacks in U.S. history. They used the flaw Harris had identified to vacuum up sensitive data from a number of federal agencies, including, ProPublica has learned, the National Nuclear Security Administration, which maintains the United States' nuclear weapons stockpile, and the National Institutes of Health, which at the time was engaged in COVID-19 research and vaccine distribution.

The Russians also used the weakness to compromise dozens of email accounts in the Treasury Department, including those of its highest-ranking officials. One federal official described the breach as “an espionage campaign designed for long-term intelligence collection.”

Harris’ account, told here for the first time and supported by interviews with former colleagues and associates as well as social media posts, upends the prevailing public understanding of the SolarWinds hack.

From the moment the hack surfaced, Microsoft insisted it was blameless. Microsoft President Brad Smith assured Congress in 2021 that “there was no vulnerability in any Microsoft product or service that was exploited” in SolarWinds.

He also said customers could have done more to protect themselves.

Harris said they were never given the chance.

“The decisions are not based on what’s best for Microsoft’s customers but on what’s best for Microsoft,” said Harris, who now works for CrowdStrike, a cybersecurity company that competes with Microsoft.

Microsoft declined to make Smith and other top officials available for interviews for this story, but it did not dispute ProPublica’s findings. Instead, the company issued a statement in response to written questions. “Protecting customers is always our highest priority,” a spokesperson said. “Our security response team takes all security issues seriously and gives every case due diligence with a thorough manual assessment, as well as cross-confirming with engineering and security partners. Our assessment of this issue received multiple reviews and was aligned with the industry consensus.”

ProPublica’s investigation comes as the Pentagon seeks to expand its use of Microsoft products — a move that has drawn scrutiny from federal lawmakers amid a series of cyberattacks on the government.

Smith is set to testify on Thursday before the House Homeland Security Committee, which is examining Microsoft’s role in a breach perpetrated last year by hackers connected to the Chinese government. Attackers exploited Microsoft security flaws to gain access to top U.S. officials’ emails. In investigating the attack, the federal Cyber Safety Review Board found that Microsoft’s “security culture was inadequate and requires an overhaul.”

Microsoft President Brad Smith testifies during a Senate Select Committee on Intelligence hearing about SolarWinds on Feb. 23, 2021. Credit: Drew Angerer/Getty Images

For its part, Microsoft has said that work has already begun, declaring that the company’s top priority is security “above all else.” Part of the effort involves adopting the board’s recommendations. “If you’re faced with the tradeoff between security and another priority, your answer is clear: Do security,” the company’s CEO, Satya Nadella, told employees in the wake of the board’s report, which identified a “corporate culture that deprioritized both enterprise security investments and rigorous risk management.”

ProPublica’s investigation adds new details and pivotal context about that culture, offering an unsettling look into how the world’s largest software provider handles the security of its own ubiquitous products. It also offers crucial insight into just how much the quest for profits can drive those security decisions, especially as tech behemoths push to dominate the newest — and most lucrative — frontiers, including the cloud market.

“This is part of the problem overall with the industry,” said Nick DiCola, who was one of Harris’ bosses at Microsoft and now works at Zero Networks, a network security firm. Publicly-traded tech giants “are beholden to the share price, not to doing what’s right for the customer all the time. That’s just a reality of capitalism. You’re never going to change that in a public company because at the end of the day, they want the shareholder value to go up.”

A “Cloud-First World”

Early this year, Microsoft surpassed Apple to become the world’s most valuable company, worth more than $3 trillion. That triumph was almost unimaginable a decade ago. (The two remain in close competition for the top spot.)

In 2014, the same year that Harris joined Microsoft and Nadella became the CEO, Wall Street and consumers alike viewed the company as stuck in the past, clinging to the “shrink-wrapped” software products like Windows that put it on the map in the 1990s. Microsoft's long-stagnant share price reflected its status as an also-ran in almost every major technological breakthrough since the turn of the century, from its Bing search engine to its Nokia mobile phone division.

As the new CEO, Nadella was determined to reverse the trend and shake off the company's fuddy-duddy reputation, so he staked Microsoft's future on the Azure cloud computing division, which then lagged far behind Amazon. In his earliest all-staff memo, Nadella told employees they would need "to reimagine a lot of what we have done in the past for a … cloud-first world."

Microsoft CEO Satya Nadella promotes the company's cloud offerings at an event in San Francisco in 2014. Credit: David Paul Morris/Bloomberg via Getty Images

Microsoft salespeople pitched business and government customers on a "hybrid cloud" strategy, where they kept some traditional, on-premises servers (typically stored on racks in customers' own offices) while shifting most of their computing needs to the cloud (hosted on servers in Microsoft data centers).

Security was a key selling point for the cloud. On-site servers were notoriously vulnerable, in part because organizations' overburdened IT staff often failed to promptly install the required patches and updates. With the cloud, that crucial work was handled by dedicated employees whose job was security.

The dawn of the cloud era at Microsoft was an exciting time to work in the field of cybersecurity for someone like Harris, whose high school yearbook features a photo of him in front of a desktop computer and monitor with a mess of floppy disks beside him. One hand is on the keyboard, the other on a wired mouse. Caption: "Harris the hacker."

Harris' high school yearbook Credit: Classmates.com

As a sophomore at Pace University in New York, he wrote a white paper titled "How to Hack the Wired Equivalent Protocol," a network security standard, and was awarded a prestigious Defense Department scholarship, which the government uses to recruit cybersecurity specialists. The National Security Agency paid for three years of his tuition, which included a master's degree in software engineering, in exchange for a commitment to work for the government for at least that long, he said.

Early in his career, he helped lead the Defense Department's efforts to protect individual devices. He became an expert in the niche field known as identity and access management, securing how people log in.

As the years wore on, he grew frustrated by the lumbering bureaucracy and craved the innovation of the tech industry. He decided he could make a bigger impact in the private sector, which designed much of the software the government used.

At Microsoft he was assigned to a secretive unit known as the "Ghostbusters" (as in: "Who you gonna call?"), which responded to hacks of the company's most sensitive customers, especially the federal government. As a member of this team, Harris first investigated the puzzling attack on the tech company and remained obsessed with it, even after switching roles inside Microsoft.

Eventually, he confirmed the weakness within Active Directory Federation Services, or AD FS, a product that allowed users to sign on a single time to access nearly everything they needed. The problem, he discovered, rested in how the application used a computer language known as SAML to authenticate users as they logged in.

Credit: Illustrations by Anuj Shrestha, special to ProPublica

This is what makes a SAML attack unique. Typically, hackers leave what cybersecurity specialists call a "noisy" digital trail. Network administrators monitoring the so-called "audit logs" might see unknown or foreign IP addresses attempting to gain access to their cloud services. But SAML attacks are much harder to detect. The forged token is the equivalent of a robber using a copied master key. There was little trail to track, just the activities of what appear to be legitimate users.

Harris and a colleague who consulted for the Department of Defense spent hours in front of both real and virtual whiteboards as they mapped out how such an attack would work, the colleague told ProPublica. The "token theft" risk, as Harris referred to it, became a regular topic of discussion for them.

A Clash With "Won't Fix" Culture

Before long, Harris alerted his supervisors about his SAML finding. Nick DiCola, his boss at the time, told ProPublica he referred Harris to the Microsoft Security Response Center, which fields reports of security vulnerabilities and determines which need to be addressed. Given its central role in improving Microsoft product security, the team once considered itself the “conscience of the company,” urging colleagues to improve security without regard to profit. In a meeting room, someone hung a framed photo of Winston “the Wolf,” the charismatic fixer in Quentin Tarantino’s movie “Pulp Fiction” who is summoned to clean up the aftermath of bloody hits.

Members of the team were not always popular within the company. Plugging security holes is a cost center, and making new products is a profit center, former employees told ProPublica. In 2002, the company’s founder, Bill Gates, tried to settle the issue, sending a memo that turned out to be eerily prescient. “Flaws in a single Microsoft product, service or policy not only affect the quality of our platform and services overall, but also our customers’ view of us as a company,” Gates wrote, adding: “So now, when we face a choice between adding features and resolving security issues, we need to choose security.”

At first, Gates’ memo was transformational and the company’s product divisions were more responsive to the center’s concerns. But over time, the center’s influence waned.

Its members were stuck between cultural forces. Security researchers — often characterized as having outsized egos — believed their findings should be immediately addressed, underestimating the business challenges of developing fixes quickly, former MSRC employees told ProPublica.

Product managers had little motivation to act fast, if at all, since compensation was tied to the release of new, revenue-generating products and features. That attitude was particularly pronounced in Azure product groups, former MSRC members said, because they were under pressure from Nadella to catch up to Amazon.

“Azure was the Wild West, just this constant race for features and functionality,” said Nate Warfield, who worked in the MSRC for four years beginning in 2016. “You will get a promotion because you released the next new shiny thing in Azure. You are not going to get a promotion because you fixed a bunch of security bugs.”

Former employees told ProPublica that the center fielded hundreds or even thousands of reports a month, pushing the perennially understaffed group to its limits. The magazine Popular Science noted that volume as one of the reasons why working in the MSRC was one of the 10 “worst jobs in science,” between whale feces researchers and elephant vasectomists.

“They’re trained, because they’re so resource constrained, to think of these cases in terms of: ‘How can I get to ‘won’t fix,’” said Dustin Childs, who worked in the MSRC in the years leading up to Harris’ saga. Staff would often punt on fixes by telling researchers they would be handled in “v-next,” the next product version, he said. Those launches, however, could be years away, leaving customers vulnerable in the interim, he said.

The center also routinely rejected researchers’ reports of weaknesses by saying they didn’t cross what its staff called a “security boundary.” But when Harris discovered the SAML flaw, it was a term with no formal definition, former employees said.

Credit: Jaap Arriens / Sipa USA via AP Images

By 2017, the lack of clarity had become the “butt of jokes,” Warfield said. Several prominent security researchers who regularly interacted with the MSRC made T-shirts and stickers that said “_____ [fill in the blank] is not a security boundary.”

“Any time Microsoft didn’t want to fix something, they’d just say, ‘That’s not a security boundary, we’re not going to fix it,’” Warfield recalled.

Unaware of the inauspicious climate, Harris met virtually with MSRC representatives and sketched out how a hacker could jump from an on-premises server to the cloud without being detected. The MSRC declined to address the problem. Its staff argued that hackers attempting to exploit the SAML flaw would first have to gain access to an on-premises server. As they saw it, Harris said, that was the security boundary — not the subsequent hop to the cloud.

Business Over Security

“WTF,” Harris recalled thinking when he got the news. “This makes no sense.”

Microsoft had told customers the cloud was the safest place to put their most precious data. His discovery proved that, for the millions of users whose systems included AD FS, their cloud was only as secure as their on-premises servers. In other words, all the buildings owned by the landlord are only as secure as the most careless tenant who forgot to lock their window.

Harris pushed back, but he said the MSRC held firm.

Harris had a reputation for going outside the chain of command to air his concerns, and he took his case to the team managing the products that verified user identities.

He had some clout, his former colleagues said. He had already established himself as a known expert in the field, had pioneered a cybersecurity threat detection method and later was listed as the named inventor on a Microsoft patent. Harris said he "went kind of crazy" and fired off an email to product manager Mark Morowczynski and director Alex Simons requesting a meeting.

He understood that developing a long-term fix would take time, but he had an interim solution that could eliminate the threat. One of the main practical functions of AD FS was to allow users to access both on-premises servers and a variety of cloud-based services after entering credentials only once, a Microsoft feature known as "seamless" single sign-on. Harris proposed that Microsoft tell its customers to turn off that function so the SAML weakness would no longer matter.

According to Harris, Morowczynski quickly jumped on a videoconference and said he had discussed the concerns with Simons.

"Everyone violently agreed with me that this is a huge issue," Harris said. "Everyone violently disagreed with me that we should move quickly to fix it."

Morowczynski, Harris said, had two primary objections.

First, a public acknowledgement of the SAML flaw would alert adversaries who could then exploit it. Harris waved off the concern, believing it was a risk worth taking so that customers wouldn't be ignorant to the threat. Plus, he believed Microsoft could warn customers without betraying any specifics that could be co-opted by hackers.

According to Harris, Morowczynski's second objection revolved around the business fallout for Microsoft. Harris said Morowczynski told him that his proposed fix could alienate one of Microsoft's largest and most important customers: the federal government, which used AD FS. Disabling seamless SSO would have widespread and unique consequences for government employees, who relied on physical "smart cards" to log onto their devices. Required by federal rules, the cards generated random passwords each time employees signed on. Due to the configuration of the underlying technology, though, removing seamless SSO would mean users could not access the cloud through their smart cards. To access services or data on the cloud, they would have to sign in a second time and would not be able to use the mandated smart cards.

Harris said Morowczynski rejected his idea, saying it wasn't a viable option.

Morowczynski told Harris that his approach could also undermine the company's chances of getting one of the largest government computing contracts in U.S. history, which would be formally announced the next year. Internally, Nadella had made clear that Microsoft needed a piece of this multibillion-dollar deal with the Pentagon if it wanted to have a future in selling cloud services, Harris and other former employees said.

Killing the Competition

By Harris' account, the team was also concerned about the potential business impact on the products sold by Microsoft to sign into the cloud. At the time, Microsoft was in a fierce rivalry with a company called Okta.

Microsoft customers had been sold on seamless SSO, which was one of the competitive advantages — or, in Microsoft parlance, "kill points" — that the company then had over Okta, whose users had to sign on twice, Harris said.

Harris' proposed fix would undermine the company's strategy to marginalize Okta and would "add friction" to the user experience, whereas the "No. 1 priority was to remove friction," Harris recalled Morowczynski telling him. Moreover, it would have cascading consequences for the cloud business because the sale of identity products often led to demand for other cloud services.

“That little speed bump of you authenticating twice was unacceptable by Microsoft’s standards,” Harris said. He recalled Morowczynski telling him that the product group’s call “was a business decision, not a technical one.”

“What they were telling me was counterintuitive to everything I’d heard at Microsoft about ‘customer first,’” Harris said. “Now they’re telling me it’s not ‘customer first,’ it’s actually ‘business first.’”

DiCola, Harris’ then-supervisor, told ProPublica the race to dominate the market for new and high-growth areas like the cloud drove the decisions of Microsoft’s product teams. “That is always like, ‘Do whatever it frickin’ takes to win because you have to win.’ Because if you don’t win, it’s much harder to win it back in the future. Customers tend to buy that product forever.”

According to Harris, Morowczynski said his team had “on the road map” a product that could replace AD FS altogether. But it was unclear when it would be available to customers.

In the months that followed, Harris vented to his colleagues about the product group’s decision. ProPublica talked to three people who worked with Harris at the time and recalled these conversations. All of them spoke on the condition of anonymity because they feared professional repercussions. The three said Harris was enraged and frustrated over what he described to them as the product group’s unwillingness to address the weakness.

Neither Morowczynski nor Simons returned calls seeking comment, and Microsoft declined to make them available for interviews. The company did not dispute the details of Harris’ account. In its statement, Microsoft said it weighs a number of factors when it evaluates potential threats. “We prioritize our security response work by considering potential customer disruption, exploitability, and available mitigations,” the spokesperson said. “We continue to listen to the security research community and evolve our approach to ensure we are meeting customer expectations and protecting them from emerging threats.”

Another Major Warning

Following the conversation with Morowczynski, Harris wrote a reminder to himself on the whiteboard in his home office: “SAML follow-up.” He wanted to keep the pressure on the product team.

Soon after, the Massachusetts- and Tel Aviv-based cybersecurity firm CyberArk published a blog post describing the flaw, which it dubbed “Golden SAML,” along with a proof of concept, essentially a road map that showed how hackers could exploit the weakness.

Years later, in his written testimony for the Senate Intelligence Committee, Microsoft’s Brad Smith said this was the moment the company learned of the issue. “The Golden SAML theory became known to cybersecurity professionals at Microsoft and across the U.S. government and the tech sector at precisely the same time, when it was published in a public paper in 2017,” Smith wrote.

Lavi Lazarovitz of CyberArk said the firm mentioned the weakness — before the post was published — in a private WhatsApp chat of about 10 security researchers from various companies, a forum members used to compare notes on emerging threats. When they raised the discovery to the group, which included at least one researcher from Microsoft, the other members were dismissive, Lazarovitz said.

“Many in the security research community — I don’t want to say mocked — but asked, ‘Well, what’s the big deal?’” Lazarovitz said.

The CyberArk headquarters in Newton, Massachusetts Credit: Sipa via AP Images

Nevertheless, CyberArk believed it was worth taking seriously, given that AD FS represented the gateway to users’ most sensitive information, including email. “Threat actors operate in between the cracks,” Lazarovitz said. “So obviously, we understood the feedback that we got, but we still believed that this technique will be eventually leveled by threat actors.”

The Israel-based team also reached out to contacts at Microsoft’s Israeli headquarters and were met with a response similar to the one they got in the WhatsApp group, Lazarovitz said.

The published report was CyberArk’s way of warning the public about the threat. Disclosing the weakness also had a business benefit for the company. In the blog post, it pitched its own security product, which it said “will be extremely beneficial in blocking attackers from getting their hands on important assets like the token-signing certificate in the first place."

The report initially received little attention. Harris, however, seized on it. He said he alerted Morowczynski and Simons from the product group as well as the MSRC. The situation was more urgent than before, Harris argued to them, because CyberArk included the proof of concept that could be used by hackers to carry out a real attack. For Harris, it harkened back to Morowczynski's worry that flagging the weakness could give hackers an advantage.

"I was more energetic than ever to have us actually finally figure out what we're going to do about this," Harris said.

But the MSRC reiterated its "security boundary" stance, while Morowczynski reaffirmed the product group's earlier decision, Harris said.

Harris said he then returned to his supervisors, including Hayden Hainsworth and Bharat Shah, who, as corporate vice president of the Azure cloud security division, also oversaw the MSRC. "I said, 'Can you guys please listen to me,'" Harris recalled. "'This is probably the most important thing I've ever done in my career.'"

Harris said they were unmoved and told him to take the problem back to the MSRC.

Microsoft did not publicly comment on the CyberArk blog post at the time. Years later, in written responses to Congress, Smith said the company's security researchers reviewed the information but decided to focus on other priorities. Neither Hainsworth nor Shah returned calls seeking comment.

Defusing a Ticking Bomb

Harris said he was deeply frustrated. On a personal level, his ego was bruised. Identifying major weaknesses is considered an achievement for cybersecurity professionals, and, despite his internal discovery, CyberArk had claimed Golden SAML.

More broadly, he said he was more worried than ever, believing the weakness was a ticking bomb. "It's out in the open now," he said.

Publicly, Microsoft continued to promote the safety of its products, even boasting of its relationship with the federal government in sales pitches. "To protect your organization, Azure embeds security, privacy, and compliance into its development methodology," the company said in late 2017, "and has been recognized as the most trusted cloud for U.S. government institutions."

Attendees walk through the exhibition floor during the Microsoft Developers Build Conference in Seattle in 2017. Credit: David Ryder/Bloomberg via Getty Images

Internally, Harris complained to colleagues that customers were being left vulnerable.

"He was definitely having issues" with the product team, said Harris' former Microsoft colleague who consulted for the Defense Department. "He vented that it was a problem that they just wanted to ignore."

Harris typically pivoted from venting to discussing how to protect customers, the former colleague said. "I asked him to show me what I'm going to have to do to make sure the customers were aware and could take corrective action to mitigate the risk," he said.

Harris also took his message to LinkedIn, where he posted a discreet warning and an offer.

"I hope all my friends and followers on here realize by now the security relationship" involved in authenticating users in AD FS, he wrote in 2019. "If not, reach out and let's fix that!"

In 2019, Harris posted a discreet warning and an offer on LinkedIn. Credit: Screenshot by ProPublica

Separately, he realized he could help customers with whom he had existing relationships, including the NYPD, the nation's largest police force.

"Knowing this exploit is actually possible, why would I not architect around it, especially for my critical customers?" Harris said.

On a visit to the NYPD, Harris told a top IT official, Matthew Fraser, about the AD FS weakness and recommended disabling seamless SSO. Fraser was in disbelief at the severity of the issue, Harris recalled, and he agreed to disable seamless SSO.

In an interview, Fraser confirmed the meeting.

“This was identified as one of those areas that was prime, ripe,” Fraser said of the SAML weakness. “From there, we figured out what’s the best path to insulate and secure.”

More Troubling Revelations

It was over beers at a conference in Orlando in 2018 that Harris learned the weakness was even worse than he’d initially realized. A colleague sketched out on a napkin how hackers could also bypass a common security feature called multifactor authentication, which requires users to perform one or more additional steps to verify their identity, such as entering a code sent via text message.

They realized that, no matter how many additional security steps a company puts in place, a hacker with a forged token can bypass them all. When they brought the new information to the MSRC, “it was a nonstarter,” Harris said. While the center had published a formal definition of “security boundary” by that point, Harris’ issues still didn’t meet it.

Nadella delivers the keynote address at a 2018 conference in Seattle for software developers.
Credit: Elaine Thompson/AP

By March 2019, concerns over Golden SAML were spilling out into the wider tech world. That month, at a conference in Germany, two researchers from the cybersecurity company Mandiant delivered a presentation demonstrating how hackers could infiltrate AD FS to gain access to organizations’ cloud accounts and applications. They also released the tools they used to do so.

Mandiant said it notified Microsoft before the presentation, making it the second time in roughly 16 months that an outside firm had flagged the SAML issue to the company.

In August 2020, Harris left Microsoft to work for CrowdStrike. In his exit interview with Shah, Harris said he raised the SAML weakness one last time. Shah listened but offered no feedback, he said.

“There is no inspector general-type thing” within Microsoft, Harris said. “If something egregious is happening, where the hell do you go? There’s no place to go.”

SolarWinds Breaks

Four months later, news of the SolarWinds attack broke. Federal officials soon announced that beginning in 2019 Russian hackers had breached and exploited the network management software offered by a Texas-based company called SolarWinds, which had the misfortune of lending its name to the attack. The hackers covertly inserted malware into the firm’s software updates, gaining “backdoor” access to the networks of companies and government agencies that installed them. The ongoing access allowed hackers to take advantage of “post-exploit” vulnerabilities, including Golden SAML, to steal sensitive data and emails from the cloud.

Despite the name, nearly a third of victims of the attack never used SolarWinds software at all, Brandon Wales, then acting director of the federal Cybersecurity and Infrastructure Security Agency, said in the aftermath. In March 2021, Wales told a Senate panel that hackers were able to “gain broad access to data stores that they wanted, largely in Microsoft Office 365 Cloud … and it was all because they compromised those systems that manage trust and identity on networks.”

Microsoft itself was also breached.

In the immediate aftermath of the attack, Microsoft advised customers of Microsoft 365 to disable seamless SSO in AD FS and similar products — the solution that Harris proposed three years earlier.

As the world dealt with the consequences, Harris took his long simmering frustration public in a series of posts on social media and on his personal blog. Challenging Brad Smith by name, and criticizing the MSRC’s decisions — which he referred to as “utter BS” — Harris lambasted Microsoft for failing to publicly warn customers about Golden SAML.

Microsoft “was not transparent about these risks, forced customers to use ADFS knowing these risks, and put many customers and especially US Gov’t in a bad place,” Harris wrote on LinkedIn in December 2020. A long-term fix was “never a priority” for the company, he wrote. “Customers are boned and sadly it’s been that way for years (which again, sickens me),” Harris said in the post.

In the months and years following the SolarWinds attack, Microsoft took a number of actions to mitigate the SAML risk. One of them was a way to efficiently detect fallout from such a hack. The advancement, however, was available only as part of a paid add-on product known as Sentinel.

The lack of such a detection, the company said in a blog post, had been a “blind spot.”

“Microsoft Is Back on Top”

In early 2021, the Senate Select Committee on Intelligence called Brad Smith to testify about SolarWinds.

Although Microsoft’s product had played a central role in the attack, Smith seemed unflappable, his easy and conversational tone a reflection of the relationships he had spent decades building on Capitol Hill. Without referencing notes or reading from a script, as some of his counterparts did, he confidently deflected questions about Microsoft’s role. Laying the responsibility with the government, he said that in the lead-up to the attack, the authentication flaw “was not prioritized by the intelligence community as a risk, nor was it flagged by civilian agencies or other entities in the security community as a risk that should be elevated” over other cybersecurity priorities.

Smith also downplayed the significance of the Golden SAML weakness, saying it was used in just 15% of the 60 cases that Microsoft had identified by that point. At the same time, he acknowledged that, “without question, these are not the only victims who had data observed or taken.”

When Sen. Marco Rubio of Florida pointedly asked him what Microsoft had done to address Golden SAML in the years before the attack, Smith responded by listing a handful of steps that customers could have taken to protect themselves. His suggestions included purchasing an antivirus product like Microsoft Defender and securing devices with another Microsoft product called Intune.

“The reality is any organization that did all five of those things, if it was breached, it in all likelihood suffered almost no damage,” Smith said.

Neither Rubio nor any other senator pressed further.

Ultimately, Microsoft won a piece of the Defense Department’s multibillion-dollar cloud business, sharing it with Amazon, Google and Oracle.

Since December 2020, when the SolarWinds attack was made public, Microsoft’s stock has soared 106%, largely on the runaway success of Azure and artificial intelligence products like ChatGPT, where the company is the largest investor. “Microsoft Is Back on Top,” proclaimed Fortune, which featured Nadella on the cover of its most recent issue.

In September 2021, just 10 months after the discovery of SolarWinds, the paperback edition of Smith’s book, “Tools and Weapons,” was published. In it, Smith praised Microsoft’s response to the attack. The MSRC, Smith wrote, “quickly activated its incident response plan” and the company at large “mobilized more than 500 employees to work full time on every aspect of the attack.”

In the new edition, Smith also reflected on his congressional testimony on SolarWinds. The hearings, he wrote, “examined not only what had happened but also what steps needed to be taken to prevent such attacks in the future.” He didn’t mention it in the book, but that certainly would include the long-term alternative that Morowczynski first promised to Harris in 2017. The company began offering it in 2022.

Development by Lucas Waldron.