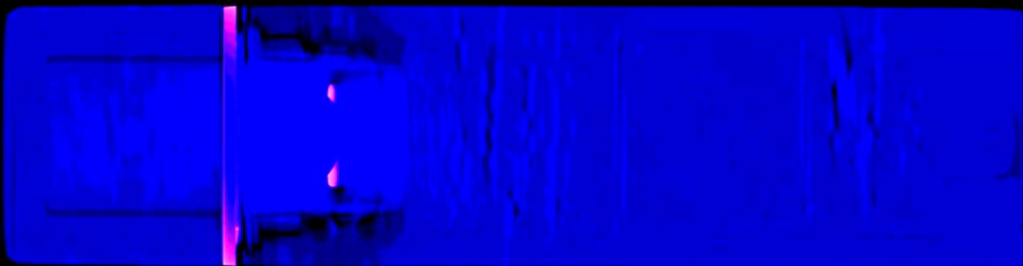


BY ANDY GREENBERG

Stefan Thomas lost the password to an encrypted USB drive holding 7,002 bitcoins. One team of hackers believes they can unlock it—if they can get Thomas to let them.



II

VIDEO: UNCIPHERED

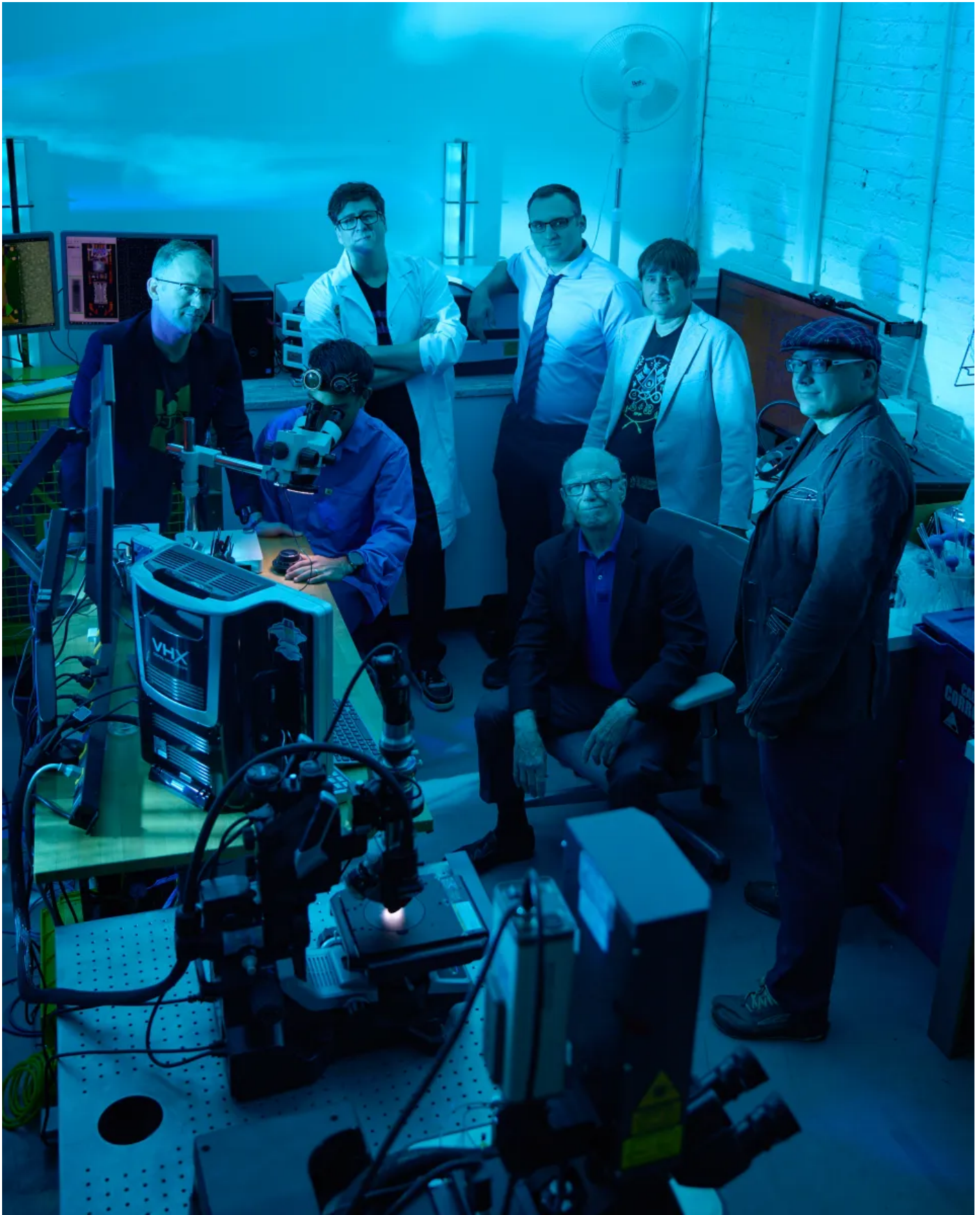


SAVE

AT 9:30 AM on a Wednesday in late September, a hacker who asked to be called Tom Smith sent me a nonsensical text message: “query voltage recurrence.”

Those three words were proof of a remarkable feat—and potentially an extremely valuable one. A few days earlier, I had randomly generated those terms, set them as

the passphrase on a certain model of encrypted USB thumb drive known as an IronKey S200, and shipped the drive across the country to Smith and his teammates in the Seattle lab of a startup called Unciphered.



Unciphered's staff in the company's Seattle lab. PHOTOGRAPH: MERON MENGHISTAB

Smith had told me that guessing my passphrase might take several days. Guessing it at all, in fact, should have been impossible: IronKeys are designed to permanently

erase their contents if someone tries just 10 incorrect password guesses. But Unciphered's hackers had developed a secret IronKey password-cracking technique—one that they've still declined to fully describe to me or anyone else outside their company—that gave them essentially infinite tries. My USB stick had reached Unciphered's lab on Tuesday, and I was somewhat surprised to see my three-word passphrase texted back to me the very next morning. With the help of a high-performance computer, Smith told me, the process had taken only 200 trillion tries.

Smith's demonstration was not merely a hacker party trick. He and Unciphered's team have spent close to eight months developing a capability to crack this specific, decade-old model of IronKey for a very particular reason: They believe that in a vault in a Swiss bank 5,000 miles to the east of their Seattle lab, an IronKey that's just as vulnerable to this cracking technique holds the keys to 7,002 bitcoins, worth close to \$235 million at current exchange rates.

For years, Unciphered's hackers and many others in the crypto community have followed the story of a Swiss crypto entrepreneur living in San Francisco named Stefan Thomas, who owns this 2011-era IronKey, and who has lost the password to unlock it and access the nine-figure fortune it contains. Thomas has said in interviews that he's already tried eight incorrect guesses, leaving only two more tries before the IronKey erases the keys stored on it and he loses access to his bitcoins forever.

Screens in Unciphered's lab show a microscopic image of the layout of the IronKey's controller chip (left) and a CT scan of the drive. PHOTOGRAPH: MERON MENGHISTAB

Now, after months of work, Unciphered's hackers believe they can open Thomas' locked treasure chest, and they're ready to use their secret cracking technique to do it. “We were hesitant to reach out to him until we had a full, provable, reliable attack,” says Smith, who asked WIRED not to reveal his real name due to the

sensitivities of working with secret hacking techniques and very large sums of cryptocurrency. “Now we’re in that place.”

The only problem: Thomas doesn't seem to want their help.

Earlier this month, not long after performing their USB-decrypting demonstration for me, Unciphered reached out to Thomas through a mutual associate who could vouch for the company’s new IronKey-unlocking abilities and offer assistance. The call didn't even get as far as discussing Unciphered's commission or fee before Thomas politely declined.

Thomas had already made a “handshake deal” with two other cracking teams a year earlier, he explained. In an effort to prevent the two teams from competing, he had offered each a portion of the proceeds if either one could unlock the drive. And he remains committed, even a year later, to giving those teams more time to work on the problem before he brings in anyone else—even though neither of the teams has shown any sign of pulling off the decryption trick that Unciphered has already accomplished.

That has left Unciphered in a strange situation: It holds what is potentially one of the most valuable lockpicking tools in the cryptocurrency world, but with no lock to pick. “We cracked the IronKey,” says Nick Fedoroff, Unciphered's director of operations. “Now we have to crack Stefan. This is turning out to be the hardest part.”

In an email to WIRED, Thomas confirmed that he had turned down Unciphered's offer to unlock his encrypted fortune. “I have already been working with a different set of experts on the recovery so I'm no longer free to negotiate with someone new,” Thomas wrote. “It's possible that the current team could decide to subcontract Unciphered if they feel that's the best option. We'll have to wait and see.” Thomas declined to be interviewed or to comment further.

A Very Valuable, Worthless USB Stick

In past interviews, Thomas has said that his 7,002 bitcoins were left over from a payment he received for making a video titled “What is Bitcoin?” that published on YouTube in early 2011, when a bitcoin was worth less than a dollar. Later that year, he told WIRED that he'd inadvertently erased two backup copies of the wallet that held those thousands of coins, and then lost the piece of paper with the password to decrypt the third copy, stored on the IronKey. By then, his lost coins were worth close to \$140,000. “I spent a week trying to recover it,” he said at the time. “It was pretty painful.”

In the 12 years since, the value of the inaccessible coins on Thomas' IronKey has at times swelled to be worth nearly half a billion dollars, before settling to its current, still-staggering price. In January 2021, as Bitcoin began to approach its peak exchange rate, Thomas described to *The New York Times* the angst that his long-lost hoard had caused him over the years. “I would just lay in bed and think about it,” he said. “Then I would go to the computer with some new strategy, and it wouldn’t work, and I would be desperate again.”

Around that same time in 2021, a team of cryptographers and white-hat hackers founded Unciphered with the goal of unlocking exactly the sort of vast, frozen funds that many unlucky crypto holders like Thomas have long since given up on. At the time of Unciphered’s official launch, the cryptocurrency tracing firm Chainalysis estimated the total sum of those forgotten wallets across blockchains to be worth \$140 billion. Unciphered says it has since successfully helped clients open locked wallets worth “many millions” of dollars—often through novel cryptographic vulnerabilities or software flaws it has discovered in cryptocurrency wallets—though nothing close to the size of Thomas' IronKey stash.

A deconstructed IronKey inside of Unciphered’s laser cutting tool. PHOTOGRAPH: MERON MENGHISTAB

Only around the beginning of 2023 did Unciphered begin to hunt for potential avenues to unlock Thomas' IronKey prize. Smith says that they quickly started to see

hints that the IronKey's manufacturer, which was sold to storage hardware firm iMation in 2011, had left them some potential openings. “We were seeing little bits and pieces,” Smith says. “Like, this looks a little sloppy, or this looks not quite like how someone should be doing things.” (Kingston Storage, which now owns IronKey, didn’t respond to WIRED’s request for comment.)

Even a decade-old IronKey is a daunting target for hackers. The USB stick, whose development was funded in part by the United States Department of Homeland Security, is FIPS-140-2 Level 3 certified, meaning it's tamper-resistant and its encryption is secure enough for use by military and intelligence agencies for classified information. But emboldened by the few hints of security flaws they'd found—and still with no participation from Thomas—Unciphered's founders decided to take on the project of cracking it. “If there is an Everest to attempt, this is it,” Fedoroff remembers telling the team. The company's founders would eventually pull together a group of around 10 staffers and outside consultants, several of whom had backgrounds at the National Security Agency or other three-letter government agencies. They called it Project Everest.

A \$235 Million Treasure Hunt

One of their first moves was to determine the exact model of IronKey that Thomas must have used, based on timing and a process of elimination. Then they bought the entire supply of that decade-plus-old model that they could find available for sale online, eventually amassing hundreds of them in their lab.

To fully reverse engineer the device, Unciphered scanned an IronKey with a CT scanner, then began the elaborate surgery necessary to deconstruct it. Using a precise laser cutting tool, they carved out the Atmel chip that serves as the USB stick's “secure enclave” holding its cryptographic secrets. They bathed that chip in nitric acid to “decap” it, removing the layers of epoxy designed to prevent tampering. They then began to polish down the chip, layer by layer, with an abrasive silica solution and a tiny spinning felt pad, removing a fraction of a micron of material from its surface at a time, taking photos of each layer with either optical microscopes or scanning electron microscopes, and repeating the process until they could build a full 3D model of the processor.

Because the chip's read-only memory, or ROM, is built into the layout of its physical wiring for better efficiency, Unciphered's visual model gave it a head start toward deciphering much of the logic of the IronKey's cryptographic algorithm. But the team went much further, attaching tenth-of-a-millimeter gauge wires to the secure element’s connections to “wiretap” the communications going into and out of it.

They even tracked down engineers who had worked on the Atmel chip and another microcontroller in the IronKey that dated back to the 1990s to quiz them for details about the hardware. “It felt very much like a treasure hunt,” says Fedoroff. “You’re following a map that’s faded and coffee-stained, and you know there’s a pot of gold at the end of a rainbow, but you have no idea where that rainbow’s leading.”

That cracking process culminated in July, when Unciphered's team gathered at an Airbnb in San Francisco. They describe standing around a table covered with millions of dollars’ worth of lab equipment when a member of the team read out the contents of a decrypted IronKey for the first time. “What just happened?” Fedoroff asked the room. “We just summited Everest,” said Unciphered's CEO, Eric Michaud.

Unciphered still won't reveal its full research process, or any details of the technique it ultimately found for cracking the IronKey and defeating its “counter” that limits password guesses. The company argues that the vulnerabilities they discovered are still potentially too dangerous to be made public, given that the model of IronKeys it cracked are too old to be patched with a software update, and some may still store classified information. “If this were to leak somehow, there would be much bigger national security implications than a cryptocurrency wallet,” Fedoroff says.

The team notes that the final method they developed doesn't require any of the invasive or destructive tactics that they used in their initial research. They've now unlocked 2011-era IronKeys—without destroying them—more than a thousand times, they say, and unlocked three IronKeys in demonstrations for WIRED.

Cryptic Contracts

None of that, however, has gotten them any closer to persuading Stefan Thomas to let them crack *his* IronKey. Unciphered’s hackers say they learned from the intermediary who contacted Thomas on their behalf that Thomas has already been in touch with two other potential players in the crypto- and hardware-hacking world to help unlock his USB stick: the cybersecurity forensics and investigations firm Naxo, and the independent security researcher Chris Tarnovsky.

Naxo declined WIRED’s request to comment. But Chris Tarnovsky, a renowned chip reverse engineer, confirmed to WIRED that he had a “meet-and-greet” call with Thomas in May of last year. Tarnovsky says that, in the meeting, Thomas had told him that if he could successfully unlock the IronKey, he would be “generous,” but didn't specify a fee or commission. Since then, Tarnovsky says that he has done very little work on the project, and that he has essentially been waiting for Thomas to start paying him on a monthly basis for initial research. “I want Stefan to cough up some

money up front," says Tarnovsky. "It's a lot of work, and I need to worry about my mortgage and my bills."

But Tarnovsky says he hasn't heard from Thomas since that first call. "Nothing came out of it," he says. "It's weird."

Unciphered's director of operations Nick Fedoroff. PHOTOGRAPH: MERON MENGHISTAB

Unciphered's team remains skeptical about Naxo's progress and whether it's any further along than Tarnovsky. There are only a small number of hardware hackers capable of the reverse engineering necessary to crack the IronKey, they argue, and none appear to be working with Naxo. As for Thomas' suggestion that they could subcontract to Naxo or another team working on the project, Unciphered's Fedoroff says he won't rule it out, but argues it doesn't make sense when Unciphered alone can crack the IronKey. "Based on what we know, we don't see any benefit to anyone in going that route," Fedoroff says.

Thomas, meanwhile, seems to display an unusual lack of urgency in unlocking his \$235 million, and has offered only vague hints about why he has yet to reveal any progress toward that goal. "When you're dealing with so much money, everything takes forever," he told the *Thinking Crypto* podcast in an [interview](#) over the summer. "The person you're working with, you need some contract with them, and that contract needs to be rock solid, because if there's some issue with the contract, there's suddenly hundreds of millions of dollars at stake."

To potentially accelerate that cryptic contract process, Unciphered plans to publish an open letter to Thomas and a video in the coming days designed to persuade—or pressure—Thomas into working with them. But Fedoroff concedes that it's possible Thomas doesn't actually care about the money: In its piece about his locked coins in

2021, *The New York Times* wrote that Thomas already had “more riches than he knows what to do with,” thanks to other crypto ventures.

Fedoroff notes that it's impossible to know for certain what Thomas' IronKey holds. Maybe the keys to the 7,002 bitcoins are held elsewhere, or gone altogether.

Science

Your weekly roundup of the best stories on health care, the climate crisis, genetic engineering, robotics, space, and more. Delivered on Wednesdays.

Your email

Enter your email


SUBMIT

By signing up you agree to our [User Agreement](#) (including the [class action waiver and arbitration provisions](#)), our [Privacy Policy & Cookie Statement](#) and to receive marketing and account-related emails from WIRED. You can unsubscribe at any time. This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

He says Unciphered is still hopeful. But the team is also ready to move on if Thomas won't work with them. There are, after all, other locked wallets out there for the company to crack. And the decision of whether and how to unlock this particular USB drive's riches will ultimately fall to its owner alone. “It's incredibly frustrating,” says Fedoroff. “But when you're dealing with people, that's always the most complex part. Code doesn't change unless you tell it to. Circuitry doesn't either. But humans are incredibly unpredictable creatures.”

Updated 10:55 am ET, October 24, 2023, to correct a misspelling of Nick Fedoroff's surname.

You Might Also Like ...

-  Make the most of chatbots with our [AI Unlocked newsletter](#)
- How [citizen surveillance](#) ate San Francisco
- [Why Teslas totaled in the US](#) are mysteriously reincarnated in Ukraine
- This is the ops manual for the most [tech-savvy animal liberation group](#) in the US
- Netflix killed *The OA*. [Now its creators are back](#) with a show about tech's ubiquity
- Will life be better [in the metaverse](#)?

-  Charge right into travel season with the best [travel adapters](#), [power banks](#), and [USB hubs](#)



[Andy Greenberg](#) is a senior writer for WIRED, covering hacking, cybersecurity and surveillance. He's the author of the new book [Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency](#). His last book was [\[*\]Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most...](#) [Read more](#)

SENIOR WRITER



TOPICS

[BITCOIN](#)

[HACKS](#)

[CRYPTOCURRENCY](#)

[CYBERSECURITY](#)

[ENCRYPTION](#)

MORE FROM WIRED

The Startup That Transformed the Hack-for-Hire Industry

Plus: The FBI's baffling inaction on a ransomware group, a massive breach of Danish electric utilities, and more.

This Cheap Hacking Device Can Crash Your iPhone With Pop-Ups

Plus: SolarWinds is charged with fraud, New Orleans police face recognition has flaws, and new details about Okta's October data breach emerge.

MATT BURGESS

Apple, Google, and Microsoft Just Patched Some Spooky Security Flaws

Plus: Major vulnerability fixes are now available for a number of enterprise giants, including Cisco, VMWare, Citrix, and SAP.

KATE O'FLAHERTY

Google's Ad Blocker Crackdown Is Growing

Plus: North Korean supply chain attacks, a Russian USB worm spreads internationally, and more.

MATT BURGESS

Running Signal Will Soon Cost \$50 Million a Year

Signal’s president reveals the cost of running the privacy-preserving platform—not just to drum up donations, but to call out the for-profit surveillance business models it competes against.

ANDY GREENBERG

OpenAI’s Custom Chatbots Are Leaking Their Secrets

Released earlier this month, OpenAI’s GPTs let anyone create custom chatbots. But some of the data they’re built on is easily exposed.

MATT BURGESS

Google's New Titan Security Key Adds Another Piece to the Password-Killing Puzzle

The new generation of hardware authentication key includes support for cryptographic passkeys as Google pushes adoption of the more secure login alternative.

LILY HAY NEWMAN

Sandworm Hackers Caused Another Blackout in Ukraine—During a Missile Strike

Russia's most notorious military hackers successfully sabotaged Ukraine's power grid for the third time last year. And in this case, the blackout coincided with a physical attack.

ANDY GREENBERG

WIRED

Get 1 year for
~~\$29.99~~ \$5

SUBSCRIBE