

The Full Story of the Stunning RSA Hack Can Finally Be Told

wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/

Andy Greenberg

May 20, 2021



Amid all the sleepless hours that Todd Leetham spent hunting ghosts inside his company’s network in early 2011, the experience that sticks with him most vividly all these years later is the moment he caught up with them. Or almost did.

It was a spring evening, he says, three days—maybe four, time had become a blur—after he had first begun tracking the hackers who were rummaging through the computer systems of RSA, the corporate security giant where he worked. Leetham—a bald, bearded, and curmudgeonly analyst one coworker described to me as a “carbon-based hacker-finding machine”—had been glued to his laptop along with the rest of the company’s incident response team, assembled around the company’s glass-encased operations center in a nonstop, 24-hours-a-day hunt. And with a growing sense of dread, Leetham had finally traced the intruders’ footprints to their final targets: the secret keys known as “seeds,” a collection of numbers that represented a foundational layer of the security promises RSA made to its customers, including tens of millions of users in government and military agencies, defense contractors, banks, and countless corporations around the world.

This article appears in the July/August 2021 issue. [Subscribe to WIRED.](#)

Photograph: Djeneba Aduayom

RSA kept those seeds on a single, well-protected server, which the company called the “seed warehouse.” They served as a crucial ingredient in one of RSA's core products: SecurID tokens—little fobs you carried in a pocket and pulled out to prove your identity by entering the six-digit codes that were constantly updated on the fob's screen. If someone could steal the seed values stored in that warehouse, they could potentially clone those SecurID tokens and silently break the two-factor authentication they offered, allowing hackers to instantly bypass that security system anywhere in the world, accessing anything from bank accounts to national security secrets.

Now, staring at the network logs on his screen, it looked to Leetham like these keys to RSA's global kingdom had already been stolen.

Leetham saw with dismay that the hackers had spent nine hours methodically siphoning the seeds out of the warehouse server and sending them via file-transfer protocol to a hacked server hosted by Rackspace, a cloud-hosting provider. But then he spotted something that gave him a flash of hope: The logs included the stolen username and password for that hacked server. The thieves had left their hiding place wide open, in plain sight. Leetham connected to the faraway Rackspace machine and typed in the stolen credentials. And there it was: The server's directory still contained the entire pilfered seed collection as a compressed .rar file.

Using hacked credentials to log into a server that belongs to another company and mess with the data stored there is, Leetham admits, an unorthodox move at best—and a violation of US hacking laws at worst. But looking at RSA's stolen holiest of holies on that Rackspace server, he didn't hesitate. “I was going to take the heat,” he says. “Either way, I'm saving our shit.” He typed in the command to delete the file and hit enter.

Moments later, his computer's command line came back with a response: “File not found.” He examined the Rackspace server's contents again. It was empty. Leetham's heart fell through the floor: The hackers had pulled the seed database off the server seconds before he was able to delete it.

After hunting these data thieves day and night, he had “taken a swipe at their jacket as they were running out the door,” as he says today. They had slipped through his fingers, escaping into the ether with his company's most precious information. And though Leetham didn't yet know it, those secrets were now in the hands of the Chinese military.

Content

This content can also be viewed on the site it [originates](#) from.

Listen to the full story here or on [the Curio app](#).

The RSA breach, when it became public days later, would redefine the cybersecurity landscape. The company's nightmare was a wake-up call not only for the information security industry—the worst-ever hack of a cybersecurity firm to date—but also a warning to the rest of the world. Timo Hirvonen, a researcher at security firm F-Secure, which published an outside analysis of the breach, saw it as a disturbing demonstration of the growing threat posed by a new class of state-sponsored hackers. “If a security company like RSA cannot protect itself,” Hirvonen remembers thinking at the time, “how can the rest of the world?”

The question was quite literal. The theft of the company's seed values meant that a critical safeguard had been removed from thousands of its customers' networks. RSA's SecurID tokens were designed so that institutions from banks to the Pentagon could demand a second form of authentication from their employees and customers beyond a username and password—something physical in their pocket that they could prove they possessed, thus proving their identity. Only after typing in the code that appeared on their SecurID token (a code that typically changed every 60 seconds) could they gain access to their account.

The SecurID seeds that RSA generated and carefully distributed to its customers allowed those customers' network administrators to set up servers that could generate the same codes, then check the ones users entered into login prompts to see if they were correct. Now, after stealing those seeds, sophisticated cyberspies had the keys to generate those codes without the physical tokens, opening an avenue into any account for which someone's username or password was guessable, had already been stolen, or had been reused from another compromised account. RSA had added an extra, unique padlock to millions of doors around the internet, and these hackers now potentially knew the combination to every one.

This past December, when it became public that the company SolarWinds was hacked by Russian spies, the world woke up to the notion of a “supply chain attack”: a technique in which an adversary compromises a point of vulnerability in a software or hardware supplier positioned upstream from—and out of sight of—its target, a blind spot in the victim's view of their cybersecurity risks. The Kremlin operatives who hacked SolarWinds hid espionage code in an IT management tool called Orion, used by as many as 18,000 companies and institutions globally.

Using the SolarWinds supply chain compromise, Russia's foreign intelligence agency, known as the SVR, penetrated deep into at least nine US federal agencies, including the State Department, the US Treasury, the Department of Justice, and NASA. In another world-shaking supply chain attack just a few years earlier, Russia's military intelligence agency, known as the GRU, hijacked a piece of obscure Ukrainian accounting software to push out a data-destroying worm known as NotPetya, inflicting \$10 billion in damage worldwide in the worst cyberattack in history.

For those with a longer memory, though, the RSA breach was the original massive supply chain attack. State cyberspies—who were later revealed to be working in the service of China's People's Liberation Army—penetrated infrastructure relied on across the globe to

protect the internet. And in doing so, they pulled the rug out from under the entire world's model of digital security. "It opened my eyes to supply chain attacks," says Mikko Hypponen, chief research officer at F-Secure, who worked with Hirvonen on the company's analysis of the RSA breach. "It changed my view of the world: the fact that, if you can't break into your target, you find the technology that they use and break in there instead."

In the decade that followed, many key RSA executives involved in the company's breach have held their silence, bound by 10-year nondisclosure agreements. Now those agreements have expired, allowing them to tell me their stories in new detail. Their accounts capture the experience of being targeted by sophisticated state hackers who patiently and persistently take on their most high-value networked targets on a global scale, where an adversary sometimes understands the interdependencies of its victims' systems better than victims do themselves, and is willing to exploit those hidden relationships.

After 10 years of rampant state-sponsored hacking and supply chain hijacks, the RSA breach can now be seen as the herald of our current era of digital insecurity—and a lesson about how a determined adversary can undermine the things we trust most.

On March 8, 2011, a brisk late-winter day, Todd Leetham finished a smoke break and was walking back into RSA's headquarters in Bedford, Massachusetts—a pair of connected buildings on the edge of a forest in the Boston suburbs—when a systems administrator pulled him aside and asked him to take a look at something strange.

The admin had noticed that one user had accessed a server from a PC that the user didn't typically work on, and that the permissions setting on the account seemed unusual. A technical director investigating the anomalous login with Leetham and the admin asked Bill Duane, a veteran RSA engineer, to take a look. To Duane, who was busy working on a cryptographic algorithm at the time, the anomaly hardly looked like cause for alarm. "I frankly thought this administrator was crazy," he remembers. "Fortunately he was stubborn enough to insist that something was wrong."

Leetham and the company's security incident responders started to trace the aberrant behavior and analyze the forensics of every machine the anomalous account had touched. They began to see more telltale oddities in employees' credentials, stretching back days. The admin had been right. "Sure enough," Duane says, "this was the tip of the iceberg."

Over the next several days, the security team at RSA's security operations center—a NASA-style control room with rows of desks and monitors covering one wall—meticulously traced the interlopers' fingerprints. The RSA staffers began putting in nearly 20-hour workdays, driven by the chilling knowledge that the breach they were tracking was still unfolding. Management demanded updates on their findings every four hours, day or night.

The analysts eventually traced the origin of the breach to a single malicious file that they believed had landed on an RSA employee's PC five days before they'd started their hunt. A staffer in Australia had received an email with the subject line "2011 Recruitment plan" and an Excel spreadsheet attached to it. He'd opened it. Inside the file was a script that exploited a zero-day vulnerability—a secret, unpatched security flaw—in Adobe Flash, planting a common piece of malicious software called Poison Ivy on the victim's machine.

That initial point of entry onto RSA's network, F-Secure's Hirvonen would later point out in his own analysis, wasn't particularly sophisticated. A hacker wouldn't have even been able to exploit the Flash vulnerability if the victim had been running a more recent version of Windows or Microsoft Office, or if he'd had limited access to install programs on his PC—as most security administrators for corporate and government networks recommend, Hirvonen says.

But it was from this ingress that the RSA analysts say the intruders began to demonstrate their real abilities. In fact, several RSA executives came to believe that at least two groups of hackers were in their network simultaneously—one highly skilled group exploiting the other's access, perhaps, with or without their knowledge. "There's the trail through the woods that the first one left, and right in the middle of it, branching off, is the second trail," says Sam Curry, who was RSA's chief security officer at the time. "And that second attack was much more skilled."

On that Australian employee's PC, someone had used a tool that pulled credentials out of the machine's memory and then reused those usernames and passwords to log into other machines on the network. They'd then scraped those computers' memories for more usernames and passwords—finding some that belonged to more privileged administrators. The hackers eventually got to a server containing hundreds of users' credentials. Today that credential-stealing hopscotching technique is common. But in 2011 the analysts were surprised to see how the hackers fanned out across the network. "It was really just the most brutal way to blow through our systems that I'd ever seen," Duane says.

Breaches as extensive as the one carried out against RSA are often discovered months after the fact, when the intruders are long gone or lying dormant. But Duane says that the 2011 incident was different: Within days, the investigators had essentially caught up to the intruders and were watching them in action. "They'd try to get into a system, then we'd detect them a minute or two later and go in and shut down that system or disable access to it," Duane says. "We were fighting them tooth and nail, in real time."

It was in the midst of that feverish chase that Leetham caught the hackers stealing what he still believes was their highest-priority target: the SecurID seeds.

RSA executives told me that the part of their network responsible for manufacturing the SecurID hardware tokens was protected by an "air gap"—a total disconnection of computers from any machine that touches the internet. But in fact, Leetham says, one server on RSA's

internet-connected network was linked, through a firewall that allowed no other connections, to the seed warehouse on the manufacturing side. Every 15 minutes, that server would pull off a certain number of seeds so that they could be encrypted, written to a CD, and given to SecurID customers. That link was necessary; it allowed RSA's business side to help customers set up their own server that could then check users' six-digit code when it was typed into a login prompt. Even after the CD was shipped to a client, those seeds remained on the seed warehouse server as a backup if the customer's SecurID server or its setup CD were somehow corrupted.

Now, instead of the usual once-every-15-minutes connections, Leetham saw logs of thousands of continuous requests for data every second. What's more, the hackers had been collecting those seeds on not one but three compromised servers, relaying requests through the one connected machine. They had packaged up the collection of seeds in three parts, moved them off to the faraway Rackspace server, and then recombined them into what appeared to be the full database of every seed RSA had stored in the seed warehouse. "I was like, 'Wow,'" Leetham says. "I kind of admired it. But at the same time: 'Oh crap.'"

As it dawned on Leetham that the seed collection had likely been copied—and after he had made his seconds-too-late attempt to delete the data off the hackers' server—the enormity of the event hit him: The trust that customers placed in RSA, perhaps its most valuable commodity, was about to be obliterated. "This is an extinction event," he remembers thinking. "RSA is over."

It was late at night when the security team learned that the seed warehouse had been plundered. Bill Duane made the call: They would physically cut off as many of RSA's network connections as necessary to limit the damage and stop any further theft of data. They hoped, in particular, to protect any customer information that mapped to the seeds, and which might be necessary for the hackers to exploit them. (Some RSA staff also suggested to me that the seeds had been stored in an encrypted state, and cutting off network connections was intended to prevent the hackers from stealing the key necessary to decrypt them.) Duane and an IT manager walked into the data center and started unplugging Ethernet cables one by one, severing the company's connections to its manufacturing facility, parts of its network that handled core business processes like customer orders, even its website. "I basically shut off RSA's business," he says. "I crippled the company in order to stop any potential further release of data."

The next day, RSA's CEO, Art Coviello, was in a meeting in the conference room that adjoined his office, preparing a public statement about the ongoing breach. Coviello had been getting updates since the intrusions were discovered. As the extent of the breach had grown, he'd canceled a business trip to Brazil. But he'd remained relatively sanguine. After all, it didn't sound like the hackers had breached any credit card data or other sensitive customer information. They'd kick out the hackers, he figured, post their statement, and get on with business.

But in the middle of the meeting, he remembers, a marketing executive at the table with him looked at her phone and murmured, “Oh dear.”

Coviello asked her what was wrong. She demurred. He took the phone out of her hand and read the message. It said that Bill Duane was coming up to Coviello’s office; he wanted to update the CEO in person. When he got upstairs, he delivered the news: The hackers had reached the SecurID seeds. “I felt like a cannonball had been shot through my stomach,” Coviello says.

In the hours that followed, RSA’s executives debated how to go public. One person in legal suggested they didn’t actually need to tell their customers, Sam Curry remembers. Coviello slammed a fist on the table: They would not only admit to the breach, he insisted, but get on the phone with every single customer to discuss how those companies could protect themselves. Joe Tucci, the CEO of parent company EMC, quickly suggested they bite the bullet and replace all 40 million-plus SecurID tokens. But RSA didn’t have nearly that many tokens available—in fact, the breach would force it to shut down manufacturing. For weeks after the hack, the company would only be able to restart production in a diminished capacity.

As the recovery effort got under way, one executive suggested they call it Project Phoenix. Coviello immediately nixed the name. “Bullshit,” he remembers saying. “We’re not rising from the ashes. We’re going to call this project Apollo 13. We’re going to land the ship without injury.”

At 7:00 the next morning, March 17, RSA’s head of North American sales, David Castignola, finished up an early workout on a treadmill at his local gym in Detroit. When he picked up his phone, he saw that he had missed no fewer than 12 calls—all from just that morning, and all from RSA’s president, Tom Haiser. RSA, Haiser’s voicemails said, was about to announce a major security breach. He needed to be in the building.

A few hours and a last-minute flight later, Castignola literally ran into RSA’s headquarters in Bedford and up to the fourth-floor conference room. He immediately noticed the pale, drawn faces of the staff who had been dealing with the unfolding crisis for more than a week. “Every little indicator I got was: This is worse than I can even get my head around,” Castignola remembers.

That afternoon, Coviello published an open letter to RSA’s customers on the company’s website. “Recently, our security systems identified an extremely sophisticated cyberattack in progress,” the letter read. “While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack,” the letter continued—somewhat downplaying the crisis.

In Bedford, Castignola was given a conference room and the authority to ask for as many volunteers from the company as he needed. A rotating group of nearly 90 staffers began the weeks-long, day-and-night process of arranging one-on-one phone calls with every customer. They worked from a script, walking customers through protective measures like adding or lengthening a PIN number as part of their SecurID logins, to make them harder for hackers to replicate. Castignola remembers walking down the halls of the building at 10 pm and hearing calls on speaker phones behind every closed door. In many cases customers were shouting. Castignola, Curry, and Coviello each did hundreds of those calls; Curry began to joke that his title was “chief apology officer.”

At the same time, paranoia was beginning to take hold in the company. The first night after the announcement, Castignola remembers walking by a wiring closet and seeing an absurd number of people walking out of it, far more than he imagined could have ever fit. “Who are those people?” he asked another nearby executive. “That’s the government,” the executive responded vaguely.

In fact, by the time Castignola had landed in Massachusetts, both the NSA and the FBI had been called to help the company’s investigation, as had defense contractor Northrop Grumman and incident response firm Mandiant. (By chance, employees of Mandiant had already been on-site prior to the breach, installing security sensor equipment on RSA’s network.)

RSA staff began to take drastic measures. Worried that their phone system might be compromised, the company switched carriers, moving from AT&T to Verizon phones. Executives, not trusting even the new phones, held meetings in person and shared paper copies of documents. The FBI, fearing an accomplice in RSA’s ranks because of the apparent level of knowledge the intruders seemed to have of company systems, started doing background checks. “I made sure that all members of the team—I don’t care who they were, what reputation they had—were investigated, because you have to be sure,” Duane says.

The windows of some executives’ offices and conference rooms were covered in layers of butcher paper, to prevent laser microphone surveillance—a long-distance eavesdropping technique that picks up conversations from vibrations in window panes—by imagined spies in the surrounding woods. The building was swept for bugs. Multiple executives insisted that they did find hidden listening devices—though some were so old that their batteries were dead. It was never clear if those bugs had any relation to the breach.

Meanwhile, RSA’s security team and the investigators brought in to help were “tearing the house down to the studs,” as Curry put it. In every part of the network that the hackers touched, he says, they scrubbed the contents of potentially compromised machines—and even ones adjacent to them. “We physically went around and, if there was a box they were on, it got wiped,” Curry says. “If you lost data, too bad.”

In late May 2011, about two months after the breach announcement, RSA was still recovering, rebuilding, and apologizing to customers when it was hit with an aftershock: A post appeared on the influential tech blogger Robert X. Cringely's website, titled "InsecureID: No More Secrets?"

The post was based on a tip from a source inside a major defense contractor, who'd told Cringely that the company was responding to an extensive intrusion by hackers who seemed to have used stolen RSA seed values to get in. Everyone at the defense contractor was having their RSA tokens replaced. Suddenly RSA's breach seemed far more severe than the company's original announcement had described it. "Well it didn't take long for whoever cracked RSA to find a lock to fit that key," Cringely wrote. "What if every RSA token has been compromised, everywhere?"

Two days later, Reuters revealed the name of the hacked military contractor: Lockheed Martin, a company that represented a cornucopia of ultra-secret plans for weapons and intelligence technologies. "The scab was healing," Castignola says. "Then Lockheed hit. That was like a mushroom cloud. We were back at it again."

In the days that followed, defense contractors Northrop Grumman and L-3 were also named in news reports. Hackers with SecurID's seed values had targeted them too, the stories said, though it was never clear how deeply the intruders had penetrated the companies. Nor was it revealed what the hackers had accessed inside Lockheed Martin. The company claimed it had prevented the spies from stealing sensitive information like customer data or classified secrets.

In another open letter to customers in early June 2011, RSA's Art Coviello admitted, "We were able to confirm that information taken from RSA in March had been used as an element of an attempted broader attack on Lockheed Martin, a major US government defense contractor."

Today, with 10 years of hindsight, Coviello and other former RSA executives tell a story that starkly contradicts accounts from the time: Most of the former RSA staff who spoke to me claim that it was never proven that SecurID had any role in the Lockheed breach. Coviello, Curry, Castignola, and Duane all argued that it was never confirmed that the intruders inside RSA's systems had successfully stolen the full list of seed values in an uncorrupted, unencrypted form, nor the customer list mapped to those seeds necessary to exploit them. "I don't think that Lockheed's attack was related to us at all," Coviello states flatly.

By contrast, in the years since 2011, Lockheed Martin has detailed how hackers used information stolen in RSA's SecurID breach as a stepping stone to penetrate its network—even as it insists that no information was successfully stolen in that event. A Lockheed source with knowledge of the company's incident response reaffirmed to WIRED the company's original claims. "We stand by our forensic investigation findings," the source says. "Our analysis determined the breach of our two-factor authentication token provider was a

direct contributing factor in the attack on our network, a fact that has been widely reported by the media and acknowledged publicly by our vendor, including Art.” In fact, the Lockheed source says the company saw the hackers entering SecurID codes in real time, confirmed that the targeted users hadn’t lost their tokens, and then, after replacing those users’ tokens, watched the hackers continue to unsuccessfully enter codes from the old tokens.

The NSA, for its part, has never had much doubt about RSA’s role in subsequent break-ins. In a [briefing to the Senate Armed Services Committee](#) a year after the RSA breach, NSA’s director, General Keith Alexander, said that the RSA hack “led to at least one US defense contractor being victimized by actors wielding counterfeit credentials,” and that the Department of Defense had been forced to replace every RSA token it used.

In the hearing, Alexander went on to pin those attacks, vaguely, on an increasingly common culprit: China. [The New York Times](#) and the [security firm Mandiant](#) would later publish a groundbreaking exposé on a Chinese state hacker group that Mandiant had named APT1. The group was believed to be People’s Liberation Army Unit 61398, based on the outskirts of Shanghai. Among its dozens of targets over the previous five years: the governments of the United States, Canada, South Korea, Taiwan, Vietnam; and the United Nations—and RSA.

After those reports became public, Bill Duane printed out a picture of the hackers’ headquarters, a 12-story white building off of Shanghai’s Datong Road. He taped it to a dartboard in his office.

I asked Duane, who retired from RSA in 2015 after more than 20 years at the company, at what point he considered RSA’s breach truly over: Was it the morning after he made the lonely decision to unplug a chunk of the company’s network? Or when the NSA, the FBI, Mandiant, and Northrop had wrapped up and left? “Our view was that the attack wasn’t ever over,” he responds. “We knew that they left backdoors, that they’re always going to be able to break in, that the attacker can, with their resources, get in when they want to get in.”

Duane’s harrowing experience in response to the intrusion taught him—and perhaps should teach all of us—that “every network is dirty,” as he puts it. Now he preaches to companies that they should segment their systems and cordon off their most sensitive data so that it remains impenetrable even to an adversary that’s already inside the firewall.





As for Todd Leetham, he watched the SolarWinds fiasco unfold over the past six months with a grim sense of *déjà vu*. “Everybody was shocked. But in hindsight, well, duh, it was kind of everywhere,” he says of SolarWinds. As was, by analogy, SecurID, 10 years earlier.

Leetham sees the lessons of RSA’s supply chain compromise in starker terms than even his colleague Bill Duane: It was “a glimpse of just how fragile the world is,” he says. “It’s a house of cards during a tornado warning.”

SolarWinds demonstrated how precarious this structure remains, he argues. As Leetham sees it, the security world blindly put its trust in something that existed outside its threat model, never imagining that an adversary might attack it. And once again, the adversary pulled out a supporting card underpinning the house's foundation—one that had been confused for solid ground.

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

More Great WIRED Stories

-  The latest on tech, science, and more: [Get our newsletters!](#)
- The Arecibo Observatory was like family. [I couldn't save it](#)
- It's true. Everyone *is* [multitasking in video meetings](#)
- This is your [brain under anesthesia](#)
- The best personal safety [devices, apps, and alarms](#)
- Ransomware's dangerous new trick: [double-encrypting data](#)
-  Explore AI like never before with [our new database](#)
-  WIRED Games: Get the latest [tips, reviews, and more](#)
-  Want the best tools to get healthy? Check out our Gear team's picks for the [best fitness trackers, running gear](#) (including [shoes](#) and [socks](#)), and [best headphones](#)