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

By Andy Greenberg

Published: 2021-05-20 · Archived: 2026-05-01 02:45:36 UTC

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.

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.

---