PHOTOGRAPH: RAMONA ROSALES

ANDY GREENBERG SECURITY 05.12.2020 06:00 AM

The Confessions of Marcus Hutchins, the Hacker Who Saved the Internet

At 22, he single-handedly put a stop to the worst cyberattack the world had ever seen. Then he was arrested by the FBI. This is his untold story.

AT AROUND 7 am on a quiet Wednesday in August 2017, Marcus Hutchins walked out the front door of the Airbnb mansion in Las Vegas where he had been partying for the past week and a half. A gangly, 6'4", 23-year-old hacker with an explosion of blond-brown curls, Hutchins had emerged to retrieve his order of a Big Mac and fries from an Uber Eats deliveryman. But as he stood barefoot on the mansion's driveway wearing only a T-shirt and jeans, Hutchins noticed a black SUV parked on the street—one that looked very much like an FBI stakeout.

He stared at the vehicle blankly, his mind still hazed from sleep deprivation and stoned from the legalized Nevada weed he'd been smoking all night. For a fleeting moment, he wondered: Is this finally it?

June 2020. Subscribe to

But as soon as the thought surfaced, he dismissed it. The FBI would never be so obvious, he told himself. His feet had begun to scald on the griddle of the driveway. So he grabbed the McDonald's bag and headed back inside, through the mansion's courtyard, and into the pool house he'd been using as a bedroom. With the specter of the SUV fully exorcised from his mind, he rolled

WIRED. PHOTOGRAPH: RAMONA ROSALES

another spliff with the last of his weed, smoked it as he ate his burger, and then packed his bags for the airport, where he was scheduled for a first-class flight home to the UK.

Hutchins was coming off of an epic, exhausting week at Defcon, one of the world's largest hacker conferences, where he had been celebrated as a hero. Less than three months earlier, Hutchins had saved the internet from what was, at the time, the worst cyberattack in history: a piece of malware called WannaCry. Just as that self-propagating software had begun exploding across the planet, destroying data on hundreds of thousands of computers, it was Hutchins who had found and triggered the secret kill switch contained in its code, neutering WannaCry's global threat immediately.

This legendary feat of whitehat hacking had essentially earned Hutchins free drinks for life among the Defcon crowd. He and his entourage had been invited to every VIP hacker party on the strip, taken out to dinner by journalists, and accosted by fans seeking selfies. The story, after all, was irresistible: Hutchins was the shy geek who had single-handedly slain a monster threatening the entire digital world, all while sitting in front of a keyboard in a bedroom in his parents' house in remote western England.

Still reeling from the whirlwind of adulation, Hutchins was in no state to dwell on concerns about the FBI, even after he emerged from the mansion a few hours later and once again saw the same black SUV parked across the street. He hopped into an Uber to the airport, his mind still floating through a cannabis-induced cloud. Court documents would later reveal that the SUV followed him along the way—that law enforcement had, in fact, been tracking his location periodically throughout his time in Vegas.

When Hutchins arrived at the airport and made his way through the security checkpoint, he was surprised when TSA agents told him not to bother taking any of his three laptops out of his backpack before putting it through the scanner. Instead, as they waved him through, he remembers thinking that they seemed to be making a special effort not to delay him.

He wandered leisurely to an airport lounge, grabbed a Coke, and settled into an armchair. He was still hours early for his flight back to the UK, so he killed time posting from his phone to Twitter, writing how excited he was to get back to his job analyzing malware when he got home. “Haven't touched a debugger in over a month now,” he tweeted. He humblebragged about some very expensive shoes his boss had bought him in Vegas and retweeted a compliment from a fan of his reverse-engineering work.

Hutchins was composing another tweet when he noticed that three men had walked up to him, a burly redhead with a goatee flanked by two others in Customs and Border Protection uniforms. “Are you Marcus Hutchins?” asked the red-haired man. When Hutchins confirmed that he was, the man asked in a neutral tone for Hutchins to come with them, and led him through a door into a private stairwell.

Then they put him in handcuffs.

In a state of shock, feeling as if he were watching himself from a distance, Hutchins asked what was going on. “We'll get to that,” the man said.

Hutchins remembers mentally racing through every possible illegal thing he'd done that might have interested Customs. Surely, he thought, it couldn't be *the thing*, that years-old, unmentionable crime. Was it that he might have left marijuana in his bag? Were these bored agents overreacting to petty drug possession?

The agents walked him through a security area full of monitors and then sat him down in an interrogation room, where they left him alone. When the red-headed man returned, he was accompanied by a small blonde woman. The two agents flashed their badges: They were with the FBI.

For the next few minutes, the agents struck a friendly tone, asking Hutchins about his education and Kryptos Logic, the security firm where he worked. For those minutes, Hutchins allowed himself to believe that perhaps the agents wanted only to learn more about his work on WannaCry, that this was just a particularly aggressive way to get his cooperation into their investigation of that world-shaking cyberattack. Then, 11 minutes into the interview, his interrogators asked him about a program called Kronos.

“Kronos,” Hutchins said. “I know that name.” And it began to dawn on him, with a sort of numbness, that he was not going home after all.

FOURTEEN YEARS EARLIER, long before Marcus Hutchins was a hero or villain to anyone, his parents, Janet and Desmond, settled into a stone house on a cattle farm in remote Devon, just a few minutes from the west coast of England. Janet was a nurse, born in Scotland. Desmond was a social worker from Jamaica who had been a firefighter when he first met Janet in a nightclub in 1986. They had moved from Bracknell, a commuter town 30 miles outside of London, looking for a place where their sons, 9-year-old Marcus and his 7-year-old brother, could grow up with more innocence than life in London's orbit could offer.

At first the farm offered exactly the idyll they were seeking: The two boys spent their days romping among the cows, watching farmhands milk them and deliver their calves. They built tree houses and trebuchets out of spare pieces of wood and rode in the tractor of the farmer who had rented their house to them. Hutchins was a bright and happy child, open to friendships but stoic and “self-contained,” as his father, Desmond, puts it, with “a very strong sense of right and wrong.” When he fell and broke his wrist while playing, he didn't shed a single tear, his father says. But when the farmer put down a lame, brain-damaged calf that Hutchins had bonded with, he cried inconsolably.

Hutchins didn't always fit in with the other kids in rural Devon. He was taller than the other boys, and he lacked the usual English obsession with soccer; he came to prefer surfing in the freezing waters a few miles from his house instead. He was one of only a few mixed-race children at his school, and he refused to cut his trademark mop of curly hair.

But above all, what distinguished Hutchins from everyone around him was his preternatural fascination and facility with computers. From the age of 6, Hutchins had watched his mother use Windows 95 on the family's Dell tower desktop. His father was often annoyed to find him dismantling the family PC or filling it with strange programs. By the time they moved to Devon, Hutchins had begun to be curious about the inscrutable HTML characters behind the websites he visited, and was coding rudimentary "Hello world" scripts in Basic. He soon came to see programming as "a gateway to build whatever you wanted," as he puts it, far more exciting than even the wooden forts and catapults he built with his brother. "There were no limits," he says.

In computer class, where his peers were still learning to use word processors, Hutchins was miserably bored. The school's computers prevented him from installing the games he wanted to play, like *Counterstrike* and *Call of Duty*, and they restricted the sites he could visit online. But Hutchins found he could program his way out of those constraints. Within Microsoft Word, he discovered a feature that allowed him to write scripts in a language called Visual Basic. Using that scripting feature, he could run whatever code he wanted and even install unapproved software. He used that trick to install a proxy to bounce his web traffic through a faraway server, defeating the school's attempts to filter and monitor his web surfing too.

On his 13th birthday, after years of fighting for time on the family's aging Dell, Hutchins' parents agreed to buy him his own computer—or rather, the components he requested, piece by piece, to build it himself. Soon, Hutchins' mother says, the computer became a "complete and utter love" that overruled almost everything else in her son's life.

Related Stories

FAMILY BUSINESS

How a Hacker's Mom Broke Into a South Dakota Prison

EXCLUSIVE

Inside Olympic Destroyer, the Most Deceptive Hack in History

COVER STORY

The Untold Story of NotPetya, the Code that Crashed the World

Hutchins still surfed, and he had taken up a sport called surf lifesaving, a kind of competitive lifeguarding. He excelled at it and would eventually win a handful of medals at the national level. But when he wasn't in the water, he was in front of his computer, playing videogames or refining his programming skills for hours on end.

Janet Hutchins worried about her son's digital obsession. In particular, she feared how the darker fringes of the web, what she only half-jokingly calls the "internet boogeyman," might influence her son, who she saw as relatively sheltered in their rural English life.

So she tried to install parental controls on Marcus' computer; he responded by using a simple technique to gain administrative privileges when he booted up the PC, and immediately turned the controls off. She tried limiting his internet access via their home router; he found a hardware reset on the router that allowed him to restore it to factory settings, then configured the router to boot *her* offline instead.

“After that we had a long chat,” Janet says. She threatened to remove the house's internet connection altogether. Instead they came to a truce. “We agreed that if he reinstated my internet access, I would monitor him in another way,” she says. “But in actual fact, there was no way of monitoring Marcus. Because he was way more clever than any of us were ever going to be.”

ILLUSTRATION: JANELLE BARONE

MANY MOTHERS' FEARS of the internet boogeyman are overblown. Janet Hutchins' were not.

Within a year of getting his own computer, Hutchins was exploring an elementary hacking web forum, one dedicated to wreaking havoc upon the then-popular instant messaging platform MSN. There he found a community of like-minded young hackers showing off their inventions. One bragged of creating a kind of MSN worm that impersonated a JPEG:

When someone opened it, the malware would instantly and invisibly send itself to all their MSN contacts, some of whom would fall for the bait and open the photo, which would fire off another round of messages, ad infinitum.

Hutchins didn't know what the worm was meant to accomplish—whether it was intended for cybercrime or simply a spammy prank—but he was deeply impressed. “I was like, wow, look what programming can do,” he says. “I want to be able to do *this* kind of stuff.”

Around the time he turned 14, Hutchins posted his own contribution to the forum—a simple password stealer. Install it on someone's computer and it could pull the passwords for the victim's web accounts from where Internet Explorer had stored them for its convenient autofill feature. The passwords were encrypted, but he'd figured out where the browser hid the decryption key too.

Hutchins' first piece of malware was met with approval from the forum. And whose passwords did he imagine might be stolen with his invention? “I didn't, really,” Hutchins says. “I just thought, ‘This is a cool thing I've made.’”

As Hutchins' hacking career began to take shape, his academic career was deteriorating. He would come home from the beach in the evening and go straight to his room, eat in front of his computer, and then pretend to sleep. After his parents checked that his lights were out and went to bed themselves, he'd get back to his keyboard. “Unbeknownst to us, he'd be up programming into the wee small hours,” Janet says. When she woke him the next morning, “he'd look ghastly. Because he'd only been in bed for half an hour.” Hutchins' mystified mother at one point was so worried she took her son to the doctor, where he was diagnosed with being a sleep-deprived teenager.

One day at school, when Hutchins was about 15, he found that he'd been locked out of his network account. A few hours later he was called into a school administrator's office. The staff there accused him of carrying out a cyberattack on the school's network, corrupting one server so deeply it had to be replaced. Hutchins vehemently denied any involvement and demanded to see the evidence. As he tells it, the administrators refused to share it. But he had, by that time, become notorious among the school's IT staff for flouting their security measures. He maintains, even today, that he was merely the most convenient scapegoat. “Marcus was never a good liar,” his mother agrees. “He was quite boastful. If he had done it, he would have said he'd done it.”

Hutchins was suspended for two weeks and permanently banned from using computers at school. His answer, from that point on, was simply to spend as little time there as possible. He became fully nocturnal, sleeping well into the school day and often skipping his classes altogether. His parents were furious, but aside from the moments when he was trapped in his mother's car, getting a ride to school or to go surfing, he mostly evaded their lectures and punishments. “They couldn't physically drag me to school,” Hutchins says. “I'm a big guy.”

Hutchins' family had, by 2009, moved off the farm, into a house that occupied the former post office of a small, one-pub village. Marcus took a room at the top of the stairs. He emerged from his bedroom only occasionally, to microwave a frozen pizza or make himself more instant coffee for his late-night programming binges. But for the most part, he kept his door closed and locked against his parents, as he delved deeper into a secret life to which they weren't invited.

AROUND THE SAME time, the MSN forum that Hutchins had been frequenting shut down, so he transitioned to another community called HackForums. Its members were a shade more advanced in their skills and a shade murkier in their ethics: a *Lord of the Flies* collection of young hackers seeking to impress one another with nihilistic feats of exploitation. The minimum table stakes to gain respect from the HackForums crowd was possession of a botnet, a collection of hundreds or thousands of malware-infected computers that obey a hacker's commands, capable of directing junk traffic at rivals to flood their web server and knock them offline—what's known as a distributed denial of service, or DDoS, attack.

There was, at this point, no overlap between Hutchins' idyllic English village life and his secret cyberpunk one, no reality checks to prevent him from adopting the amoral atmosphere of the underworld he was entering. So Hutchins, still 15 years old, was soon bragging on the forum about running his own botnet of more than 8,000 computers, mostly hacked with simple fake files he'd uploaded to BitTorrent sites and tricked unwitting users into running.

Even more ambitiously, Hutchins also set up his own business: He began renting servers and then selling web hosting services to denizens of HackForums for a monthly fee. The enterprise, which Hutchins called Gh0sthosting, explicitly advertised itself on HackForums as a place where “all illegal sites” were allowed. He suggested in another post that buyers could use his service to host phishing pages designed to impersonate login pages and steal victims' passwords. When one customer asked if it was acceptable to host "warez"—black market software—Hutchins immediately replied, "Yeah any sites but child porn."

But in his teenage mind, Hutchins says, he still saw what he was doing as several steps removed from any *real* cybercrime. Hosting shady servers or stealing a few Facebook passwords or exploiting a hijacked computer to enlist it in DDoS attacks against other hackers—those hardly seemed like the serious offenses that would earn him the attention of law enforcement. Hutchins wasn't, after all, carrying out bank fraud, stealing actual money from innocent people. Or at least that's what he told himself. He says that the red line of financial fraud, arbitrary as it was, remained inviolable in his self-defined and shifting moral code.

What Is a Bot?

Our in-house Know-It-Alls answer questions about your interactions with technology.

BY PARIS MARTINEAU

In fact, within a year Hutchins grew bored with his botnets and his hosting service, which he found involved placating a lot of "whiny customers." So he quit both and began to focus on something he enjoyed far more: perfecting his own malware. Soon he was taking apart other hackers' rootkits—programs designed to alter a computer's operating system to make themselves entirely undetectable. He studied their features and learned to hide his code inside other computer processes to make his files invisible in the machine's file directory.

When Hutchins posted some sample code to show off his growing skills, another HackForums member was impressed enough that he asked Hutchins to write part of a program that would check whether specific antivirus engines could detect a hacker's malware, a kind of anti-antivirus tool. For that task, Hutchins was paid $200 in the early digital currency Liberty Reserve. The same customer followed up by offering $800 for a “formgrabber” Hutchins had written, a rootkit that could silently steal passwords and other data that people had entered into web forms and send them to the hacker. He happily accepted.

Hutchins began to develop a reputation as a talented malware ghostwriter. Then, when he was 16, he was approached by a more serious client, a figure that the teenager would come to know by the pseudonym Vinny.

Vinny made Hutchins an offer: He wanted a multifeatured, well-maintained rootkit that he could sell on hacker marketplaces far more professional than HackForums, like Exploit.in and Dark0de. And rather than paying up front for the code, he would give Hutchins half the profits from every sale. They would call the product UPAS Kit, after the Javanese upas tree, whose toxic sap was traditionally used in Southeast Asia to make poison darts and arrows.

Vinny seemed different from the braggarts and wannabes Hutchins had met elsewhere in the hacker underground—more professional and tight-lipped, never revealing a single personal detail about himself even as they chatted more and more frequently. And both Hutchins and Vinny were careful to never log their conversations, Hutchins says. (As a result, WIRED has no record of their interactions, only Hutchins' account of them.)

Hutchins says he was always careful to cloak his movements online, routing his internet connection through multiple proxy servers and hacked PCs in Eastern Europe intended to confuse any investigator. But he wasn't nearly as disciplined about keeping the details of his personal life secret from Vinny. In one conversation, Hutchins complained to his business partner that there was no quality weed to be found anywhere in his village, deep in rural England. Vinny responded that he would mail him some from a new ecommerce site called Silk Road.

This was 2011, early days for Silk Road, and the notorious dark-web drug marketplace was mostly known only to those in the internet underground, not the masses who would later discover it. Hutchins himself thought it had to be a hoax. “Bullshit,” he remembers writing to Vinny. “Prove it.”

So Vinny asked for Hutchins' address—and his date of birth. He wanted to send him a birthday present, he said. Hutchins, in a moment he would come to regret, supplied both.

On Hutchins' 17th birthday, a package arrived for him in the mail at his parents' house. Inside was a collection of weed, hallucinogenic mushrooms, and ecstasy, courtesy of his mysterious new associate.

ILLUSTRATION: JANELLE BARONE

HUTCHINS FINISHED WRITING UPAS Kit after nearly nine months of work, and in the summer of 2012 the rootkit went up for sale. Hutchins didn't ask Vinny any questions about who was buying. He was mostly just pleased to have leveled up from a HackForums show-off to a professional coder whose work was desired and appreciated.

The money was nice too: As Vinny began to pay Hutchins thousands of dollars in commissions from UPAS Kit sales—always in bitcoin—Hutchins found himself with his first real disposable income. He upgraded his computer, bought an Xbox and a new sound system for his room, and began to dabble in bitcoin day trading. By this point, he had dropped out of school entirely, and he'd quit surf lifesaving after his coach retired. He told his parents that he was working on freelance programming projects, which seemed to satisfy them.

With the success of UPAS Kit, Vinny told Hutchins that it was time to build UPAS Kit 2.0. He wanted new features for this sequel, including a keylogger that could record victims' every keystroke and the ability to see their entire screen. And most of all, he wanted a feature that could insert fake text-entry fields and other content into the pages that victims were seeing—something called a web inject.

> **Vinny added that he knew Hutchins' identity and address. If their business relationship ended, perhaps he would share that information with the FBI.**

That last demand in particular gave Hutchins a deeply uneasy feeling, he says. Web injects, in Hutchins' mind, had a very clear purpose: They were designed for bank fraud. Most banks require a second factor of authentication when making a transfer; they often send a code via text message to a user's phone and ask them to enter it on a web page as a double check of their identity. Web injects allow hackers to defeat that security measure by sleight of hand. A hacker initiates a bank transfer from the victim's account, and then, when the bank asks the hacker for a confirmation code, the hacker injects a fake message onto the victim's screen asking them to perform a routine reconfirmation of their identity with a text message code. When the victim enters that code from their phone, the hacker passes it on to the bank, confirming the transfer out of their account.

Over just a few years, Hutchins had taken so many small steps down the unlit tunnel of online criminality that he'd often lost sight of the lines he was crossing. But in this IM conversation with Vinny, Hutchins says, he could see that he was being asked to do something very wrong—that he would now, without a doubt, be helping thieves steal from innocent victims. And by engaging in actual financial cybercrime, he'd also be inviting law enforcement's attention in a way he never had before.

Until that point, Hutchins had allowed himself to imagine that his creations might be used simply to steal access to people's Facebook accounts or to build botnets that mined cryptocurrency on people's PCs. “I never knew definitively what was happening with my code,” he says. “But now it was obvious. This would be used to steal money from people. This would be used to wipe out people's savings.”

He says he refused Vinny's demand. “I'm not fucking working on a banking trojan,” he remembers writing.

Vinny insisted. And he added a reminder, in what Hutchins understood as equal parts joke and threat, that he knew Hutchins' identity and address. If their business relationship ended, perhaps he would share that information with the FBI.

As Hutchins tells it, he was both scared and angry at himself: He had naively shared identifying details with a partner who was turning out to be a ruthless criminal. But he held his ground and threatened to walk away. Vinny, knowing that he needed Hutchins' coding skills, seemed to back down. They reached an agreement: Hutchins would work on the revamped version of UPAS Kit, but without the web injects.

As he developed that next-generation rootkit over the following months, Hutchins began attending a local community college. He developed a bond with one of his computer science professors and was surprised to discover that he actually wanted to graduate. But he strained under the load of studying while also building and maintaining Vinny's malware. His business partner now seemed deeply impatient to have their new rootkit finished, and he pinged Hutchins constantly, demanding updates. To cope, Hutchins began turning back to Silk Road, buying amphetamines on the dark web to replace his nighttime coffee binges.

After nine months of all-night coding sessions, the second version of UPAS Kit was ready. But as soon as Hutchins shared the finished code with Vinny, he says, Vinny responded with a surprise revelation: He had secretly hired another coder to create the web injects that Hutchins had refused to build. With the two programmers' work combined, Vinny had everything he needed to make a fully functional banking trojan.

Hutchins says he felt livid, speechless. He quickly realized he had very little leverage against Vinny. The malware was already written. And for the most part, it was Hutchins who had authored it.

In that moment, all of the moral concerns and threats of punishment that Hutchins had brushed off for years suddenly caught up with him in a sobering rush. “There is no getting out of this,” he remembers thinking.

"The FBI is going to turn up at my door one day with an arrest warrant. And it will be because I trusted this fucking guy."

STILL, AS DEEP as Hutchins had been reeled in by Vinny, he had a choice.

Vinny wanted him to do the work of integrating the other programmer's web injects into their malware, then test the rootkit and maintain it with updates once it launched. Hutchins says he knew instinctively that he should walk away and never communicate with Vinny again. But as Hutchins tells it, Vinny seemed to have been preparing for this conversation, and he laid out an argument: Hutchins had already put in nearly nine months of work. He had already essentially built a banking rootkit that would be sold to customers, whether Hutchins liked it or not.

Besides, Hutchins was still being paid on commission. If he quit now, he'd get nothing. He'd have taken all the risks, enough to be implicated in the crime, but would receive none of the rewards.

As angry as he was at having fallen into Vinny's trap, Hutchins admits that he was also persuaded. So he added one more link to the yearslong chain of bad decisions that had defined his teenage life: He agreed to keep ghostwriting Vinny's banking malware.

Hutchins got to work, stitching the web inject features into his rootkit and then testing the program ahead of its release. But he found now that his love of coding had evaporated. He would procrastinate for as long as possible and then submerge into daylong coding binges, overriding his fear and guilt with amphetamines.

In June 2014, the rootkit was ready. Vinny began to sell their work on the cybercriminal marketplaces Exploit.in and Dark0de. Later he'd also put it up for sale on AlphaBay, a site on the dark web that had replaced Silk Road after the FBI tore the original darknet market offline.

After arguments with jilted customers, Vinny had decided to rebrand and drop the UPAS label. Instead, he came up with a new moniker, a play on Zeus, one of the most notorious banking trojans in the history of cybercrime. Vinny christened his malware in the name of a cruel giant in Greek mythology, the one who had fathered Zeus and all the other vengeful gods in the pantheon of Mount Olympus: He called it Kronos.

WHEN HUTCHINS WAS 19, his family moved again, this time into an 18th-century, four-story building in Ilfracombe, a Victorian seaside resort town in another part of Devon. Hutchins settled into the basement of the house, with access to his own bathroom and a kitchen that had once been used by the house's servants. That setup allowed him to cut himself off even further from his family and the world. He was, more than ever, alone.

When Kronos launched on Exploit.in, the malware was only a modest success. The largely Russian community of hackers on the site were skeptical of Vinny, who didn't speak their language and had priced the trojan at an ambitious $7,000. And like any new software, Kronos had bugs that needed fixing. Customers demanded constant updates and new features. So Hutchins was tasked with nonstop coding for the next year, now with tight deadlines and angry buyers demanding he meet them.

To keep up while also trying to finish his last year of college, Hutchins ramped up his amphetamine intake sharply. He would take enough speed to reach what he describes as a state of euphoria. Only in that condition, he says, could he still enjoy his programming work and stave off his growing dread. “Every time I heard a siren, I thought it was coming for me,” he says. Vanquishing those thoughts with still more stimulants, he would stay up for days, studying and coding, and then crash into a state of anxiety and depression before sleeping for 24-hour stretches.

All that slingshotting between manic highs and miserable lows took a toll on Hutchins' judgment—most notably in his interactions with another online friend he calls Randy.

When Hutchins met Randy on a hacker forum called TrojanForge after the Kronos release, Randy asked Hutchins if he'd write banking malware for him. When Hutchins refused, Randy instead asked for help with some enterprise and educational apps he was trying to launch as legitimate businesses. Hutchins, seeing a way to launder his illegal earnings with legal income, agreed.

Randy proved to be a generous patron. When Hutchins told him that he didn't have a MacOS machine to work on Apple apps, Randy asked for his address—which again, Hutchins provided—and shipped him a new iMac desktop as a gift. Later, he asked if Hutchins had a PlayStation console so that they could play games together online. When Hutchins said he didn't, Randy shipped him a new PS4 too.

Unlike Vinny, Randy was refreshingly open about his personal life. As he and Hutchins became closer, they would call each other or even video chat, rather than interact via the faceless instant messaging Hutchins had become accustomed to. Randy impressed Hutchins by describing his philanthropic goals, how he was using his profits to fund charities like free coding education projects for kids. Hutchins sensed that much of those profits came from cybercrime. But he began to see Randy as a Robin Hood–like figure, a model he hoped to emulate someday. Randy revealed that he was based in Los Angeles, a sunny paradise where Hutchins had always dreamed of living. At some points, they even talked about moving in together, running a startup out of a house near the beach in Southern California.

Randy trusted Hutchins enough that when Hutchins described his bitcoin daytrading tricks, Randy sent him more than $10,000 worth of the cryptocurrency to trade on his behalf. Hutchins had set up his own custom-coded programs that hedged his bitcoin buys with short selling, protecting his holdings against bitcoin's dramatic fluctuations. Randy asked him to manage his own funds with the same techniques.

One morning in the summer of 2015, Hutchins woke up after an amphetamine bender to find that there had been an electrical outage during the night. All of his computers had powered off just as bitcoin's price crashed, erasing close to $5,000 of Randy's savings. Still near the bottom of his spasmodic cycle of drug use, Hutchins panicked.

He says he found Randy online and immediately admitted to losing his money. But to make up for the loss, he made Randy an offer. Hutchins revealed that he was the secret author of a banking rootkit called Kronos. Knowing that Randy had been looking for bank fraud malware in the past, he offered Randy a free copy. Randy, always understanding, called it even.

This was the first time Hutchins had divulged his work on Kronos to anyone. When he woke up the next day with a clearer head, he knew that he had made a terrible mistake. Sitting in his bedroom, he thought of all the personal information that Randy had so casually shared with him over the previous months, and he realized that he had just confided his most dangerous secret to someone whose operational security was deeply flawed. Sooner or later, Randy would be caught by law enforcement, and he would likely be just as forthcoming with the cops.

Hutchins had already come to view his eventual arrest for his cybercrimes as inevitable. But now he could see the Feds' path to his door. “Shit,” Hutchins thought to himself. “This is how it ends.”

ILLUSTRATION: JANELLE BARONE

WHEN HUTCHINS GRADUATED from college in the spring of 2015, he felt it was time to give up his amphetamine habit. So he decided to quit cold turkey.

At first the withdrawal symptoms simply mired him in the usual depressive low that he had experienced many times before. But one evening a few days in, while he was alone in his room watching the British teen drama *Waterloo Road*, he began to feel a dark sensation creep over him—what he describes as an all-encompassing sensation of "impending doom." Intellectually, he knew he was in no physical danger. And yet, "My brain was telling me, I'm about to die," he remembers.

He told no one. Instead he just rode out the withdrawal alone, experiencing what he describes as a multiday panic attack. When Vinny demanded to know why he was behind on his Kronos work, Hutchins says he found it was easier to say he was still busy with school, rather than admit that he was caught in a well of debilitating anxiety.

But as his symptoms drew on and he became even less productive over the weeks that followed, he found that his menacing business associate seemed to bother him less. After a few scoldings, Vinny left him alone. The bitcoin payments for Kronos commissions ended, and with them went the partnership that had pulled Hutchins into the darkest years of his life as a cybercriminal.

For the next months, Hutchins did little more than hide in his room and recover. He played videogames and binge-watched *Breaking Bad*. He left his house only rarely, to swim in the ocean or join groups of storm chasers who would gather on the cliffs near Ilfracombe to watch 50- and 60-foot waves slam into the rocks. Hutchins remembers enjoying how small the waves made him feel, imagining how their raw power could kill him instantly.

It took months for Hutchins' feeling of impending doom to abate, and even then it was replaced by an intermittent, deep-seated angst. As he leveled out, Hutchins began to delve back into the world of hacking. But he had lost his taste for the cybercriminal underworld. Instead, he turned back to a blog that he'd started in 2013, in the period between dropping out of secondary school and starting college.

The site was called MalwareTech, which doubled as Hutchins' pen name as he began to publish a slew of posts on the technical minutiae of malware. The blog's clinical, objective analysis soon seemed to attract both blackhat and whitehat visitors. “It was kind of this neutral ground,” he says. “Both sides of the game enjoyed it.”

At one point he even wrote a deep-dive analysis of web injects, the very feature of Kronos that had caused him so much anxiety. In other, more impish posts, he'd point out vulnerabilities in competitors' malware that allowed their victims' computers to be commandeered by other hackers. Soon he had an audience of more than 10,000 regular readers, and none of them seemed to know that MalwareTech's insights stemmed from an active history of writing malware himself.

During his post-Kronos year of rehabilitation, Hutchins started reverse-engineering some of the largest botnets out in the wild, known as Kelihos and Necurs. But he soon went a step further, realizing he could actually *join* those herds of hijacked machines and analyze them for his readers from the inside. The Kelihos botnet, for instance, was designed to send commands from one victim computer to another, rather than from a central server—a peer-to-peer architecture designed to make the botnet harder to take down. But that meant Hutchins could actually code his own program that mimicked the Kelihos malware and “spoke” its language, and use it to spy on all the rest of the botnet's operations—once he had broken past all the obfuscation the botnets' designers had devised to prevent that sort of snooping.

Using this steady stream of intelligence, Hutchins built a Kelihos botnet “tracker,” mapping out on a public website the hundreds of thousands of computers around the world it had ensnared. Not long after that, an entrepreneur named Salim Neino, the CEO of a small Los Angeles-based cybersecurity firm called Kryptos Logic, emailed MalwareTech to ask if the anonymous blogger might do some work for them. The firm was hoping to create a botnet tracking service, one that would alert victims if their IP addresses showed up in a collection of hacked machines like Kelihos.

In fact, the company had already asked one of its employees to get inside Kelihos, but the staffer had told Neino that reverse-engineering the code would take too much time. Without realizing what he was doing, Hutchins had unraveled one of the most inscrutable botnets on the internet.

Neino offered Hutchins $10,000 to build Kryptos Logic its own Kelihos tracker. Within weeks of landing that first job, Hutchins had built a tracker for a second botnet too, an even bigger, older amalgamation of hacked PCs known as Sality. After that, Kryptos Logic made Hutchins a job offer, with a six-figure annual salary. When Hutchins saw how the numbers broke down, he thought Neino must be joking. “What?” he remembers thinking. “You're going to send me this much money *every month*?”

It was more than he had ever earned as a cybercriminal malware developer. Hutchins had come to understand, too late, the reality of the modern cybersecurity industry: For a talented hacker in a Western country, crime truly doesn't pay.

IN HIS FIRST months at Kryptos Logic, Hutchins got inside one massive botnet after another: Necurs, Dridex, Emotet—malware networks encompassing millions of computers in total. Even when his new colleagues at Kryptos believed that a botnet was impregnable, Hutchins would surprise them by coming up with a fresh sample of the bot's code, often shared with him by a reader of his blog or supplied by an underground source. Again and again, he would deconstruct the program and—still working from his bedroom in Ilfracombe—allow the company to gain access to a new horde of zombie machines, tracking the malware's spread and alerting the hackers' victims.

“When it came to botnet research, he was probably one of the best in the world at that point. By the third or fourth month, we had tracked every major botnet in the world with his help,” Neino says. “He brought us to another level.”

Hutchins continued to detail his work on his MalwareTech blog and Twitter, where he began to be regarded as an elite malware-whisperer. “He's a reversing savant, when it comes down to it,” says Jake Williams, a former NSA hacker turned security consultant who chatted with MalwareTech and traded code samples with him around that time. “From a raw skill level, he's off the charts. He's comparable to some of the best I've worked with, anywhere.” Yet aside from his Kryptos Logic colleagues and a few close friends, no one knew MalwareTech's real identity. Most of his tens of thousands of followers, like Williams, recognized him only as the Persian cat with sunglasses that Hutchins used as a Twitter avatar.

In the fall of 2016, a new kind of botnet appeared: A piece of malware known as Mirai had begun to infect so-called internet-of-things devices —wireless routers, digital video recorders, and security cameras—and was lashing them together into massive swarms capable of shockingly powerful DDoS attacks. Until then, the largest DDoS attacks ever seen had slammed their targets with a few hundred gigabits per second of traffic. Now victims were being hit with more like 1 *terabit* per second, gargantuan floods of junk traffic that could tear offline anything in their path. To make matters worse, the author of Mirai, a hacker who went by the name Anna-Senpai, posted the code for the malware on HackForums, inviting others to make their own Mirai offshoots.

In September of that year, one Mirai attack hit the website of the security blogger Brian Krebs with more than 600 gigabits per second, taking his site down instantly. Soon after, the French hosting company OVH buckled under a 1.1-terabit-per-second torrent. In October, another wave hit Dyn, a provider of the domain-name-system servers that act as a kind of phone book for the internet, translating domain names into IP addresses. When Dyn went down, so did Amazon, Spotify, Netflix, PayPal, and Reddit for users across parts of North America and Europe. Around the same time, a Mirai attack hit the main telecom provider for much of Liberia, knocking most of the country off the internet.

Hutchins, always a storm chaser, began to track Mirai's tsunamis. With a Kryptos Logic colleague, he dug up samples of Mirai's code and used them to create programs that infiltrated the splintered Mirai botnets, intercepting their commands and creating a Twitter feed that posted news of their attacks in real time. Then, in January 2017, the same Mirai botnet that hit Liberia began to rain down cyberattacks on Lloyds of London, the largest bank in the UK, in an apparent extortion campaign that took the bank's website down multiple times over a series of days.

Thanks to his Mirai tracker, Hutchins could see which server was sending out the commands to train the botnet's firepower on Lloyds; it appeared that the machine was being used to run a DDoS-for-hire service. And on that server, he discovered contact information for the hacker who was administering it. Hutchins quickly found him on the instant messaging service Jabber, using the name “popopret.”

So he asked the hacker to stop. He told popopret he knew that he wasn't directly responsible for the attack on Lloyds himself, that he was only selling access to his Mirai botnet. Then he sent him a series of messages that included Twitter posts from Lloyds customers who had been locked out of their accounts, some of whom were stuck in foreign countries without money. He also pointed out that banks were designated as critical infrastructure in the UK, and that meant British intelligence services were likely to track down the botnet administrator if the attacks continued.

The DDoS attacks on the banks ended. More than a year later, Hutchins would recount the story on his Twitter feed, noting that he wasn't surprised the hacker had ultimately listened to reason. In his tweets, Hutchins offered a rare hint of his own secret past—he knew what it was like to sit behind a keyboard, detached from the pain inflicted on innocents far across the internet.

“In my career I've found few people are truly evil, most are just too far disconnected from the effects of their actions,” he wrote. “Until someone reconnects them.”

AROUND NOON ON May 12, 2017, just as Hutchins was starting a rare week of vacation, Henry Jones was sitting 200 miles to the east amid a cluster of a half-dozen PCs in an administrative room at the Royal London Hospital, a major surgical and trauma center in northeast London, when he saw the first signs that something was going very wrong.

Jones, a young anesthesiologist who asked that WIRED not use his real name, was finishing a lunch of chicken curry and chips from the hospital cafeteria, trying to check his email before he was called back into surgery, where he was trading shifts with a more senior colleague. But he couldn't log in; the email system seemed to be down. He shared a brief collective grumble with the other doctors in the room, who were all accustomed to computer problems across the National Health Service; after all, their PCs were still running Windows XP, a nearly 20-year-old operating system. “Another day at the Royal London,” he remembers thinking.

But just then, an IT administrator came into the room and told the staff that something more unusual was going on: A virus seemed to be spreading across the hospital's network. One of the PCs in the room had rebooted, and now Jones could see that it showed a red screen with a lock in the upper left corner. “Ooops, your files have been encrypted!” it read. At the bottom of the screen, it demanded a $300 payment in bitcoin to unlock the machine.

Jones had no time to puzzle over the message before he was called back into the surgical theater. He scrubbed, put on his mask and gloves, and reentered the operating room, where surgeons were just finishing an orthopedic procedure. Now it was Jones' job to wake the patient up again. He began to slowly turn a dial that tapered off the sevoflurane vapor feeding into the patient's lungs, trying to time the process exactly so that the patient wouldn't wake up before he'd had a chance to remove the breathing tube, but wouldn't stay out long enough to delay their next surgery.

As he focused on that task, he could hear the surgeons and nurses expressing dismay as they tried to record notes on the surgery's outcome: The operating room's desktop PC seemed to be dead.

Jones finished rousing the patient and scrubbed out. But when he got into the hallway, the manager of the surgical theater intercepted him and told him that all of his cases for the rest of the day had been canceled. A cyberattack had hit not only the whole hospital's network but the entire trust, a collection of five hospitals across East London. All of their computers were down.

Jones felt shocked and vaguely outraged. Was this a coordinated cyberattack on multiple NHS hospitals? With no patients to see, he spent the next hours at loose ends, helping the IT staff unplug computers around the Royal London. But it wasn't until he began to follow the news on his iPhone that he learned the full scale of the damage: It wasn't a targeted attack but an automated worm spreading across the internet. Within hours, it hit more than 600 doctor's offices and clinics, leading to 20,000 canceled appointments, and wiped machines at dozens of hospitals. Across those facilities, surgeries were being canceled, and ambulances were being diverted from emergency rooms, sometimes forcing patients with life-threatening conditions to wait crucial minutes or hours longer for care. Jones came to a grim realization: “People may have died as a result of this.”

Cybersecurity researchers named the worm WannaCry, after the .wncry extension it added to file names after encrypting them. As it paralyzed machines and demanded its bitcoin ransom, WannaCry was jumping from one machine to the next using a powerful piece of code called EternalBlue, which had been stolen from the National Security Agency by a group of hackers known as the Shadow Brokers and leaked onto the open internet a month earlier. It instantly allowed a hacker to penetrate and run hostile code on any unpatched Windows computer—a set of potential targets that likely numbered in the millions. And now that the NSA's highly sophisticated spy tool had been weaponized, it seemed bound to create a global ransomware pandemic within hours.4 bill

“It was the cyber equivalent of watching the moments before a car crash,” says one cybersecurity analyst who worked for British Telecom at the time and was tasked with incident response for the NHS. “We knew that, in terms of the impact on people's lives, this was going to be like nothing we had ever seen before.”

As the worm spread around the world, it infected the German railway firm Deutsche Bahn, Sberbank in Russia, automakers Renault, Nissan, and Honda, universities in China, police departments in India, the Spanish telecom firm Telefónica, FedEx, and Boeing. In the space of an afternoon, it destroyed, by some estimates, nearly a quarter-million computers' data, inflicting between $4 billion and $8 billion in damage.

> **Wannacry seemed poised to spread to the US health care system. "If this happens en masse,**

> **how many people die?" Corman remembers thinking. "Our worst nightmare seemed to be coming true."**

For those watching WannaCry's proliferation, it seemed there was still more pain to come. Josh Corman, at the time a cybersecurity-focused fellow for the Atlantic Council, remembers joining a call on the afternoon of May 12 with representatives from the US Department of Homeland Security, the Department of Health and Human Services, the pharmaceutical firm Merck, and executives from American hospitals. The group, known as the Healthcare Cybersecurity Industry Taskforce, had just finished an analysis that detailed a serious lack of IT security personnel in American hospitals. Now WannaCry seemed poised to spread to the US health care system, and Corman feared the results would be far worse than they had been for the NHS. “If this happens en masse, how many people die?” he remembers thinking. “Our worst nightmare seemed to be coming true.”

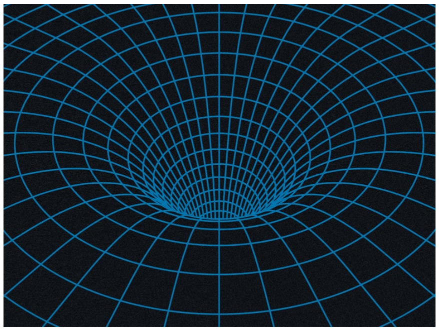
AT AROUND 2:30 on that Friday afternoon, Marcus Hutchins returned from picking up lunch at his local fish-and-chips shop in Ilfracombe, sat down in front of his computer, and discovered that the internet was on fire. “I picked a hell of a fucking week to take off work,” Hutchins wrote on Twitter.

Within minutes, a hacker friend who went by the name Kafeine sent Hutchins a copy of WannaCry's code, and Hutchins began trying to dissect it, with his lunch still sitting in front of him. First, he spun up a simulated computer on a server that he ran in his bedroom, complete with fake files for the ransomware to encrypt, and ran the program in that quarantined test environment. He immediately noticed that before encrypting the decoy files, the malware sent out a query to a certain, very random-looking web address: *iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com*.

That struck Hutchins as significant, if not unusual: When a piece of malware pinged back to this sort of domain, that usually meant it was communicating with a command-and-control server somewhere that might be giving the infected computer instructions. Hutchins copied that long website string into his web browser and found, to his surprise, that no such site existed.

So he visited the domain registrar Namecheap and, at four seconds past 3:08 pm, registered that unattractive web address at a cost of $10.69. Hutchins hoped that in doing so, he might be able to steal control of some part of WannaCry's horde of victim computers away from the malware's creators. Or at least he might gain a tool to monitor the number and location of infected machines, a move that malware analysts call “sinkholing.”

Sure enough, as soon as Hutchins set up that domain on a cluster of servers hosted by his employer, Kryptos Logic, it was bombarded with thousands of connections from every new computer that was being infected by WannaCry around the world. Hutchins could now



What Is Sinkholing?

BY LILY HAY NEWMAN

see the enormous, global scale of the attack firsthand. And as he tweeted about his work, he began to be flooded with hundreds of emails from other researchers, journalists, and system administrators trying to learn more about the plague devouring the world's networks. With his sinkhole domain, Hutchins was now suddenly pulling in information about those infections that no one else on the planet possessed.

For the next four hours, he responded to those emails and worked frantically to debug a map he was building to track the new infections popping up globally, just as he had done with Kelihos, Necurs, and so many other botnets. At 6:30 pm, around three and a half hours after Hutchins had registered the domain, his hacker friend Kafeine sent him a tweet posted by another security researcher, Darien Huss.

The tweet put forward a simple, terse statement that shocked Hutchins: “Execution fails now that domain has been sinkholed.”

In other words, since Hutchins' domain had first appeared online, WannaCry's new infections had continued to spread, but they hadn't actually done any new damage. The worm seemed to be neutralized.

Huss' tweet included a snippet of WannaCry's code that he'd reverse-engineered. The code's logic showed that before encrypting any files, the malware first checked if it could reach Hutchins' web address. If not, it went ahead with corrupting the computer's contents. If it did reach that address, it simply stopped in its tracks. (Malware analysts still debate what the purpose of that feature was—whether it was intended as an antivirus evasion technique or a safeguard built into the worm by its author.)

Hutchins hadn't found the malware's command-and-control address. He'd found its kill switch. The domain he'd registered was a way to simply, instantly turn off WannaCry's mayhem around the world. It was as if he had fired two proton torpedoes through the Death Star's exhaust port and into its reactor core, blown it up, and saved the galaxy, all without understanding what he was doing or even noticing the explosion for three and a half hours.

When Hutchins grasped what he'd done, he leaped up from his chair and jumped around his bedroom, overtaken with joy. Then he did something equally unusual: He went upstairs to tell his family.

Janet Hutchins had the day off from her job as a nurse at a local hospital. She had been in town catching up with friends and had just gotten home and started making dinner. So she had only the slightest sense of the crisis that her colleagues had been dealing with across the NHS. That's when her son came upstairs and told her, a little uncertainly, that he seemed to have stopped the worst malware attack the world had ever seen.

“Well done, sweetheart,” Janet Hutchins said. Then she went back to chopping onions.

ILLUSTRATION: JANELLE BARONE

IT TOOK A few hours longer for Hutchins and his colleagues at Kryptos Logic to understand that WannaCry was still a threat. In fact, the domain that Hutchins had registered was still being bombarded with connections from WannaCry-infected computers all over the globe as the remnants of the neutered worm continued to spread: It would receive nearly 1 million connections over the next two days. If their web domain went offline, every computer that attempted to reach the domain and failed would have its contents encrypted, and WannaCry's wave of destruction would begin again. “If this goes down, WannaCry restarts,” Hutchins' boss, Salim Neino, remembers realizing. “Within 24 hours, it would have hit every vulnerable computer in the world.”

Almost immediately, the problem grew: The next morning, Hutchins noticed a new flood of pings mixed into the WannaCry traffic hitting their sinkhole. He quickly realized that one of the Mirai botnets that he and his Kryptos colleagues had monitored was now slamming the domain with a DDoS attack—perhaps as an act of revenge for their work tracking Mirai, or simply out of a nihilistic desire to watch WannaCry burn down the internet. "It was like we were Atlas, holding up the world on our shoulders," Neino says. "And now someone was kicking Atlas in the back at the same time."

For days afterward, the attacks swelled in size, threatening to bring down the sinkhole domain. Kryptos scrambled to filter and absorb the traffic, spreading the load over a collection of servers in Amazon data centers and the French hosting firm OVH. But they got another surprise a few days later, when local police in the French city of Roubaix, mistakenly believing that their sinkhole domain was being used by the cybercriminals behind WannaCry, physically seized two of their servers from the OVH data center. For a week, Hutchins slept no more than three consecutive hours as he struggled to counter the shifting attacks and keep the WannaCry kill switch intact.

Meanwhile, the press was chipping away at Hutchins' carefully maintained anonymity. On a Sunday morning two days after WannaCry broke out, a local reporter showed up at the Hutchins' front door in Ilfracombe. The reporter's daughter had gone to school with Hutchins, and she recognized him in a Facebook photo that named him in its caption as MalwareTech.

Soon more journalists were ringing the doorbell, setting up in the parking lot across the street from their house, and calling so often that his family stopped answering the phone. British tabloids began to run headlines about the “accidental hero” who had saved the world from his bedroom. Hutchins had to jump over his backyard's wall to avoid the reporters staking out his front door. To defuse the media's appetite, he agreed to give one interview to the Associated Press, during which he was so nervous that he misspelled his last name and the newswire had to run a correction.

In those chaotic first days, Hutchins was constantly on edge, expecting another version of WannaCry to strike; after all, the hackers behind the worm could easily tweak it to remove its kill switch and unleash a sequel. But no such mutation occurred. After a few days, Britain's National Cybersecurity Center reached out to Amazon on Kryptos' behalf and helped the firm negotiate unlimited server capacity in its data centers. Then, after a week, the DDoS mitigation firm Cloudflare stepped in to offer its services, absorbing as much traffic as any botnet could throw at the kill-switch domain and ending the standoff.

When the worst of the danger was over, Neino was concerned enough for Hutchins' well-being that he tied part of his employee's bonus to forcing him to get some rest. When Hutchins finally went to bed, a week after WannaCry struck, he was paid more than $1,000 for every hour of sleep.

AS UNCOMFORTABLE AS the spotlight made Hutchins, his newfound fame came with some rewards. He gained 100,000 Twitter followers virtually overnight. Strangers recognized him and bought him drinks in the local pub to thank him for saving the internet. A local restaurant offered him free pizza for a year. His parents, it seemed, finally understood what he did for a living and were deeply proud of him.

But only at Defcon, the annual 30,000-person Las Vegas hacker conference that took place nearly three months after WannaCry hit, did Hutchins truly allow himself to enjoy his new rock star status in the cybersecurity world. In part to avoid the fans who constantly asked for selfies with him, he and a group of friends rented a real estate mogul's mansion off the strip via Airbnb, with hundreds of palm trees surrounding the largest private pool in the city. They skipped the conference itself, with its hordes of hackers lining up for research talks. Instead they alternated between debaucherous partying—making ample use of the city's marijuana dispensaries and cybersecurity firms' lavish open-bar events—and absurd daytime acts of recreation.

One day they went to a shooting range, where Hutchins fired a grenade launcher and hundreds of high-caliber rounds from an M134 rotary machine gun. On other days they rented Lamborghinis and Corvettes and zoomed down Las Vegas Boulevard and through the canyons around the city. At a performance by one of Hutchins' favorite bands, the Chainsmokers, he stripped down to his underwear and jumped into a pool in front of the stage. Someone stole his wallet out of the pants he'd left behind. He was too elated to care.

Three years had passed since Hutchins' work on Kronos, and life was good. He felt like a different person. And as his star rose, he finally allowed himself—almost—to let go of the low-lying dread, the constant fear that his crimes would catch up with him.

Then, on his last morning in Vegas, Hutchins stepped barefoot onto the driveway of his rented mansion and saw a black SUV parked across the street.

ALMOST IMMEDIATELY, HUTCHINS gave his FBI interrogators a kind of half-confession. Minutes after the two agents brought up Kronos in the McCarran Airport interrogation room, he admitted to having created parts of the malware, though he falsely claimed to have stopped working on it before he turned 18. Some part of him, he says, still hoped that the agents might just be trying to assess his credibility as a witness in their WannaCry investigation or to strong-arm him into giving them control of the WannaCry sinkhole domain. He nervously answered their questions—without a lawyer present.

His wishful thinking evaporated, however, when the agents showed him a printout: It was the transcript of his conversation with “Randy” from three years earlier, when 20-year-old Hutchins had offered his friend a copy of the banking malware he was still maintaining at the time.

> **As his star rose, he finally allowed himself—almost—to let go of the low-lying dread, the constant fear that his crimes would catch up with him.**

Finally, the red-headed agent who had first handcuffed him, Lee Chartier, made the agents' purpose clear. “If I'm being honest with you, Marcus, this has absolutely nothing to do with WannaCry,” Chartier said. The agents pulled out a warrant for his arrest on conspiracy to commit computer fraud and abuse.

Hutchins was driven to a Las Vegas jail in a black FBI SUV that looked exactly like the one he'd spotted in front of his Airbnb that morning. He was allowed one phone call, which he used to contact his boss, Salim Neino. Then he was handcuffed to a chair in a room full of prisoners and left to wait for the rest of the day and the entire night that followed. Only when he asked to use the bathroom was he let into a cell where he could lie down on a concrete bed until someone else asked to use the cell's toilet. Then he'd be moved out of the cell and chained to the chair again.

Instead of sleep, he mostly spent those long hours tumbling down the bottomless mental hole of his imagined future: months of pretrial detention followed by years in prison. He was 5,000 miles from home. It was the loneliest night of his 23-year-old life.

UNBEKNOWNST TO HUTCHINS, however, a kind of immune response was already mounting within the hacker community. After receiving the call from jail, Neino had alerted Andrew Mabbitt, one of Hutchins' hacker friends in Las Vegas; Mabbitt leaked the news to a reporter at Vice and raised the alarm on Twitter. Immediately, high-profile accounts began to take up Hutchins' cause, rallying around the martyred hacker hero.

“The DoJ has seriously fucked up,” tweeted one prominent British cybersecurity researcher, Kevin Beaumont. “I can vouch for @MalwareTechBlog being a really nice guy and also for having strong ethics,” wrote Martijn Grooten, the organizer of the Virus Bulletin cybersecurity conference, using Hutchins' Twitter handle. Some believed that the FBI had mistakenly arrested Hutchins for his WannaCry work, perhaps confusing him with the hackers behind the worm: “It's not often I see the entire hacker community really get this angry, but arresting @MalwareTechBlog for *stopping an attack* [is] unacceptable,” wrote Australian cypherpunk activist Asher Wolf.

Not everyone was supportive of Hutchins: Ex-NSA hacker Dave Aitel went so far as to write in a blog post that he suspected Hutchins had created WannaCry himself and triggered his own kill switch only after the worm got out of control. (That theory would be deflated eight months later, when the Justice Department indicted a North Korean hacker as an alleged member of a state-sponsored hacking team responsible for WannaCry.) But the overwhelming response to Hutchins' arrest was sympathetic. By the next day, the representative for Hutchins' region in the UK parliament, Peter Heaton-Jones, issued a statement expressing his “concern and shock,” lauding Hutchins' work on WannaCry and noting that “people who know him in Ilfracombe, and the wider cyber community, are astounded at the allegations against him.”

Mabbitt found Hutchins a local attorney for his bail hearing, and after

Hutchins spent a miserable day in a crowded cage, his bail was set at $30,000. Stripped of his computers and phones, Hutchins couldn't get access to his bank accounts to cover that cost. So Tor Ekeland, a renowned hacker defense attorney, agreed to manage a legal fund in Hutchins' name to help cover the bond. Money poured in. Almost immediately, stolen credit cards began to show up among the sources of donations, hardly a good look for a computer fraud defendant. Ekeland responded by pulling the plug, returning all the donations and closing the fund.

But the hacker community's goodwill toward Hutchins hadn't run out. On the day he was arrested, a pair of well-known cybersecurity professionals named Tarah Wheeler and Deviant Ollam had flown back to Seattle from Las Vegas. By that Sunday evening, the recently married couple were talking to Hutchins' friend Mabbitt and learning about the troubles with Hutchins' legal fund.

Wheeler and Ollam had never met Hutchins and had barely even interacted with him on Twitter. But they had watched the Justice Department railroad idealistic young hackers for years, from Aaron Swartz to Chelsea Manning, often with tragic consequences. They imagined Hutchins, alone in the federal justice system, facing a similar fate. “We basically had a young, foreign, nerdy person of color being held in federal detention," Wheeler says. "He was the closest thing to a global hero the hacker community had. And no one was there to help him."

Wheeler had just received a five-figure severance package from the security giant Symantec because her division had been shuttered. She and Ollam had been planning to use the money as a down payment on a home. Instead, on a whim, they decided to spend it bailing out Marcus Hutchins.

Within 24 hours of leaving Las Vegas, they got on a flight back to the city. They landed on Monday afternoon, less than 90 minutes before the courthouse's 4 pm deadline for bail payments. If they didn't make it in time, Hutchins would be sent back to jail for another night. From the airport, they jumped in a Lyft to a bank where they took out a $30,000 cashier's check. But when they arrived at the courthouse, a court official told them it had to be notarized. Now they had only 20 minutes left until the court's office closed.

Wheeler was wearing Gucci loafers. She took them off and, barefoot in a black sweater and pencil skirt, sprinted down the street in the middle of a scorching Las Vegas summer afternoon, arriving at the notary less than 10 minutes before 4 pm. Soaked in sweat, she got the check notarized, flagged down a stranger's car, and convinced the driver to ferry her back to the courthouse. Wheeler burst through the door at 4:02 pm, just before the clerk closed up for the day, and handed him the check that would spring Marcus Hutchins from jail.

ILLUSTRATION: JANELLE BARONE

FROM THERE, HUTCHINS was bailed to a crowded halfway house, while even more forces in the hacker community were gathering to come to his aid. Two veteran lawyers, Brian Klein and well-known hacker defense attorney Marcia Hofmann, took his case pro bono. At his arraignment he pleaded not guilty, and a judge agreed that he could be put under house arrest in Los Angeles, where Klein had an office. Over the next two months, his lawyers chipped away at his pretrial detainment conditions, allowing him to travel beyond his Marina del Rey apartment and to use computers and the internet—though the court forbade him access to the WannaCry sinkhole domain he had created. Eventually, even his curfew and GPS monitoring ankle bracelet were removed.

Hutchins got the news that those last pretrial restrictions were being lifted while attending a bonfire party on the beach with friendly hackers from the LA cybersecurity conference Shellcon. Somehow, getting indicted for years-old cybercrimes on a two-week trip to the US had delivered him to the city where he'd always dreamed of living, with relatively few limits on his freedom of movement. Kryptos Logic had put him on unpaid leave, so he spent his days surfing and cycling down the long seaside path that ran from his apartment to Malibu.

And yet he was deeply depressed. He had no income, his savings were dwindling, and he had charges hanging over him that promised years in prison.

Beyond all of that, he was tormented by the truth: Despite all the talk of his heroics, he knew that he had, in fact, done exactly what he was accused of. A feeling of overwhelming guilt had set in the moment he first regained access to the internet and checked his Twitter mentions a month after his arrest. “All of these people are writing to the FBI to say ‘you've got the wrong guy.’ And it was heartbreaking,” Hutchins says. “The guilt from this was a thousand times the guilt I'd felt for Kronos." He says he was tempted to publish a full confession on his blog, but was dissuaded by his lawyers.

Many supporters had interpreted his not-guilty plea as a statement of innocence rather than a negotiating tactic, and they donated tens of thousands of dollars more to a new legal fund. Former NSA hacker Jake Williams had agreed to serve as an expert witness on Hutchins' behalf. Tarah Wheeler and Deviant Ollam had become almost foster parents, flying with him to Milwaukee for his arraignment and helping him get his life set up in LA. He felt he deserved none of this—that everyone had come to his aid only under the mistaken assumption of his innocence.

In fact, much of the support for Hutchins was more nuanced. Just a month after his arrest, cybersecurity blogger Brian Krebs delved into Hutchins' past and found the chain of clues that led to his old posts on HackForums, revealing that he had run an illegal hosting service, maintained a botnet, and authored malware—though not necessarily Kronos. Even as the truth started to come into focus, though, many of Hutchins' fans and friends seemed undeterred in their support for him. "We are all morally complex people," Wheeler says. "For most of us, anything good we ever do comes either because we did bad before or because other people did good to get us out of it, or both."

But Hutchins remained tortured by a kind of moral impostor syndrome. He turned to alcohol and drugs, effacing his emotions with large doses of Adderall during the day and vodka at night. At times, he felt suicidal. The guilt, he says, "was eating me alive."

IN THE SPRING of 2018, nearly nine months after his arrest, prosecutors offered Hutchins a deal. If he agreed to reveal everything he knew about the identities of other criminal hackers and malware authors from his time in the underworld, they would recommend a sentence of no prison time.

Hutchins hesitated. He says he didn't actually know anything about the identity of Vinny, the prosecutors' real target. But he also says that, on principle, he opposed snitching on the petty crimes of his fellow hackers to dodge the consequences of his own actions. Moreover, the deal would still result in a felony record that might prevent him from ever returning to the US. And he knew that the judge in his case, Joseph Stadtmueller, had a history of unpredictable sentencing, sometimes going well below or above the recommendations of prosecutors. So Hutchins refused the deal and set his sights on a trial.

Soon afterward, prosecutors hit back with a superseding indictment, a new set of charges that brought the total to 10, including making false statements to the FBI in his initial interrogation. Hutchins and his lawyers saw the response as a strong-arm tactic, punishing Hutchins for refusing to accept their offer of a deal.

After losing a series of motions—including one to dismiss his Las Vegas airport confession as evidence—Hutchins finally took his lawyers' advice and accepted a plea bargain in April 2019. This new deal was arguably worse than the one he'd been offered earlier: After nearly a year and a half of wrangling with prosecutors, they now agreed only to make no recommendation for sentencing. Hutchins would plead guilty to two of the 10 charges, and would face as much as 10 years in prison and a half-million-dollar fine, entirely up to the judge's discretion.

Along with his plea, Hutchins finally offered a public confession on his website—not the full, guts-spilling one he wanted, but a brief, lawyerly statement his attorneys had approved. “I've pleaded guilty to two charges related to writing malware in the years prior to my career in security,” he wrote. “I regret these actions and accept full responsibility for my mistakes.”

Then he followed up with a more earnest tweet, intended to dispel an easy story to tell about his past immorality: that the sort of whitehat work he'd done was only possible because of his blackhat education—that a hacker's bad actions should be seen as instrumental to his or her later good deeds.

“There's [a] misconception that to be a security expert you must dabble in the dark side,” Hutchins wrote. “It's not true. You can learn everything you need to know legally. Stick to the good side.”

ILLUSTRATION: JANELLE BARONE

ON A WARM day in July, Hutchins arrived at a Milwaukee courthouse for his sentencing. Wearing a gray suit, he slipped in two hours early to avoid any press. As he waited with his lawyers in a briefing room, his vision tunneled; he felt that familiar sensation of impending doom begin to creep over him, the one that had loomed periodically at the back of his mind since he first went through amphetamine withdrawal five years earlier. This time, his anxiety wasn't irrational: The rest of his life was, in fact, hanging in the balance. He took a small dose of Xanax and walked through the halls to calm his nerves before the hearing was called to order.

When Judge Stadtmueller entered the court and sat, the 77-year-old seemed shaky, Hutchins remembers, and he spoke in a gravelly, quavering voice. Hutchins still saw Stadtmueller as a wild card: He knew that the judge had presided over only one previous cybercrime sentencing in his career, 20 years earlier. How would he decipher a case as complicated as this one?

But Hutchins remembers feeling his unease evaporate as Stadtmueller began a long soliloquy. It was replaced by a sense of awe.

Stadtmueller began, almost as if reminiscing to himself, by reminding Hutchins that he had been a judge for more than three decades. In that time, he said, he had sentenced 2,200 people. But none were quite like Hutchins. “We see all sides of the human existence, both young, old, career criminals, those like yourself,” Stadtmueller began. “And I appreciate the fact that one might view the ignoble conduct that underlies this case as against the backdrop of what some have described as the work of a hero, a true hero. And that is, at the end of the day, what gives this case in particular its incredible uniqueness.”

The judge quickly made clear that he saw Hutchins as not just a convicted criminal but as a cybersecurity expert who had “turned the corner” long before he faced justice. Stadtmueller seemed to be weighing the deterrent value of imprisoning Hutchins against the young hacker's genius at fending off malevolent code like WannaCry. “If we don't take the appropriate steps to protect the security of these wonderful technologies that we rely upon each and every day, it has all the potential, as your parents know from your mom's work, to raise incredible havoc,” Stadtmueller said, referring obliquely to Janet Hutchins' job with the NHS. “It's going to take individuals like yourself, who have the skill set, even at the tender age of 24 or 25, to come up with solutions.” The judge even argued that Hutchins might deserve a full pardon, though the court had no power to grant one.

Then Stadtmueller delivered his conclusion: “There are just too many positives on the other side of the ledger,” he said. “The final call in the case of Marcus Hutchins today is a sentence of time served, with a one-year period of supervised release.”

Hutchins could hardly believe what he'd just heard: The judge had weighed his good deeds against his bad ones and decided that his moral debt was canceled. After a few more formalities, the gavel dropped. Hutchins hugged his lawyers and his mother, who had flown in for the hearing. He left the courtroom and paid a $200 administrative fee. And then he walked out onto the street, almost two years since he had first been arrested, a free man.

AFTER FIVE MONTHS of long phone calls, I arranged to meet Marcus

Hutchins in person for the first time at a Starbucks in Venice Beach. I spot his towering mushroom cloud of curls while he's still on the crowded sidewalk. He walks through the door with a broad smile. But I can see that he's still battling an undercurrent of anxiety. He declines a coffee, complaining that he hasn't been sleeping more than a few hours a night.

We walk for the next hours along the beach and the sunny backstreets of Venice, as Hutchins fills in some of the last remaining gaps in his life story. On the boardwalk, he stops periodically to admire the skaters and street performers. This is Hutchins' favorite part of Los Angeles, and he seems to be savoring a last look at it. Despite his sentence of time served, his legal case forced him to overstay his visa, and he's soon likely to be deported back to England. As we walk into Santa Monica, past rows of expensive beach homes, he says his goal is to eventually get back here to LA, which now feels more like home than Devon. "Someday I'd like to be able to live in a house by the ocean like this," he says, "Where I can look out the window and if the waves are good, go right out and surf."

Despite his case's relatively happy ending, Hutchins says he still hasn't been able to shake the lingering feelings of guilt and impending punishment that have hung over his life for years. It still pains him to think of his debt to all the unwitting people who helped him, who donated to his legal fund and defended him, when all he wanted to do was confess.

I point out that perhaps this, now, is that confession. That he's cataloged his deeds and misdeeds over more than 12 hours of interviews; when the results are published—and people reach the end of this article—that account will finally be out in the open. Hutchins' fans and critics alike will see his life laid bare and, like Stadtmueller in his courtroom, they will come to a verdict. Maybe they too will judge him worthy of redemption. And maybe it will give him some closure.

He seems to consider this. “I had hoped it would, but I don't really think so anymore,” he says, looking down at the sidewalk. He's come to believe, he explains, that the only way to earn redemption would be to go back and stop all those people from helping him—making sacrifices for him—under false pretenses. “The time when I could have prevented people from doing all that for me has passed.”

His motives for confessing are different now, he says. He's told his story less to seek forgiveness than simply to have it told. To put the weight of all those feats and secrets, on both sides of the moral scale, behind him. And to get back to work. “I don't want to be the WannaCry guy or the Kronos guy,” he says, looking toward the Malibu hills. “I just want to be someone who can help make things better.”

ANDY GREENBERG *(@a_greenberg) is a senior writer at* WIRED *and the author of the book* Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. *A small section of this story is adapted from that book.*

This article appears in the June issue. Subscribe now.

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

When you buy something using the retail links in our stories, we may earn a small affiliate commission. Read more about how this works.

More Great WIRED Stories

- 27 days in Tokyo Bay: What happened on the *Diamond Princess*
- To run my best marathon at age 44, I had to outrun my past
- Why farmers are dumping milk, even as people go hungry
- What is fleeceware, and how can you protect yourself?
- Tips and tools for cutting your hair at home
- 👁️ AI uncovers a potential Covid-19 treatment. Plus: Get the latest AI news
- 🏃‍♀️ 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

Andy Greenberg is a senior writer for WIRED, covering security, privacy, information freedom, and hacker culture. He's the author of the book *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. The book and excerpts from it published in WIRED won a Gerald Loeb... Read more

SENIOR WRITER

Featured Video

NSA Director of Cybersecurity Anne Neuberger in Conversation with Garrett Graff

Anne Neuberger, Director of Cybersecurity at the National Security Agency, speaks with WIRED's Garrett Graff as part of WIRED25, WIRED's second annual conference in San Francisco.

TOPICS COVER STORY LONGREADS HACKING CYBERSECURITY MAGAZINE-28.06