Gray Hat

Marcus Hutchins stopped one of the most dangerous cyberattacks ever. Then the FBI arrested him. Does a hacker hero always have to have a past?

By **Reeves Wiedeman**

Photographs by **Jeff Minton**

Photographs by Jeff Minton

f Share Tweet in Share Comment

March 6, 2018 8:00 am

Marcus Hutchins was still recovering from the night before as he settled into a lounge at the Las Vegas airport one afternoon this past August. Hutchins, a 23-year-old cybersecurity researcher, had come from his home in rural England in part to attend DefCon, the world's biggest computer-hacking conference, and in part to take a well-deserved vacation.

Three months earlier, a North Korean cyberattack known as WannaCry had crippled the British health-care system and caused a billion dollars in losses across 150 countries. The damage could have been much worse — tens of billions, by one estimate — but a few hours after the attack began, Hutchins figured out how to stop it, almost by accident, while sitting at a computer in his bedroom at his parents' house.

That act made Hutchins the closest thing cybersecurity had ever had to a global celebrity. "Oops! I Saved the World," read the cover of the New York *Daily News*. "Cyber Geek Accidentally Stops Huge Hack Attack." Edward Snowden congratulated Hutchins, and strangers recognized him at Heathrow. Hutchins had gone to DefCon the year before and found the convention unpleasant — "I remember slowly moving down a packed hall in a sea of people who smelled like they hadn't showered in days" — but in 2017, Cisco invited him into the VIP section at its party. "A year earlier, I'd never have gotten in," Hutchins said. At six-foot-four, with hair that adds an inch or two, Hutchins was easy to spot, and conferencegoers asked him to pose for photos that they put online with the tag #WannaCrySlayer.

The post-WannaCry attention had been a bit overwhelming for Hutchins, but he loved Vegas. He stayed in an Airbnb with the city's largest private pool, lit up a bin Laden target at a gun range, and drove around in a friend's rented Lamborghini. Hutchins didn't gamble, but he hung around the casino floor to get free drinks. "About to cross 'turn up at a club in clothes I bought on the way' off my bucket list," he announced on Twitter as he went to the nightclub XS to see one of his favorite groups, the Chainsmokers. He wasn't even mad when he lost his credit card and ID. "Chainsmokers was definitely worth the lost wallet," he said.

In short, Hutchins was having the kind of Vegas experience that a 23-year-old's dreams are made of — so much so that he was oblivious to the American law-enforcement agents who were watching him in Nevada. Hutchins didn't know it, but before he came to the United States, a grand jury in Wisconsin had indicted him, alleging that, three years earlier, he had coded a piece of malware called Kronos that could steal people's online banking information and conspired to sell Kronos to cybercriminals — charges that carried a maximum 40-year sentence. The legal system has struggled to deal with the reality that between the poles of "white hats," the good guys, and "black hats," who use their skills to do harm, many of the world's cybersecurity experts got good by probing the large gray area in the middle. Whatever Hutchins had or hadn't done years earlier, he now seemed to be one of the good guys — a hero, even — and a prosecution like this threatened to fray the already fragile connection between hackers and the government at a moment when the internet can use all the help it can get. All of which left Hutchins surprised, as he sat in the airport tweeting about his eagerness to start investigating a new cyberthreat, when several federal officers walked up and said they needed to ask him a few questions.

One Saturday in February, Hutchins walked into a bar in Santa Monica wearing black Etnies skate shoes, a gray T-shirt, and Apple headphones he kept in his ears until he met me at a table in the back. After his arrest last summer, he'd had a long weekend in jail, followed by a court date in Milwaukee, where he pleaded not guilty to the charges. A hacker he'd never met paid his $30,000 bail, though he wasn't allowed to return to the U.K. (During intake at a halfway house, Hutchins, whose mother is Scottish and father is Jamaican, said an employee insisted on listing him as African-American, despite Hutchins's noting that he was neither. "America is the only place that could try so hard to be politically correct that they just end up being plain racist," he said.)

With nowhere else to go while awaiting trial, he had moved to L.A., where the cybersecurity company he works for is based but where he knew almost no one. At one point in October, he couldn't recall having had a conversation with another human being for two weeks. "Not Going Home November is over and I'm halfway into Don't Go Home December," Hutchins wrote on Twitter, where he has documented his life with surprising candor for someone facing a federal conspiracy charge. "Pretty pumped for Just Stay In America January."

Hutchins had been living under decreasing levels of surveillance — house arrest, a curfew, a GPS monitor on his ankle — but much of his old life had fallen apart around him. A girl he'd been seeing off and on stopped talking to him, and when a friend suggested Tinder, Hutchins pointed out that "I'm under federal indictment, don't have a car, and can't go out between 9 p.m. and 6 a.m." didn't seem like a very good pickup line. He spent his days playing video games, learning to cook — this was his first time living away from home — and day-trading cryptocurrency: One night, Hutchins got drunk and shorted bitcoin, and a subsequent crash paid the rent on his L.A. one-bedroom for three months. His defense team was working pro bono, but he'd just been forced to sell most of his holdings to help cover the legal fees that came with retaining two immigration lawyers and another attorney "to explain to me where the fuck I'm supposed to pay tax." He wasn't allowed to work and was having trouble sleeping. "The FBI took everything from me," Hutchins told me. "My job, my girlfriend, my bitcoin."

Hutchins is a self-described introvert and pessimist. ("I don't really like people," he deadpanned.) But he also has the youthful confidence that comes with knowing he possesses one of the world's most in-demand skills: By his own estimate, there are only five people in the world — "I know of three, but five is a round number" — with his particular expertise. When I asked about his post-WannaCry life as a "mini-celebrity," he objected to the modifier. He was annoyed at those who defended him by saying he wasn't skilled enough to have made Kronos in the first place. "I don't know what hurts more," Hutchins said. "That people think I'm a shitty person or that people think I'm that bad at programming."

One of the few bits of solace Hutchins had found in L.A., once a judge removed his ankle bracelet, was surfing, which he had learned to do growing up in Ilfracombe, a town of 11,000 on the southwestern coast of England. Hutchins was a competitive swimmer and excelled at "Surf Life Saving" — lifeguarding as a sport, essentially — but he was now out of shape compared with a shirtless photo he'd recently seen from those days, which he described as "biceps for days." I asked what had happened in the intervening years. "Computers," he said. "Computers and weed."

Hutchins started learning to code when he was 12. By high school, his skills were advanced enough that administrators blamed him for an attack that took down the school's servers. (Hutchins maintains his innocence.) He went on to a local technical school for two years, where he found the computer-science offerings primitive. In 2013, he started a blog. Malwaretech.com featured wonky posts in which Hutchins detailed his amateur explorations into "reverse engineering," a critical cybersecurity job in which researchers dissect malware to figure out how it works. In a post titled "Coding Malware for Fun and Not for Profit (Because That Would Be Illegal)," Hutchins declared that he was "so bored" with the malware being produced that he had made some himself, assuring readers that, "before you get on the phone to your friendly neighborhood FBI agent," he had designed the malware so it couldn't be deployed.

A year later, Hutchins started looking for a job in cybersecurity. He says he applied to GCHQ, the British equivalent of the NSA — his résumé included links to his blog and a childhood swimming certification — but the background check took ten months. By then, he'd become interested in tracking botnets, the giant networks of poorly secured computers, baby monitors, and other devices that cybercriminals use to deploy malware. "I was never trying to make a career out of it," Hutchins said. "I was just kind of bored." But in 2015, Salim Neino, who runs Kryptos Logic, a computer-security firm in L.A., saw Hutchins's blog posts about a major botnet called Kelihos and offered him a job without even meeting him. "He was extremely talented," Neino said. "You can teach certain things, but in computer security, raw talent is almost irreplaceable."

Suddenly, at 22, Hutchins had a six-figure salary, two employees reporting to him, and the ability to work remotely from three computer monitors in his bedroom on his own schedule. ("My first question upon waking up and seeing the clock said 9:30 was 'a.m. or p.m.?' #DreamJob.") He quickly developed a reputation in the world of "InfoSec," or information security, as being an unusually generous member of the community: A researcher in Bulgaria said Hutchins helped him track a botnet there for free. In 2017, he was invited into an initiative run by the U.K.'s National Cyber Security Centre to recruit "the best and the brightest" in cybersecurity to collaborate with the government. Hutchins maintained a hacker's natural skepticism of authority but came to believe that public and private cooperation is essential to securing the internet. The sense of power that comes with such connections could also be exhilarating: If Hutchins had information to share or a question to ask, he could quickly get in touch with British intelligence or someone at the FBI.

Hutchins at his arraignment last August. Photo: Lorenzo Franceschi-Bicchierai?Motherboard/Vice Media

Hutchins had been on a weeklong staycation last May when he woke up to reports that computers around the U.K. had been hit by a new strain of malware called WannaCry that demanded a bitcoin ransom. Such ransomware attacks had become so common that he thought little of it and left to get lunch with a friend. But when he returned, new victims were appearing by the minute: more than a dozen British hospitals, a Spanish telecom company, the Romanian Ministry of Foreign Affairs, police departments in India. The malware took advantage of EternalBlue, a Windows vulnerability discovered by the NSA, which had not reported it to Microsoft in order to use it for the agency's own purposes. (EternalBlue had recently been exposed by a group of hackers calling themselves The Shadow Brokers.) "I picked a hell of a fucking week to take off work," Hutchins said on Twitter.

Hutchins got a sample of WannaCry from a friend and began picking it apart. He quickly noticed that the code included a seemingly random domain name —iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com — that was unregistered. To Hutchins, the code suggested that WannaCry was regularly pinging the domain; if he registered it, he thought he might be able to direct the traffic to a "sinkhole," which would allow him to monitor the attack. After a quick conversation with Neino, Hutchins bought the domain on NameCheap.com for $10.69.

When Hutchins registered the domain, he unknowingly activated a "kill switch" in the code that stopped WannaCry from spreading. In the U.K. alone, the attack resulted in an estimated 19,000 canceled doctor's appointments and forced five emergency rooms to turn away patients, but Hutchins saved 92 other facilities from attack and had intervened early enough in the American workday to keep WannaCry from spreading widely in the U.S. "Everyone was clapping online," Dan Tentler, an InfoSec friend of Hutchins's, told me. "Who knew you could basically save the world by accidentally kill-switching malware?"

Two days later, a friend called to tell Hutchins his picture was in the *Daily Mail*. Hutchins had given interviews pseudonymously, as MalwareTech, but he feared reprisal from the WannaCry hackers and had taken great pains to maintain his "OpSec," hacker shorthand for operational security. (The rest of us call it privacy.) Most of his friends in Ilfracombe didn't know what he did for work, partly because he couldn't talk about it, and most of his InfoSec friends didn't know his real name. Hutchins had tried to keep pictures and information about himself off the internet, avoiding services that asked for his physical address, but he'd slipped up a year earlier when he "got way too drunk and agreed to some group selfies," which the British tabloids had found.

Suddenly, Hutchins was everywhere. (*Surf Europe* magazine: "Marcus Hutchins could well be the most famous UK surfer since Wham's Andrew Ridgeley.") With journalists staking out his home, Hutchins hid inside, slipping out once by leaping over a wall in the back, wearing a hoodie, to go to his favorite fish-and-chips shop. Eventually, he granted an interview to the Associated Press; when the reporters asked Hutchins to spell his last name, he was so nervous he left out the *n*. A month later, when he began looking into another ransomware attack and ordered his standard "Cyber Attack Survival Pack" — two pizzas and two liters of Dr Pepper — the delivery guy recognized him and asked whether he was investigating the new malware. His Twitter following quintupled, which was cool, though he tried to remain detached about it, posting a photo of the ocean with a digital-age koan: "50k new followers won't bring you happiness, but the sea will."

His reception in the cybersecurity world was even more adoring.
Hutchins delivered the keynote at a conference in Copenhagen, and at another event, when he started talking to a girl he thought was cute, he was bombarded by so many people asking him for photos that she got fed up and left. In July, during an interview with a cybersecurity website, he was asked whether black hats could make as much money "by coming to the 'good' side." Hutchins pointed out that the hackers behind WannaCry, one of the largest cyberattacks ever, had made off with just $135,503 — roughly what a malware researcher like him made as a salary without "the risk of being caught." But Hutchins had also expressed doubt that many would switch teams. Several months earlier, in a conversation about a group of black hats who had supposedly come clean, Hutchins declared on Twitter, "Bad guys who come to the good side rarely become good guys, remember that."

The six-count indictment against Hutchins accused him of building malware known as Kronos, a banking Trojan that could surreptitiously install itself on a computer and steal passwords and other information entered into financial websites. It first appeared in 2014, after Hutchins had finished school but before he had found work, and it spread in part via Kelihos, the botnet he'd been tracking when he got his job. In addition to creating the malware, Hutchins was accused of conspiring to sell Kronos to cybercriminals for $2,000 and advertising it on AlphaBay, a dark-web marketplace the FBI has since shut down.

To obtain a conviction, the government would have to prove not only that Hutchins had built Kronos but that he intended it to do harm. According to prosecutors, Hutchins admitted to creating Kronos while being questioned following his arrest at the Vegas airport. (His attorneys say he was sleep-deprived and intoxicated during the interview.) The FBI also showed Hutchins 150 pages of online chat logs in which he allegedly talked to an unidentified co-defendant about selling Kronos and how to split the proceeds. During a phone call from jail, prosecutors say, Hutchins described the chats as "undeniable." "The government usually doesn't go after someone unless they credibly could win," said Katie Moussouris, a prominent hacker who works to foster better relations with government agencies.

The cybersecurity world was stunned. It was rare for an individual hacker to become a hero, as Hutchins had, and disconcerting for that person then to be charged as a cybercriminal. Some turned on him, speculating, without any real evidence, that Hutchins had been behind WannaCry all along and had "discovered" the kill switch only after the attack had grown out of control. (The U.S. and other governments have blamed the attack on North Korea.) Researchers who worked with Hutchins were spooked. "This is bad," wrote one member of a cybersecurity forum. "We need to assume for the period he was among us, any and all traffic was compromised and could be, along with our names etc., in the hands of various adversaries."

Things got worse for Hutchins a month after his arrest, when Brian Krebs, a journalist who covers cybersecurity, published an exhaustive article connecting Hutchins to a variety of online user names — "Touch My Malware," "Da Loser," "Flipertyjopkins" — that had apparently engaged in low-level cybercrime when Hutchins was a teenager. Da Loser had bragged about a password-stealing program he had created; Flipertyjopkins posted a YouTube video explaining how to use a particular piece of malware. Krebs emphasized that the alleged crimes were "fairly small-time" and that he had found no evidence connecting Hutchins to Kronos, but the article fed rumors circulating on InfoSec forums that Hutchins's past wasn't pure.

Still, many in InfoSec were quick to defend him. "A lot of people do have criminal pasts — or criminal presents — but we also have a lot of experience with people getting arrested for no good reason," said Robert Graham, a security researcher. Hutchins had worked with law enforcement many times, including during WannaCry, when he publicly thanked the FBI for its help. Hutchins also sent a curious tweet in 2014 — "Anyone got a kronos sample?" — that suggested he had learned about Kronos along with the rest of the security community (or was trying to distance himself from his handiwork).

Some of the skepticism lay in the InfoSec community's distrust of the Computer Fraud and Abuse Act, a 32-year-old law that is behind many cybercrime prosecutions in America, including the case against Hutchins. Both law enforcement and the security community generally agree the law is antiquated — its definition of a computer cites typewriters and handheld calculators — and it has produced several questionable prosecutions. One issue has been figuring out how to handle young hackers whose intentions are not always clear. In 2010, Stephen Watt, a former programmer at Morgan Stanley, was convicted of writing code used in a credit-card-theft ring called "Operation Get Rich or Die Tryin." Watt hadn't actually deployed the malware, received no money, and claimed not to know what it was being used for. Judge Nancy Gertner, who heard Watt's case, told me she found herself in a difficult position when it came to sentencing — prosecutors argued for five years in prison, the defense wanted probation — and settled on a two-year prison sentence. "People lost money, and he deserved to be punished, but he was also a kid," Gertner said.

While the teenage exploits that Brian Krebs uncovered were troubling, many security researchers saw themselves in the allegations. "How does someone like Marcus become so talented?" Neino, his boss, said. "The best security researchers need to expose themselves to real threats. A lot of researchers hang out in underground forums and befriend criminals." Cybersecurity also has a long history of bad guys who become good. Kevin Mitnick spent five years in prison for various cybercrimes in the '90s but now runs a security company that consults with the FBI. Amit Serper, who is now 31 and helped stop a major Russian cyberattack last summer, told me that he and many others in the field had done things as a teenager that "could be counted as illegal." Nearly everyone I spoke to from the InfoSec world cited research suggesting the human brain doesn't fully form until people reach their mid-20s. Many of the most talented cybersecurity experts, they point out, honed their skills by testing boundaries as teens. "I call this period the Age of Rage," Moussouris told me. "It might be about feeling important for the first time in your life and being recognized as powerful. It's the first time you taste that feeling we all yearn for — significance."

Even prosecutors had acknowledged in court that Hutchins's alleged crimes were "historical" and allowed Hutchins full access to the internet while awaiting trial, which was unusual and suggested they no longer considered him a threat. If Hutchins made money from selling Kronos, it likely wasn't much — he allegedly complained in chat logs about how little he received — and while Kronos had hit banks in countries ranging from Canada to India, it was a relatively minor piece of malware. In a set of guidelines from 2014, the Department of Justice cited several concerns beyond innocence or guilt in determining whether to bring a prosecution under the CFAA, including the "increased need for deterrence." It seemed possible that Hutchins's intervention during the WannaCry attack had made him a visible target. Or perhaps the government was pressuring Hutchins to provide information — about WannaCry, Russian hackers, or something else — that he was otherwise reluctant to offer.

Even Hutchins's defenders say if he's guilty some punishment is in order, but his prosecution also sends a mixed message. Hutchins had been a model of public-private cooperation at a time when the government was having difficulty recruiting cybersecurity talent. (James Comey irritated the community in 2014 when he said the FBI struggled to hire people because "some of those kids want to smoke weed on the way to the interview.") Some security researchers said they would stop sharing information with the government in protest. "It just gives people in the community a feeling of persecution," Jennifer Granick, who works on cybersecurity for the ACLU, said.

While the government has tried to improve its outreach to hackers — the DOJ is hosting a panel at South by Southwest this month about teaching ethics to hackers — relatively little is being done to nudge talented young people toward the light, which could leave someone with Hutchins's skills and a still-developing moral compass feeling adrift. Around the time Hutchins was allegedly coding Kronos, he was also on Twitter trying to figure out how to get a job, asking about résumé formatting and whether to join LinkedIn. At one point, he worried that he might not be able to get a job at all. From this angle, even a critical reading of Hutchins's story could be hopeful: Having once done things he shouldn't have, he had realized that doing good was more rewarding, financially and otherwise, than doing bad. "We can fit in a car the number of people who do this for fun — the defenders of the internet," Tentler, Hutchins's InfoSec friend, said. "If you wanna have a good relationship with hackers, it's probably not a good idea to destroy their lives."

Hutchins in Los Angeles last month.

A few days after we met for beers, Hutchins and I took a walk along Venice Beach. When we had parted ways the other night, Hutchins had told me he was going to meet some friends and "get so drunk I don't remember anything." He said he'd invite me along, but he wasn't sure the others would be okay with it. "It's a bunch of InfoSec people," he said. "They're all paranoid."

While Hutchins objected to parts of the Krebs article, he admitted that "I think everyone can see I have some shady things in my past." But he didn't think this was so unusual. "Most of cybersecurity has done something they shouldn't at some point," he said. "We only talk about the people who get caught." Hutchins said he knew of one cybercriminal who masquerades as a white hat and is sometimes quoted as an upstanding security expert in the press. And, he said, other cybercriminals would sometimes disappear from forums and then pop up months later working for the government.

After we'd been on the boardwalk for half an hour, Hutchins paused and looked toward the sea. "All this time, I've never actually just walked on the sand," he said. He had gone to the waves and back to surf, but he'd never thought to just take a stroll. As we walked along the water, still wearing our shoes, Hutchins said that he'd previously felt little desire to leave Ilfracombe. His friends were there, real estate was cheap — he'd been planning to use his savings and his bitcoin earnings to pay $400,000 in cash for a large house — and there seemed to be no professional point in moving to London or San Francisco when he could stop a global cyberattack from his bedroom. But his time in L.A. had revealed a wider world, one in which he could go to multiple clubs playing the Chainsmokers, rather than the one club in Ilfracombe, and where apps would deliver food at the odd hours he liked to keep. Hutchins assumed that he would have to go back to the U.K. after the case, regardless of its resolution, and there was no telling when he would be able to return.

Most of all, Hutchins was bored, and he wanted to work again. “Not having access to my botnet-monitoring stuff is depressing,” he said. While Hutchins declined to discuss details of his case, except to maintain his innocence — the trial is still pending, though such cases often end in settlements — he feared the damage was already done. Cybersecurity is a business based in trust, and he worried that the allegations alone made him unemployable. (He had recently noticed a number of Twitter bots commenting on his case with anti-American bents, which he speculated could be someone trying to use his case to divide the American cybersecurity community.)

As we walked up to the Santa Monica Pier, Hutchins grew wistful, thinking back to moments that could have led him anyplace but here. He was convinced, for instance, that he had become a target after WannaCry, which would mean that the greatest moment of his life had led directly to the worst. The world has never been more dependent on people like Hutchins, with their deep mastery of the digital systems undergirding things the rest of us take for granted. He seemed to realize this could be both a privilege and a burden. “I liked the connections and the power,” Hutchins said as a violinist played “Tale As Old As Time” on the pier. “Now I’m not sure it was worth it.”

**This article appears in the February 19, 2018, issue of* New York *Magazine*.

**This article has been corrected to show that Eternal Blue was exposed by the hacker group The Shadow Brokers, not by Wikileaks.*

CONNECT: e sletters Faceboo T itter Instagram RSS Feedly

Privacy Terms Sitemap Media Kit Ad Choices About Us Contacts Feedback
We’re Hiring!