The Mirai Confessions

Three Young Hackers Who Built a Web-Killing Monster Finally Tell Their Story.

How to Create a Monster

Amazon, Spotify, Netflix, PayPal, Slack: all blown off the internet for millions of people. Three young hackers built a web-killing super weapon called Mirai. Then they lost control of it. This is their untold story.

BY ANDY GREENBERG
ARTWORK BY JAMES JUNK AND MATTHEW MILLER

PROLOGUE

Early in the morning on October 21, 2016, Scott Shapiro got out of bed, opened his Dell laptop to read the day's news, and found that the internet was broken.

Not *his* internet, though at first it struck Shapiro that way as he checked and double-checked his computer's Wi-Fi connection and his router. *The* internet.

The *New York Times* website was offline, as was Twitter. So too were the websites of *The Guardian, The Wall Street Journal,* CNN, the BBC, and Fox News. (And WIRED.) When Twitter intermittently sputtered back online, users cataloged an alarming, untold number of other digital services that were also victims

of the outage. Amazon, Spotify, Reddit, PayPal, Airbnb, Slack, SoundCloud, HBO, and Netflix were all, to varying degrees, crippled for most of the East Coast of the United States and other patches of the country.

Shapiro, a very online professor at Yale Law School who was teaching a new class on cyber conflict that year, found the blackout deeply disorienting and isolating. A presidential election unlike any other in US history loomed in just under three weeks. “October surprises” seemed to be piling up: Earlier that month, US intelligence agencies had jointly announced that hacker breaches of the Democratic National Committee and Hillary Clinton’s presidential campaign had in fact been carried out by the Russian government. Meanwhile, Julian Assange’s WikiLeaks had been publishing the leaked emails from those hacks, pounding out a drumbeat of scandalous headlines. Spooked cybersecurity analysts feared that a more climactic cyberattack might strike on Election Day itself, throwing the country into chaos.

Those anxieties had been acutely primed just a month earlier by a blog post written by the famed cryptographer and security guru Bruce Schneier. It was titled “Someone Is Learning How to Take Down the Internet.”

“Over the past year or two, someone has been probing the defenses of the companies that run critical pieces of the internet,” Schneier, one of the most highly respected voices in the cybersecurity community, had warned. He described how an unknown force appeared to be repeatedly barraging this key infrastructure with relentless waves of malicious traffic at a scale that had never been seen before. “These probes take the form of precisely calibrated attacks designed to determine exactly how well these companies can defend themselves, and what would be required to take them down. We don’t know who is doing this, but it feels like a large nation-state. China or Russia would be my first guesses.”

Now it seemed to Shapiro that Schneier’s warning was coming to fruition, right on schedule. “This is *the attack,”* he remembers thinking. Was it “the big one?” he asked himself. Or was it perhaps a test for the true “big one” that would hit on November 8? “Obviously, it has to be a nation-state,” Shapiro thought. “It has to be the Russians.”

For Shapiro, the internet outage was a kind of turning point: In the months and years that followed, he would become obsessed with trying to understand how someone could simply stamp out such a large swath of digital connectivity across the world, who would do such a thing, and why. But meanwhile, a little less than 500 miles west of Shapiro’s Connecticut home, in the town of Washington, Pennsylvania, another sort of observer was watching the attack unfold.

After a typical sleepless night at his keyboard, 19-year-old Josiah White sat staring at the three flatscreen monitors he’d set up on a workbench in a messy basement storage area connected to the bedroom he shared with his brother in their parents’ house. He was surrounded by computer equipment—old hard drives and a friend’s desktop machine he had offered to fix—and boxes of his family’s toys and Christmas tree ornaments.
For weeks, a cyber weapon that he’d built with two of his young friends, Paras Jha and Dalton Norman, had wreaked havoc across the internet, blasting victims offline in one unprecedented attack after another. As the damage mounted, Josiah had grown accustomed to the thrills, the anxiety, the guilt, the sense that it had all gotten so absurdly out of hand—and the thought that he was now probably being hunted by law enforcement agencies around the world.

He’d reached a state of numbness, compartmentalizing his dread even as he read Bruce Schneier’s doomsday post and understood that it was describing his own work—and now, even as a White House

press secretary assured reporters in a streamed press conference that the Department of Homeland Security was investigating the mass outage that had resulted directly from his actions.

But what Josiah remembers feeling above all else was simply awe—awe at the scale and chaotic power of the Frankenstein's monster that he and his friends had unleashed. Awe at how thoroughly it had now escaped their control. Awe that the internet itself was being shaken to its foundations by this thing that three young hackers had built in a flurry of adolescent emotions, whims, rivalries, rationalizations, and mistakes. A thing called Mirai.

PART ONE

None of the three young men who built Mirai fit the profile of a cybercriminal, least of all Josiah White, who could lay perhaps the most direct claim to being its inventor. Josiah had grown up in a rural county an hour south of Pittsburgh. He was the youngest of four children in a close-knit Christian family, all homeschooled, as his mom put it, to better "find out how God had created them and what he had created them to pursue." She describes the thin, dark-haired baby of the family as a stubborn and independent but unusually kind child, who would sit beside the new kid in Sunday school to make them feel welcome.

Josiah's father was an engineer turned insurance salesman, and the family lived in a fixer-upper surrounded by woods and farmland. As early as he can remember, Josiah followed his father around the house while he tinkered and made repairs. In 2002, when he was 5, Josiah was delighted to receive for Christmas the components of an electrical socket. Later his parents gave him a book called *101 Electronics Projects,* and he would beg his mother to drive him to RadioShack, arriving with a shopping list of breadboard componentry. Before he was 10, he was advising his father on how to wire three-way switches.
Josiah's father would take him along to their church's "car ministry," where they'd repair congregants' cars for free and refurbish donated vehicles for missionaries. Josiah would stand in the corner of the shop, waiting for the foreman to give him a task, like reassembling a car's broken water pump.

Josiah reveled in impressing the adults with his technical abilities. But he was always drawn to computers, cleaner and more logical than any car component. "You give it an input, you get an output," he says. "It's something that gave me more control." After years of vying for time on his family's computer, he got his own PC when he was close to his 13th birthday, a tower with a Pentium III processor.

Around the same time, Josiah's brother, seven years older than him, figured out how to reprogram cell phones so they could be transferred from one telephone carrier to another. Josiah's brother started to perform this kind of unlocking as a service, and soon it was so in demand that their father used it to launch a computer repair business.

By the time he was 15, Josiah would work in the family's shop after school, setting up Windows for customers and installing antivirus software on their machines. From there, he got curious about how HTML worked, then began teaching himself to program, then started exploring web-hosting and network protocols and learning Visual Basic.

As wholesome as Josiah's childhood was, he felt at times that he was being raised "on rails," as he puts it, shepherded from homeschooling to church to the family computer shop. But the only rules he really chafed against were those set by his mother to limit his computer time or force him to earn internet access through schoolwork and household chores. Eventually, on these points, she gave up. "I sort of wore her out," he says. She relented in part because a hands-on understanding of the minutiae of computing was quickly becoming essential to the family business. Josiah, now with near-unlimited computer time, dreamed of a day when he'd use his skills to start a business of his own, just as his brother had.

In fact, like most kids his age, much of Josiah's time at the keyboard was spent on games. One of them was called *Uplink.* In it, the protagonist is a freelance hacker who can choose between two warring online movements, each of which has built a powerful piece of self-spreading code. One hacker group is bent on using its creation to destroy the internet. The other on stopping them. Josiah, not the sort of kid to do things in half measures, played through the game on both sides.

Immersing himself in that cyberpunk simulation—and learning about famous hackers like Apple cofounder Steve Wozniak and Kevin Mitnick, who had evaded the FBI in a cat-and-mouse pursuit in the 1990s—cultivated in Josiah's teenage mind a notion of hacking as a kind of secret, countercultural craft. The challenge of understanding technical systems better than even their designers appealed to him. So did the subversive, exploratory freedom it offered to a teenager with strict Christian parents. When he googled a few hacking terms to learn more, he ended up on a site called Hack Forums, a free-for-all of young digital misfits: innocent explorers, wannabes, and full-blown delinquents, all vying for clout and money.

On the internet of 2011, the most basic trick in the playbook of every unskilled hacker was the denial-of-service attack, a brute-force technique that exploits a kind of eternal, fundamental limitation of the internet: Write a program that can send enough junk data at an internet-connected computer, and you can knock it offline.

The previous year, for instance, the hacker group Anonymous had responded to the refusal by Visa, Mastercard, PayPal, and Bank of America to allow donations to WikiLeaks by urging its plebes to bombard the companies' servers with data requests, creating so-called distributed denial-of-service attacks that briefly took down the companies' online services. But most DDoS attacks were less principled: the constant AK-47 cross fire of the cybercriminal internet's internecine wars and vandalism.

On Hack Forums, many hackers ran their own "booter" services that, for a few dollars a month, would launch denial-of-service attacks against anyone a customer chose—often online gaming services, to troll or sabotage rival players. Users and admins of booters talked casually of "hitting off" targets, or worse, "holding off" a service or a single user's connection, repeatedly bombarding it to prevent it from coming back online.

Some booters launched attacks from botnets, collections of thousands of unwitting users' PCs, hijacked with hidden malware to form a lemming-like swarm of machines pummeling a target with data. Other

booters used “reflection” or “amplification” attacks: If a hacker could find an online service that would respond to a query by sending back a larger chunk of data than the request itself, they could spoof the origin of their question so the service would send its answer to a victim. By bouncing a stream of thousands of questions off a server, the hacker could bombard the victim with its responses and vastly multiply their attack’s firepower.

Josiah, fascinated by the cleverness of those tricks, was naturally determined to understand them at their deepest level. He stumbled upon a blog post from a cybersecurity blogger describing a reflection attack that used the servers of the online first-person-shooter game *Quake III Arena.* Ping them with a simple “getinfo” or “getstatus” request, and the servers would send back information that included the usernames of the players on the server and the map of the level they were playing on—an answer that was nearly 10 times as big as the question and could be directed at any spoofed IP address a hacker chose.

The post was intended as a warning. It cautioned that this kind of attack could be used to take down a service with as much as 23 megabits per second of bandwidth, a pipe that seemed enormous to Josiah on his 1.5-megabits-per-second home DSL connection. A competent programmer exploiting the problem, the blog post’s author wrote, “can easily create a full-fledged attack suite in a lazy afternoon.”

Josiah took this as a challenge. He cobbled together a simple script to perform the attack and posted it to Hack Forums under his handle, “Ohnoes1479.” He asked only for anyone who used it to give him an upvote “if its good ✌” to increase the prestige of his forum profile.

Josiah didn’t think too much about the morality of his creation. After all, it took a computer offline only temporarily, right? More of a mischievous hiccup than a crime, he figured. He couldn’t use it himself anyway, because his home internet connection didn’t allow the IP spoofing the attack required. Still, as other hackers on the forum—some of whom he suspected ran their own booter services—asked questions about how to use the program and even requested feature updates, he was happy to help.

Mostly, like the technical wunderkind he’d once been in his church’s auto shop, he aimed to impress. “I wanted to make something cool,” he says. “And I wanted respect.”

In that anarchic Hack Forums scene, Josiah soon found a kindred spirit, a user who called himself “moldjelly.” In the offline world, his name was Dalton Norman. He was a teenage hacker just a year older than Josiah who was far more in touch with his rebellious side.

Like Josiah, Dalton had grown up with an engineer for a father. His dad led the maintenance team for a skyscraper in New Orleans, where the family lived. And like Josiah, Dalton had a natural technical talent.

As a preteen, he wrote cheating mods for video games that he presented on his own YouTube channel in a squeaky voice. He and his father would work in their spare time on his dad's souped-up Chevrolet Monte Carlo, which had so much horsepower that Dalton remembers the feeling of its exterior twisting as it accelerated. He says he inherited that same drive to push technology to its limits.
But far more than Josiah's, Dalton's childhood was tinged with adversity. As a small child, he had struggled with a stutter that deeply scarred him. He remembers his family laughing at him at the dinner table as he labored in vain to pronounce his younger sister's name. "It was awful and kind of contributed to me just being in my room and having low self-esteem and trying to raise it by being super good at something," Dalton says.

By the end of elementary school, to Dalton's relief, the stutter had faded away. But just as it seemed like he might enjoy a normal adolescence, his life was disrupted by misfortune on a far larger scale: Hurricane Katrina. Dalton's family evacuated to Mississippi and didn't return for more than five years. In exile one state over, Dalton found himself at a "culty" Christian private school, where students prayed before class and, as he remembers it, a math teacher assured him that Barack Obama was the Antichrist. "When I wouldn't pray or do any of that," he says, "I would get shit for it."

Dalton wrote his first program when he was 12. It was a spam tool that he used to torture a teacher he disliked, wrecking her inbox. He says he carried out his first denial-of-service attack not long after, targeting his school's network from within.

While connected to the school's Wi-Fi, he flooded its router with junk requests until the entire intranet collapsed. "It's easy to take down a network when you're inside of it," he says. Ironically, as Dalton describes it, he had gotten enough of a reputation for IT know-how that school staff asked for his help fixing the problem. He stopped his attack script, unplugged the router, plugged it back in, and showed the school administrators that it magically worked again. During another attack, however, he says he overheated the router so badly in its poorly ventilated closet that it was fried.

In his early teens, he remembers watching *The Social Network* and taking exactly the wrong message from the movie: Rather than feeling cautioned by the film's fictionalized origin story of an icily amoral Mark Zuckerberg, Dalton was profoundly inspired. "That movie basically changed how I viewed the world," he says. "It's like, with a laptop and a great idea, you can take control of your life and build something cool."

After a failed attempt to launch his own social network—he had no idea how to gain users and no budget to advertise it—he returned to hacking: He wrote a keylogger program, designed to snoop on a victim's keystrokes after infecting their PC via thumb drive. He also found his way onto Hack Forums. Soon he was running his own booter service, hiring other hackers to handle customer service so he could focus on finding new methods to amplify his attack traffic.

It was around this time that Dalton encountered Josiah, who was, he says, the smartest hacker he'd ever met. The two teens soon moved off Hack Forums to talk regularly on Skype and then later TeamSpeak, another internet conferencing service. In those conversations, Dalton eventually used his real name, while Josiah went by "Joey," a thin veneer of a pseudonym. They enjoyed competing with each other to find new denial-of-service amplification tricks. In a friendly rivalry, they'd stay up into the early morning hours, plumbing the internet for eclectic servers that they could use to multiply their attack traffic dozens and eventually hundreds of times over.

In those late-night cyberattack sessions, the two hackers say, they would typically set up their own website for target practice, or use a friend's, so that they could measure the size of the traffic they were blasting at it. At times they would clock attacks of more than 100 gigabits a second, they say—more than 4,000 times as big as the 23-megabit attack that had initially amazed Josiah. Very often they would knock their target website offline, along with the server of the hosting service it ran on, causing downtime for an untold number of other websites too.

By this time, Josiah admits, he'd become mildly intoxicated by the power of the tools they'd learned to wield, though he still considered himself a kind of innocent, exploratory hacker. "I was stupid, and I was just angry sometimes, and I wanted to see damage, at points," he says. "But it wasn't my primary motivator—for a while."

Dalton, who was already running a for-profit attack service, had no such illusions of innocence and admits—a little proudly—to using his growing arsenal of booter artillery on any Hack Forums rival who sufficiently annoyed him. In some cases, he boasts, he would "hit people off so hard" that their internet service providers would cut the victim's connection for 24 hours to avoid further collateral damage. "It was a lot of power," he says. "If someone was bullying or being an asshole, then yeah, they went offline for a while."

Both teenagers managed to hide these dalliances with illegal hacking from their families. But for Dalton, the consequences soon spilled violently into his physical world.

It began when he discovered that someone who worked for his booter service, an older kid to whom he'd foolishly given his real name, had been stealing their profits. He fired the guy. A few days later, Dalton and his family were sitting around the dinner table when a team of police officers in bulletproof vests burst through the door, screaming at everyone to get on the ground. The cops pointed shotguns at Dalton and his terrified parents and siblings, barking orders and questions.

It turned out that the police had received a spoofed 911 call. The caller had warned that Dalton had shot his mother and was now holding the rest of the family hostage. Dalton had been "swatted," targeted with the most dangerous retaliatory measure in the toolkit of nihilist teen hackers. When the police realized there was no hostage crisis, Dalton explained to the cops and his parents that an angry kid online had inflicted this situation on them—leaving out the part about his booter service. As a measure of the skewed risk assessments of his teenager's brain, his biggest fear during the entire incident was how his furious parents would punish him. He was grounded.

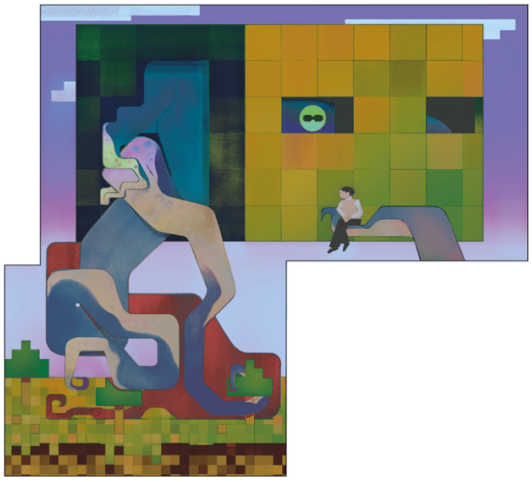
Dalton says the real lesson he drew from the incident was to tighten his operational security, no longer telling anyone in the hacking world his real name—except Josiah. "I trusted no one except for Joey," he says.

In the midst of all this, when Dalton was 15, another kind of calamity struck: His stutter came back. He says it happened when he met another stutterer at his high school. Somehow, the event triggered his brain to start tripping up his speech all over again. And the change seemed to be permanent. All the difficulty he'd had speaking as a small child, along with all the anxiety and shame that came with it, flooded back. It was, he says, "a nightmare."

Like many stutterers, Dalton found workarounds for the arbitrary lexicon of words that would halt his speech, substituting others to hide his disability. But names, which allowed no substitutions, were particularly tough. At one point, to get out of gym class, he volunteered with his high school's tech office and found that the job included delivering laptops to students. He remembers standing in front of a classroom trying to say a student's name as the entire class laughed at him. Even his own name was often impossible to get out. "It broke me," he says. "But afterward, I was just like, 'I don't care what other people think. Fuck it.'"

Dalton's stutter, he says, drove him into cybercrime with a renewed fervor. He cut ties with real-world friends, retreated to his computer, and focused his energy on hacking. His skewed teenage logic kicked in again, telling him to abandon any hope of a normal life or legitimate career. "I thought, 'No one's gonna hire me because I can't talk. How am I going to get past an interview when I can barely say my name?' " Dalton remembers.

He had, he told himself, no other option. "I have to find a way to make this blackhat thing work out."



Of the three young hackers who would go on, together, to be responsible for the biggest DDoS attacks in history, Paras Jha came to that path from the most innocent and childlike place of all: a love of M*inecraft.*

Born in Mumbai, Paras was less than a year old when his family emigrated to the US, where they eventually settled near central New Jersey. His parents demanded academic perfection, and Paras was gifted enough to easily deliver. Too easily, in fact: For years of elementary and middle school, he would read entire textbooks as soon as he got them, he says, then never study them again and ace every test.

> **Josiah told the others that he was launching the attack. Across the internet, Paras could hear the tap of the enter key on Josiah's keyboard. The world stopped.**

At the same time, Paras was aware that he had a paradoxical problem with focus. He remembers being in third grade and disassociating as a teacher spoke to him, tracing out her face in the air with his finger. That teacher later suggested to Paras' parents that he be tested for attention deficit disorder. Coming from a culture that stigmatized such a diagnosis, Paras says, his family was skeptical of the teacher's warning. His mother and father filled out the school's evaluation for learning disabilities; it came back negative, and he was never treated.

As Paras grew older, his scattered mental state meant he often forgot school assignments, and his strict parents would respond by grounding him. To pass the time, he gravitated to computers. His beloved video games were forbidden on weekdays, so he would spend hours playing with Microsoft's Visual Studio, teaching himself to program.

By his early years of high school, Paras had become obsessed with *Minecraft,* an immersive online world that essentially presents a blocky, lo-res, nearly infinite metaverse. More than playing the game however, Paras was drawn to the possibilities of running his own *Minecraft* world on an online server. He would host mini-games of tag or capture the flag, endlessly tinkering with his server's code to modify the rules. He loved to join his own world, turn himself invisible, and then observe how players responded within the

universe he controlled and changed at will. It was like watching 8-bit ants with human intelligence move around his very own ant farm.

Paras soon discovered he could make thousands of dollars using his coding skills to build modifications and mini-games for other *Minecraft* administrators. In fact, it turned out that the *Minecraft* ecosystem supported its own surprisingly high-stakes industry. Players paid small fees for access to perks and upgrades on their favorite servers, and administrators of the most popular worlds within that decentralized metaverse made as much as six figures a year in revenue. All of that money meant this innocent-seeming industry had developed a surprisingly ruthless dark side. *Minecraft* servers came under constant barrage from booters' DDoS attacks, launched by aggrieved players, competitors, and trolls. Many paid thousands of dollars a month to DDoS protection firms that promised to filter or absorb the attack traffic.

One day, Paras found himself in a Skype group chat with an acquaintance who also ran a *Minecraft* server. This person was determined, for reasons Paras can no longer remember, to take down a particular rival's world. Paras read along as the acquaintance asked another member of the chat for help—a figure by the name of LiteSpeed, who had attained a certain infamy for his denial-of-service wizardry.

Josiah had changed his handle on Hack Forums from Ohnoes1479 to this less-cute moniker about nine months after he'd joined the site, and these days he carried himself online with significantly more swagger. He was happy to oblige.

Josiah, Paras, and a few friends all entered the target *Minecraft* world, apparating into its blocky landscape full of hundreds of other players' lo-res figures. Then, over Skype, now in a voice chat, Josiah told the others that he was launching the attack. Across the internet, Paras could hear the tap of the Enter key on Josiah's keyboard. And the world stopped.

Instead of going dark or returning an error message, the universe hosted on the server that Josiah had knocked offline simply froze, as each player was suddenly disconnected and confined to their own computer's splintered version of it. Paras marveled at how he could move through that world and see other players paralyzed where they stood, or floating in midair.

That frozen state lasted for 30 seconds before the world crashed entirely. To Paras, it was a hilarious magic trick. "It felt like a secret superpower almost," he says. "Even though it wasn't me who did it, it was cool to just be in the know about what's going on."

He became friendly with Josiah and found that this talented hacker was happy to take down practically any target server that Paras asked him to, mostly just for sheer amusement. Josiah also seemed to be surprisingly open to sharing his knowledge. Having moved on from the amplification attacks he and Dalton had experimented with early on, Josiah now carried out his attacks with a botnet of thousands of computers around the internet that he'd infected with his own malware, exploiting a security flaw in the web-hosting software phpMyAdmin to turn the underlying servers into his personal army.

Later Josiah would switch to wielding an even more powerful collection of Supermicro servers that he'd hacked via a vulnerability in their baseboard management controllers, chips meant to allow an administrator to remotely connect to a server and monitor its performance. The attacks he was triggering were soon so powerful that he and his friends had difficulty even gauging their strength: Everything they'd

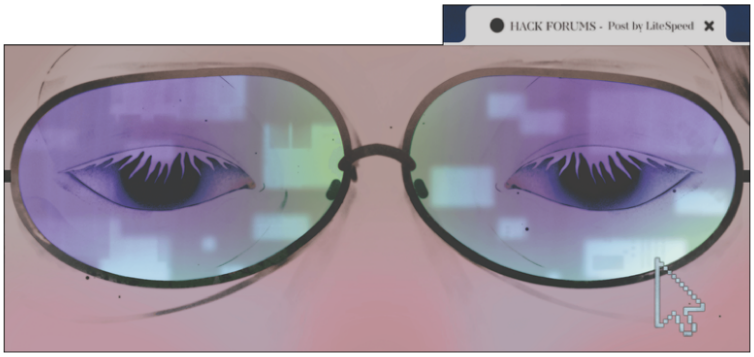
hit with it—the best-protected *Minecraft* servers, even their own measurement tools—would immediately fall offline.

Paras wanted this superpower too. Josiah was happy to help him troubleshoot his DDoS attack code and even offered thousands of computers from his own botnet for Paras to test it on. “Instead of just pressing the button, I wanted to say I had *made* the button,” says Paras. Soon he was a relatively sophisticated botnet herder with his own DDoS zombie horde.

By 10th grade, to his parents’ dismay, Paras had begun to struggle in school as subjects became more complex and his disaffected-prodigy tactics reached their limits. But online, where he went by the handle “dreadiscool,” he embraced his new godlike capabilities with roguish abandon, knocking off targets on the slightest whim. He and another friend would even sometimes find the phone number for a company that hosted certain *Minecraft* servers, call their business line from a burner number, and verbally taunt them as Paras launched a DDoS attack that ripped their machines offline.

Somehow, the rule-following, high-achieving kid from a strict immigrant household had become a rampant online vandal. But at that point, Paras says, it was never quite clear to him—or Josiah, or Dalton—how serious the consequences of their attacks might be. They were, after all, still just taking some computers off the internet, right? “Like, the servers come back online,” Paras says. “You wake up the next day and you go to school.”

At other times he would almost check himself, coming to grips with his spiraling behavior. He remembers sitting in the bathroom of his parents’ house just after taking down one of the biggest *Minecraft* servers, Hypixel, and realizing that if he kept going, he was bound, sooner or later, to get arrested. “Don’t get sucked into it,” he told himself. “Don’t get sucked into it.”



Paras got sucked into it. They all did.

In particular, Josiah, the Christian homeschooler who’d once kidded himself that he was a harmless hacker-explorer or a Wozniak-style prankster, had taken a rapid, step-by-step slide into moneymaking cybercrime. Under his LiteSpeed handle, he’d begun selling his amplification techniques to known booter service operators for a few hundred dollars a customer, spending most of the money to rent servers in remote data centers to further his hacking. He reverse engineered Skype’s code to find ways of extracting users’ IP addresses, the identifiers for their home internet connections that could allow them to be directly DDoSed. Soon he was selling this IP-extraction tool on a per-use basis to his fellow hackers and booters.

When one of his friend's would-be victims bragged that he couldn't be hit offline because he had a dynamic IP address that changed every time he rebooted his home router, Josiah figured out he could use a traceroute command to see the IP address of every router between that target and his internet service provider. So he and the friend started hitting the computers farther upstream in that network, going after the bigger arteries that fed data to and from his computer instead of the capillaries that linked to his home machine, until all of those routers were unresponsive too. This indiscriminate tactic, as far as they could tell, took out the internet service for the target's entire town, all just to prevent him from dodging their attack.

Each step, Josiah says, felt small enough that, like the mythical boiling frog, he barely noticed the change in moral temperature. He'd found something he was very good at—better than perhaps anyone he knew. And he wasn't, he told himself, carrying out hardcore cybercrime like breaching networks or stealing credit card data. Another Hack Forums user reassured him that the FBI cared only about botnets bigger than 10,000 computers, a story he naively accepted. "I rationalized a lot of it away," Josiah says. "The pot was boiling."

In early 2014, when Josiah was still 16 years old, he dialed the temperature up another fateful degree with the creation of a powerful new form of botnet. It began when a friend pointed out to him that home routers, aside from making good targets for DDoS attacks, could themselves be hacked and potentially turned into botnets' zombie conscripts. In fact, many routers still used an old protocol called telnet that allowed administrators to remotely configure them, sometimes without the need for any authentication or else requiring only default credentials, like the password "admin." All those routers represented countless thousands of hackable devices, in other words, waiting to be taken over and added into Josiah's army.

The catch was that the routers were small, simple gadgets that used cheap, low-performance embedded-device chips—not the kind of system that most hackers were accustomed to exploiting. But Josiah was never one to be daunted by the task of learning the arcane details of a new machine. He started from scratch, learned to write the native language of routers' ARM chips, and built a compact piece of malware that could be installed over telnet onto the relatively dumb devices to make them obey his attack commands.

The routers' operating systems didn't normally allow software to be installed on them. But Josiah figured out that they did have an "echo" command that could write out any line of text that you typed into a new file. He used that command to copy his code, line by line, into a file small enough to fit into the routers' few megabytes of memory. The feat was the equivalent of assembling a model ship inside a 12-ounce bottle. He called the code Qbot.
Qbot was Josiah's first foray into hacking the so-called internet of things, the vast universe of internet-connected devices beyond traditional computers, from security camera systems to smart appliances, that would turn out to be ripe for exploitation. Even in this first, crude attempt, it was immediately clear that Qbot was a potent new weapon.

Josiah could see the power he'd stumbled into: There seemed to be many thousands of vulnerable routers online that Qbot could commandeer. He was initially more careful with this creation than he'd been with his previous coding projects, keeping Qbot's code private and sharing it only with his friends: Dalton, Paras, and a few other young hackers who had formed a loose network and hung out on Skype and TeamSpeak. But Josiah made the mistake of also giving the code to one other contact. The guy went by the name "vypor" and, Josiah says, had a reputation for trading in other hackers' secrets as a means of

impressing more talented acquaintances. Vypor immediately began trading Qbot for favors and clout with, it soon seemed, his entire contact list.

When that betrayal became clear, Dalton retaliated on Josiah's behalf by hiring a rapper through the gig-work service Fiverr to record a profanity-laden track brutally mocking vypor's lack of coding skills. The diss track was uploaded to YouTube. Vypor immediately responded by threatening to swat all of them: Dalton, Josiah, even Paras, who had only recently joined the group.

All three of the young hackers were terrified of being swatted—or swatted again, in Dalton's case. They agreed that their best bet to protect themselves was to knock vypor offline and hold him off as long as possible. If he couldn't reach a VoIP service to spoof a call to the police, their short-term reasoning told them, he couldn't swat anyone. Maybe they could at least enjoy the weekend before he brought armed police to their doorsteps.

So all of them, together, bombed vypor with every DDoS tool they had. For days, they repeatedly hit not only his home connection but also routers two and three steps upstream, using Qbot and every other botnet and amplification technique they'd learned to wield. The three believe they probably blasted vypor's entire town off the internet, though they never got confirmation aside from seeing the entire chain of network devices stop responding to their pings.

Regardless, the attack seemed to serve its purpose. Vypor disappeared from the scene and never bothered them again.

Allison Nixon, who would become one of the first security researchers in the world to fully understand the dangers posed by weaponized routers and internet-of-things appliances, had no idea who Josiah White was. But she knew LiteSpeed.

At the beginning of her career in New York a few years earlier, Nixon had worked the night shift in the Security Operations Center of Dell's SecureWorks subsidiary, essentially as the cybersecurity equivalent of a patrolling night watchman. A petite, hoodie-wearing security analyst in her early twenties, she monitored the company's clients' networks for attacks in real time and investigated them just enough to know whether to escalate to someone more senior. "Kind of a grind," she remembers.

But she was curious about where all these daily, wide-ranging hacking attempts were coming from. So in the long stretches of downtime between alerts, she started googling and was amazed to discover Hack Forums, a platform on the open web where young digital deviants were bragging about their attacks and brazenly selling their toolkits. She found booter services especially shocking: how publicly, and cheaply, these miscreants sold a kind of cyberattack that could cost companies millions of dollars a year and often made her and her colleagues' lives hell. Many of the young hackers doing this damage could even be identified, thanks to their rash public posting, sloppy operational security, and the frequent "doxing" of rivals—digging up and outing another hacker's real identity. But no one seemed to be doing anything to stop them.

As Nixon lurked longer on the forum, she could see that most hackers on the site weren't actually developing their own techniques. Instead, almost all of their tools seemed to trickle down from just a few skilled individuals. LiteSpeed was one of them. His attack amplification tricks and bot infection tools had established him as a kind of Hack Forums alpha, an unmistakable standout in the scrum. "Sometimes you

kind of get a gut feeling when you're tracking someone that they're going to blow up in one way or another," she says. "I knew I wanted to keep an eye on him."

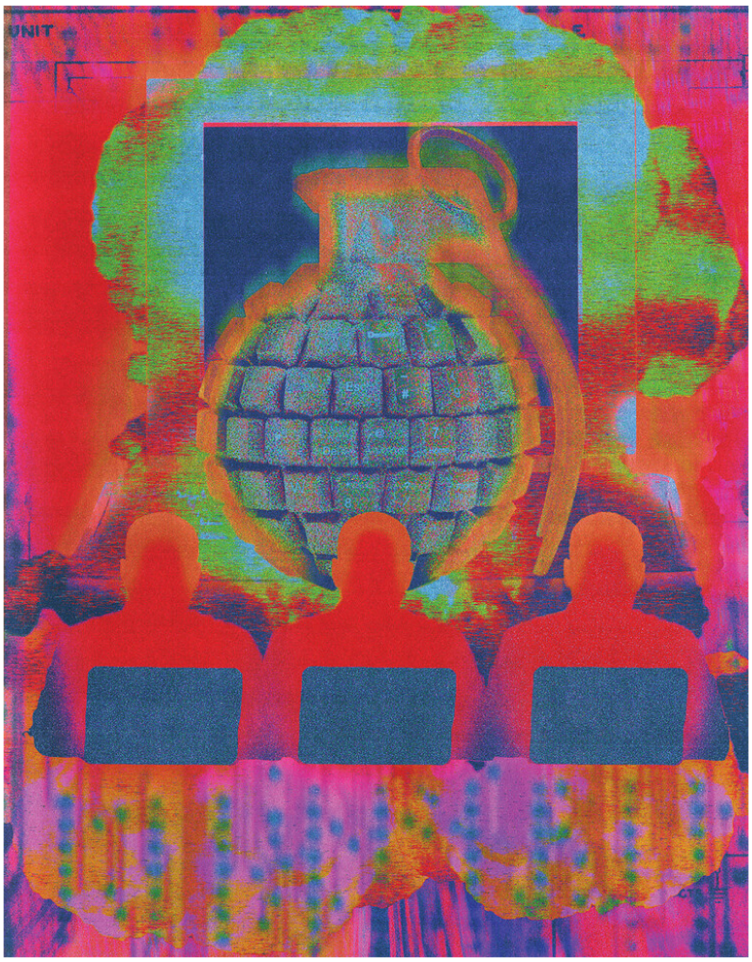
Nixon says the more senior researchers on SecureWorks' counterthreat team had little interest in DDoS attacks, which were considered primitive compared to the cutting-edge intrusion methods that they focused on. But Nixon was fascinated by the anarchic *Lord of the Flies* world of young hackers building an entire cyberattack industry, seemingly with no repercussions or even notice from law enforcement.

Nixon partnered with a university researcher and began testing out booter services on Hack Forums, barraging a guinea-pig target server with waves of junk traffic. Some of the attacks topped 30 gigabits a second, easily enough to knock someone offline or cripple a website.

By 2014, Nixon had quit the security operations center and taken a job hunting hackers full time, but she couldn't let go of her DDoS obsession. At a meeting in Pittsburgh of cybercrime fighters, called the National Cyber-Forensics and Training Alliance, she stood before a room of several dozen researchers, academics, and law enforcement officials. With the participation of an internet service provider that had just presented its DDoS protection plan, she demonstrated that she could click a button on a booter website and launch a cyberattack at will—a daring move in front of a crowd of federal agents and prosecutors.

> **"We'll do it a few times," Josiah thought. "We'll cause trouble for a little bit, and then we'll just forget about it. We'll stop."**

One agent from the FBI's Pittsburgh field office, named Elliott Peterson—a former Marine from Alaska who'd recently led the landmark takedown of a Russian-origin cybercriminal malware and botnet known as GameOver ZeuS—was particularly impressed. He and Nixon talked about the booter problem. She pointed out how freely the services operated, how many of the culprits were identifiable, and how powerful any intervention in that world might be. And she shared her growing sense that, if the larger problem were left unchecked, it would pose a serious threat to the operation of the internet.



For Josiah, the conflict with vypor was a wake-up call. He felt he'd narrowly avoided watching his secret hacking hobby burst into his peaceful family life. For more than a year, he backed away from Hack Forums and let his LiteSpeed handle go dormant. But he continued to chat with his friends Paras and Dalton, and the three of them began sharing a rented server for coding experiments and internet scanning, which they referred to as the Fun Box.

Paras, meanwhile, continued his free fall into hacker nihilism. In the fall of 2014, he started college at Rutgers and found himself alone and unmoored. He had looked forward to delving into the study of computer science and was appalled to learn that he would have to enroll in other kinds of courses that, to him, seemed like months of wasted time and tuition. Even the computer science exams, to his horror, had to be taken with pencil and paper. "I absolutely hate college," he texted a friend. "There is absolutely nothing for me here."

He sank into a malaise and gained weight, sometimes eating a large Papa Johns pizza in one sitting. He couldn't sleep at night and often couldn't find the motivation to get out of bed, much less go to class. Aside from his roommate, he had little social contact in the real world—certainly nothing that could compare to the rich, battle-tested friendships he'd built online.
Paras was particularly frustrated to find he couldn't even get into some of the computer science courses he wanted to register for: Third-and fourth-years got first dibs, and only once their registration round was over did second-and first-years get a chance to choose from the leftovers.

But Paras soon realized he had just the superpower to right this injustice: He could use one of his botnets, built mostly of vulnerable home routers, to blast the entire registration system offline until it was his turn.

He took a trollish delight in tormenting the institution that he felt was tormenting him. Under the Twitter handle @ogexfocus, accompanied by a picture of a ghostly mask, Paras publicly taunted his target. “Rutgers IT department is a joke,” he wrote in a public manifesto, bragging, after three attacks in succession, about crushing the university’s network “like a tin can under the heel of my boot … I’m fairly certain I could run circles around all of you with my eyes closed and one leg amputated.”

When dreaded exams rolled around, he tore down Rutgers’ network again to delay them, buying himself a few more days of miserable procrastination. Later, he took the network down to prevent his parents from seeing his increasingly horrendous grades. “I was feeling very frustrated—I guess with myself—and lashing out,” he says.

On one occasion in the spring of 2015, Paras totaled the Rutgers network so thoroughly that he had to text Josiah to ask him to continue the attacks on his behalf. “Admiral can you execute my command?” he wrote in the jokey, naval-themed slang they’d developed. The outages persisted long enough that some Rutgers students later demanded a tuition refund.

Paras enjoyed the sense of control the attacks gave him, watching their cascading effects on the university the same way he’d invisibly watched players respond to his tweaks of *Minecraft* worlds years earlier. But when the attacks were over, his problems were still there. By his second year, it was clear to Paras that college wasn’t working for him.

Around the same time, he had started batting around an idea with Josiah that seemed like a way out: What if they founded their own startup offering DDoS protection, to defend paying customers from exactly the sort of attacks that they had become so expert at launching?

To Josiah, it made perfect sense. He understood DDoS attacks on a deep technical level—he had, in fact, built or at least used many of the attack tools that other DDoS protection firms were combating daily—and Paras had built a reputation as a skilled programmer, particularly among *Minecraft* server administrators, who might be a good initial customer base.

Paras borrowed $10,000 from his father, and he and Josiah used it to cofound a company: ProTraf Solutions, short for “protected traffic.” They had seen other firms struggle to defend customers from new forms of DDoS, and they were sure they could do better.

It wasn’t so simple. After launching ProTraf, they realized their potential customers didn’t often shop around for DDoS protection. Typically, they didn’t feel the need to switch providers unless the one they already had was failing to shield them from an attack, which occurred only rarely. Meanwhile, the bandwidth Josiah and Paras had rented on servers around the world—the cushion they would use to absorb attack traffic aimed at customers—was quickly eating through their capital.

Soon they came to an idea. Only when customers were actually knocked offline would they consider switching to ProTraf.

Maybe the two young partners just needed to hurry this process along. “We could wait for one of these outages,” Josiah says, “or we could *cause* one of these outages.”

They agreed: They would use their own DDoS attacks to hit off their competitors’ customers—just enough to get their own fully legitimate business on its feet, of course. “We’ll do it a few times,” Josiah remembers thinking. “We’ll cause trouble for a little bit, and then we’ll just forget about it. We’ll stop.”

Josiah and Paras began building the new attack botnet they’d use in what would become—whatever story they told themselves—a kind of DDoS protection racket.

The two teenagers used Josiah’s old Qbot code to reinfect a new army of thousands of routers and started wielding it to target their rivals’ clients—all *Minecraft* servers—easily obliterating their protections. For a while, this veiled extortion scheme actually worked. More than a dozen *Minecraft* administrators, desperate to get back online, did switch to ProTraf, paying $150 or $200 a month each.

It still wasn’t enough. They’d expanded too quickly, buying infrastructure that was eating up their capital faster than their revenue could replenish it. And they found that when their attacks stopped, some customers switched back to their competitors—perhaps because they sensed that the attacks, timed so closely to the launch of this new startup, had been a little too convenient. “People had their suspicions,” Josiah says.

Josiah was still working at his family’s computer repair business as he struggled to get ProTraf on its feet. When he wasn’t helping customers there, he resorted to making phone calls to drum up sales. He figured if his father and brother could pitch customers and build a business, so could he. But no one who picked up the phone wanted to listen to this fast-talking teenager selling a mission-critical security service. The calls were dead ends, and Josiah came to loathe making them.
Just around a year after launching, in the late spring of 2016, ProTraf was flaming out. For Josiah in particular, the company’s looming death was hard to accept. His parents had been so proud of his business ambitions: He seemed to be making good on his enormous potential, following in his family’s entrepreneurial footsteps. Was he really going to admit that he’d already failed? He felt trapped and ashamed.

So Josiah began to consider other sources of cash flow. A friend from the hacker scene had been impressed with his rebuilt collection of Qbot-infected routers. He asked whether Josiah might be willing to build a new DDoS botnet. If so, he would have customers lined up to pay thousands of dollars in bitcoin for access to it.

Josiah suggested to Paras that they could accept the offer and build a new, even bigger botnet, renting slices of its attack power to the highest bidder in a last-ditch attempt to keep ProTraf alive. It would essentially mean turning the company from a protection racket into a front for their new, real business: selling cyberattacks as a service.

“Sounds ill ey gahl,” Paras joked. *Sounds illegal.*

“Eh,” Josiah wrote back. “Kinda.”

To build the chief weapon of their secret DDoS-for-hire sideline, Josiah and Paras started from scratch. A few years had passed since Qbot's creation, and they both had a few new ideas of how to infect and commandeer a vastly larger collection of internet-of-things devices.

In the time since Josiah's original Qbot code had leaked—thanks to Josiah's old friend vypor—the hacker community had been steadily upgrading it. Some versions had now been redesigned into "worms": Infected routers would automatically scan for other vulnerable devices and try to hack and infect them, too, in a self-spreading cycle. But when Josiah and Paras examined those newer botnet systems, they seemed inefficient and unreliable. Someone else's hacked router was an unwieldy vantage point from which to find vulnerabilities in new machines. Plus, that decentralized setup made it slow and difficult to upgrade their bot software.

So instead, they designed a more centralized, three-step structure. Their infected machines would scan for other hackable devices—using a new system they say was as much as a hundred times faster than the bootleg Qbot worms they'd previously seen—and then report the vulnerable gadgets they found to a "loader" server, which would hack the machines via telnet to install their malware. Then a separate command-and-control server would shepherd those malware-infected bots, periodically sending new commands for which targets to attack.

Paras and Josiah were surprised to discover just how powerful this new automated zombie recruitment process turned out to be. Josiah remembers leaving the system running overnight and waking up to find 160,000 freshly brainwashed routers ready to do his bidding—far more than he'd ever controlled before. When he saw the scale of what they were building, Josiah's plan—raise some money with a few cyberattacks, then return to ProTraf and go straight—began to seem like a wasted opportunity, a waste of his talents. "This is cool," he remembers thinking. "This is innovative. No one else is doing this."

As their botnet's size exploded, Josiah suggested to Paras that they would be able to rent even small fractions of their firepower to attackers for $2,000 or $3,000 a month, easily topping $10,000 in monthly revenue.

"Lol," Paras wrote back. "And how big does the armada have to be."

"That wont be a problem," Josiah responded.

Seeing their botnet grow so deliriously large so quickly had now triggered in Josiah an old impulse, purer than any profit motive. "What are the limits here?" he began to ask himself. "How far can we spread this thing?"

Naturally, he turned to his old friend Dalton, who had always shared that urge to push the technological envelope. Josiah and Paras agreed to cut Dalton in on shared control of their growing creation, letting him sell access to a part of it through his own booter service. In return, Dalton would contribute his hacking skills to finding new populations of devices to add to their horde.

To maximize their malware's footprint, Dalton began to plumb the teeming vulnerabilities of the internet of things. He dug up tens of thousands more gadgets across the world with unpatched flaws, machines that went far beyond home routers: Smart appliances such as online fridges, toasters, and light bulbs all became part of their agglomerated mass of raw computing power. All these eclectic digital objects had the advantage of being relatively greenfield territory. While countless hackers vied for control of

traditional computing devices, like PCs and even routers, many of these newer devices remained untouched by malware and uncontested.

Surveillance cameras' digital video recorder systems, with hardware capable of processing large video files, turned out to be especially strong new recruits. Some scans even turned up more exotic hackable devices, like internet-connected industrial cement mixers and municipal water utilities' control systems. (The three hackers say they did avoid hacking those industrial devices for fear of being mistaken for cyberterrorists.)

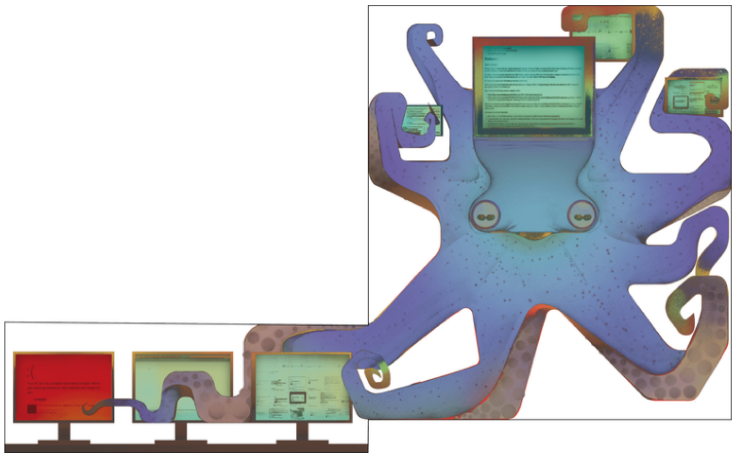
They settled into a workflow. Dalton would scan for new species of exploitable devices and write code to infect them. Josiah would refine Dalton's code and create software to take control of new additions to their menagerie of networked gadgets.

Paras, meanwhile, focused on the administration software that ran on their command-and-control server—its own complex programming task as their botnet grew to nearly 650,000 devices. He sensed that the scale of their creation would soon draw attention, and he took it upon himself to create a trail of misdirection to hide their identities from public scrutiny. To advertise the botnet, Paras created new sock-puppet accounts with names like OGMemes and Ristorini on Hack Forums, Skype, Reddit, and Jabber. He then created a collection of fake "dox" linked to those handles—the posts that hackers typically use to out rivals' real identities, but in this case all pointing at people whom Paras had chosen as patsies.

To make their connection to the botnet's command-and-control server harder to trace, Josiah found a vulnerable server in France that they could hack and use as a jump point, connecting to that hacked machine only through the anonymity software Tor, which made it look like that computer's owner was the real mastermind. The machine was actually a "seed box," a server left online to continuously trade in pirated movies over the BitTorrent protocol.

The French server, in fact, was filled with anime videos, a subject Paras knew something about. He was a fan of the psychedelic animated Japanese show *Mirai Nikki,* in which a teenage outcast discovers he's part of a battle royal among 12 owners of magical cell phones, and eventually—spoiler alert—uses his phone's powers to become the god of all space and time. The show, Paras had texted a friend, "literally defines the genre of psychological thrillers."

Paras knew that the file name for their program, now running on an ever-increasing base of hundreds of thousands of devices worldwide, would soon be a subject of notoriety. So in keeping with their work to pin the botnet's creation on a random anime collector, he chose a suitable name. All the better that it also evoked a cyberpunk superweapon brought back to the present by a time-traveler, an instrument for which the world was wholly unprepared: *Mirai.* In Japanese, it meant "the future."



To Allison Nixon and any other security researcher observing it from the outside, the advent of Mirai initially looked less like the rise of a new superpower than the start of a world war—one where the battlefield was the internet's multitudes of insecure gadgets.

In 2014 and 2015, the years leading up to what she would call "the battle of the botnets," Nixon began noticing that groups of nihilistic young blackhats with names like Lizard Squad and vDOS were picking up LiteSpeed's leaked Qbot code and then selling access to their own hordes of zombie devices, or using them to terrorize and extort online gaming services. So Nixon, who around this time started working at the security firm Flashpoint, created "honeypots"—internet-connected simulations of vulnerable devices designed to be infected by the hackers' bot software, acting as her own spies amid the botnets' ranks. The result was a real-time intelligence feed revealing the booters' commands and intended targets.

It was in early September 2016, while monitoring those botnet honeypots, that Nixon and some colleagues spotted an intriguing new sample of code that was infecting routers and internet-of-things gadgets: the one the world would come to know as Mirai.

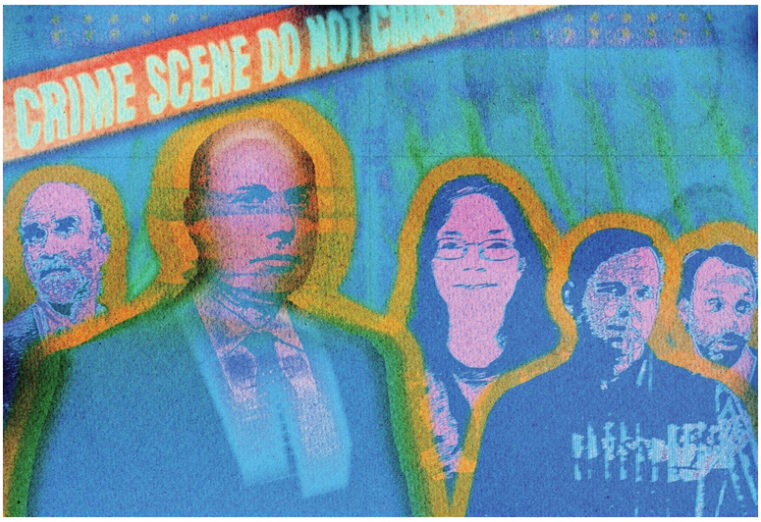
This new code seemed capable of detecting when it was running on a honeypot instead of a real device and would immediately terminate itself when it did. So Nixon and her coworker ordered a cheap DVR machine off of eBay, connected it to the internet, and watched the device—they nicknamed it the "sad DVR" due to its life of victimization—get infected over and over again by Mirai and its competitors.

In fact, unbeknownst to Nixon, Mirai's creators were by then locked in an escalating turf war with vDOS, a competing botnet crew, which had built an especially large army of hacked machines using an updated version of Qbot. Both the Mirai and vDOS teams had designed their bot software to identify and kill any program that appeared to be their rivals', and the two botnets began vying for control of hundreds of thousands of vulnerable machines, like warlords repeatedly conquering and reconquering the same strip of no-man's-land.

Soon the Mirai crew and vDOS resorted to anonymously filing abuse complaints with the companies hosting each other's command-and-control servers, forcing them to build new infrastructure. At one point, a company called BackConnect, which had been hosting Mirai's server and was run by acquaintances of the Mirai team, came under a DDoS attack from the vDOS crew. To Nixon's shock, BackConnect responded by using a so-called BGP hijack—the highly controversial tactic of essentially lying

to other internet service providers to misdirect a wide swath of traffic—to effectively pull vDOS's command-and-control server offline.

Soon, Paras, Josiah, and Dalton got tired of the endless tit for tat. They reprogrammed Mirai, allowing it to sever the telnet connections on the victim devices—thus making them harder to update but shutting out vDOS and any other rival from easily reinfecting those machines. That seemed to do the trick: To the Mirai team, it appeared vDOS had given up. (In reality, their adversaries had been questioned by law enforcement and later arrested.)



(L to R) Bruce Schneier, Elliott Peterson, Allison Nixon, Brian Krebs, and Scott Shapiro.

Nixon remembers the feeling she and her team of researchers had as they watched Mirai win that war and come to dominate the internet's mass of vulnerable devices. Once, that messy landscape had been infected with a rich diversity of malware species. Now, for the first time she had ever witnessed, all of that malevolent code seemed to go quiet as Mirai's superior infection techniques took hold of hundreds of thousands of networked devices across the globe. "From our perspective, it was like this new apex predator was prowling the savanna, and all of the other animals had disappeared," says Nixon. "From that point forward, we were on the hunt for this monster."

For much of the cybersecurity research community, the purpose of this gargantuan botnet still remained unclear. They couldn't know that Josiah, Dalton, and Paras had opened Mirai for business and put its services up for sale—that the monster Nixon was hunting was, itself, on the hunt for its first victims.

PART TWO

For Brian Krebs, September 22, 2016, was an inconvenient day to become the target of the most powerful DDoS botnet in history.

A construction crew had been replacing the siding on Krebs' rural house in Northern Virginia all morning. The incessant hammering was freaking out his dog, who responded as if barbarians were laying siege to their home. Krebs worked as an independent investigative reporter and security researcher—one of the best known in the cybersecurity industry. He had no workplace to escape to. "I was already losing my mind," Krebs says.

It was only a little later that day, Krebs says, that it started to become clear that his dog was not wrong. He was, in fact, under siege. And the barbarians were winning.
Two nights before, Prolexic, the service that provided his DDoS protection, had warned him that something was amiss. His website, KrebsonSecurity, had been hit with an attack that peaked at a mind-boggling 623 gigabits a second, according to Prolexic's measurements. The company had never seen an attack even half that big. But it had heroically managed to absorb the traffic, the Prolexic rep told Krebs, and his site had stayed online.

"Holy moly. Prolexic reports my site was just hit with the largest DDOS the internet has ever seen," Krebs tweeted that night. "Site's still up. #FAIL."

Krebs prided himself on his work hunting cybercriminals, a role in which he was nearly peerless in the world of journalism and one that had made him plenty of enemies. He'd been swatted by a target of his investigations and once had someone ship dark-web heroin to his house in an attempt to frame him. DDoS attacks from aggrieved subjects of his reporting were nothing new. But taunting the source of this particular attack, he now realized, had perhaps been ill-advised.

For two days, he continued to get notices from Prolexic that the massive DDoS was still going. In fact, whoever was barraging his server had persistently switched tactics throughout that time, firing new forms of data designed to be harder for Prolexic to filter out, or targeting machines further upstream. "These guys were real bastards," Krebs says. "They were throwing the kitchen sink."

Amid all this, more than 36 hours after the attack had begun, a member of the work crew at Krebs' house managed to kick his satellite dish, knocking out his home's internet connection. He tried to tether his computer to his cell phone, but its bandwidth was too spotty. And the attack kept coming, an overwhelming, sustained tsunami of malicious ones and zeros.

Krebs was still struggling to get online on the afternoon of the 22nd when he got another call from Prolexic. This time the company told him, in polite but clear terms, that he'd better find a new source of DDoS protection. They were dropping him. One of the biggest DDoS defense firms in the world could no longer handle the scale of the data torrent barraging his site.

Krebs got in his car and drove to a local business's parking lot to try to find a stable Wi-Fi connection for his laptop. From there, he called his web-hosting provider to warn that, without Prolexic's layer of defense, it was about to get hit with an unfathomable wall of digital pain. He suggested that rather than allow all its customers to be taken offline, it should instead configure his website to point to a nonexistent

IP address, essentially routing the attack traffic—and anyone trying to visit his site—into "a hole in the ground."

The hosting company took his advice. KrebsonSecurity.com instantly dropped offline. It would remain that way for days to come, as Mirai loomed, seemingly ready to obliterate the site again the moment it resurfaced.

For Krebs, being successfully censored by cybercriminals was a wholly new experience. "Someone just took my site offline," Krebs remembers marveling. "And there's nothing I can do about it."

Josiah, Dalton, and Paras had unlocked their superweapon, and already it seemed there was almost nothing on the internet that could withstand it.

When Krebs tweeted that his website had been hit with "the largest DDoS the internet has ever seen," he was almost right. Mirai had actually struck the French internet provider OVH around the same time with an attack that had reached the even more shocking volume of a terabit per second. The botnet's hundreds of thousands of hacked devices had also quietly KO'd a web-hosting firm and a *Minecraft* service in August with attacks that were nearly as large but had gone mostly unnoticed by the security world.

Within just a few months of launching their fully operational Death Star and making it available for hire, the three hackers—all still too young to legally drink alcohol—had assembled a small but devoted collection of clients. A fellow hacker who went by the handle "Drake" allegedly acted as a kind of sales rep: He would periodically hit off arbitrary targets as a form of marketing, to demonstrate Mirai's bristling firepower to potential paying customers. One such patron, who claimed to be in Russia, had rented Mirai to launch attacks against rivals in the cybercriminal web-hosting world, knocking out his adversaries' sites. Their most frequent user seemed to be a hacker in Brazil, who repeatedly and inexplicably rented access to Mirai to fire off attacks at the network of the Rio Olympics, at one point bombing it with more than a half terabit per second of traffic.

Paras himself used Mirai a couple of times against his old whipping boy, the Rutgers IT department, mostly just for vengeful fun. On another occasion he briefly tried using it for straightforward extortion against one of their former ProTraf customers, slamming a *Minecraft* server with a Mirai attack and then demanding a bitcoin payment. In an attempt to make the connection to ProTraf less suspect, he even copied his own ProTraf email address as a recipient of the ransom note. The company didn't pay. Josiah disapproved of Paras' extortion attempt, and they never tried it again.

It was their Brazilian customer, Paras says, who had decided to DDoS Krebs into oblivion. Paras woke up that day, read news stories about the monumental attack on Krebs—by far the most high-profile Mirai victim to date—and instantly felt a mix of excitement and dread in the pit of his stomach. "This had better not have been our botnet," he remembers thinking. He checked their user logs. "It was our freaking botnet."

After the Brazilian's earlier attacks on the Olympics, Paras and Josiah had decided this user was perhaps a little too reckless in his targeting. They'd attempted to limit his access to Mirai, ending his sessions after just 10 minutes. But Paras saw that the nihilistic Brazilian had simply manually restarted the attack on Krebs' site again and again throughout the night—and he was still going.

Paras messaged Josiah and Dalton, and they jumped onto an emergency call on a private, encrypted VoIP server. They all agreed: Annihilating the website of a very well-known journalist had crossed the line beyond helpful marketing into a kind of attention they didn't need—the kind that got you arrested. "You don't want to poke the bear," says Josiah. "This was a pretty big poke."

By this point, too, they were all 19 or older. They were adults, carrying out an extremely visible criminal conspiracy. The heat Mirai was now bringing them, they began to realize, wasn't worth it. And despite all the chaos it had caused in its early months of life, Mirai had made only a small fraction of the money Josiah hoped it would: about $14,000 worth of cryptocurrency in total. Even the biggest DDoS attacks in the world were, for their perpetrators, a relatively cheap commodity.

They had only just launched this world-shaking creation. Now they already needed an exit strategy. It was Paras who, a day or two later, suggested a new idea. Their "Russian" customer had, despite renting occasional access to Mirai, suggested to him that DDoS was a bad business. Not enough money. Far too noisy. He'd advised they instead consider partnering with him to use their botnet-building skills for a much stealthier and more lucrative opportunity: click fraud.

Put all those hijacked machines to use quietly clicking on pay-per-click web ads instead of pummeling victims, Paras explained, and they could make tens of thousands of dollars a month by invisibly defrauding advertisers, a far less disruptive form of cybercrime. Josiah and Dalton agreed they should start to transition away from the cyberattack-for-hire industry and into this more respectable black-market business.

But they couldn't quite bring themselves to kill their monster just yet. Instead, Paras and Josiah, who held more control of Mirai's targeting than Dalton, attempted to add the IP address for KrebsonSecurity.com to a block list that would at least end the attack—though they'd find in the days to come that their efforts to restrain their least predictable customer had failed again.

Regardless, by that point it was too late. Josiah was right. They had poked the bear. Now it was wide awake.

Elliott Peterson was sitting thousands of miles to the northwest in the FBI's Anchorage, Alaska, office when he read the news that Brian Krebs, a journalist whose work he knew well, had been wiped off the face of the web.

He was shocked to learn that an attack could hit Prolexic—a firm owned by the internet giant Akamai, whose entire business model depended on handling giant flows of traffic—so hard that it could essentially jam one of the biggest digital conduits in the world. And all to silence a journalist. Peterson knew that he'd just witnessed the start of a new era. "All of a sudden, the world woke up to the fact that someone's throwing around a terabit of traffic," he says. "No one was ready for that."

Two years had passed since Peterson had seen Allison Nixon's live booter demonstration at a Pittsburgh cybercrime conference. He'd since returned to his native Alaska, taken up an assignment at the FBI's smallest field office, and turned it into an unlikely hub for takedowns of botnet and booter operations. Just days earlier, he'd learned of the detainment in Israel of vDOS's two administrators, the rival hackers with whom the Mirai crew had recently been at war. Peterson had been involved in the investigation of vDOS for months. The resulting bust was, in fact, the real reason that Mirai had definitively won that rivalry.

Now Peterson was disturbed to see that the takedown had only cleared the field for someone wielding an even bigger weapon. He knew he would need to take on this case, too.
Working from his cubicle in the "cyber atrium"—a glass-roofed enclosure that houses the handful of FBI agents focused on cybercrime inside Anchorage's brutalist, red-brick federal building—he started digging. He and Nixon had helped create an industry working group called Big Pipes that dealt with DDoS attacks, and he immediately learned from contacts there that Akamai had been hit by a mysterious new botnet called Mirai.

Even in the midst of Krebs' unfolding crisis, Peterson understood that for the Anchorage office to take on this new monster, he'd first have to get over a legalistic hurdle: He needed to prove that either its victims or creators were in Alaska. Krebs and Akamai were thousands of miles away. So he realized that he would have to somehow find Mirai-infected devices in his own state. Luckily, by this point, there were hundreds of thousands of those infected devices online, a digital pandemic that reached nearly every country in the world.

Meanwhile, Peterson could only watch helplessly as Krebs' website was held offline by Mirai for more than 48 hours. Only then did Krebs finally manage to get it back up with the help of a new DDoS defender: Google. The web giant had recently expanded a pro bono DDoS protection service called Project Shield to a wider array of users, and it was eager to prove that it could withstand the internet's biggest attacks.

Within two hours of KrebsonSecurity coming back up, it received another blast from Mirai. The site's IP address had changed, Paras says, so his and Josiah's block list didn't prevent their Brazilian customer from relaunching his attack. But this time the site stayed online.
Google reached out to the FBI, and with Krebs' permission, the company eventually shared a list of IPs that had been the sources of the Mirai attack traffic. Peterson and his four-person team began to comb through it. Sure enough, he could see in the data that Mirai had infected devices across Alaska, along with practically every other state in the country. He started tracking down the Alaskan device owners, trying to explain to them in phone calls that their routers and security camera systems had been unwittingly turned into cannon fodder. Finally, Peterson got a break: He managed to persuade the owner of a hunting lodge in the town of Ketchikan to unplug its malware-infected security camera DVR and ship it to Anchorage to be dissected and used as evidence.

Peterson had found his Alaska victim. He launched an investigation to hunt for the hackers behind Mirai.

After serving in the Marines but before joining the FBI, Elliott Peterson had served as a “dean of men” at a college in Michigan. In that job, he had helped kids with emotional problems and substance abuse issues, essentially acting as a guidance counselor and mentor. It was an unusual role for a future federal agent, but the two jobs reflected Peterson’s strange hybrid personality: half by-the-book, buzz-cut g-man, and half well-meaning, friendly midwestern youth pastor.

Peterson brought that same peculiar cordiality into his Mirai manhunt. He began politely asking around among the Hack Forums crowd and their ilk, a scene he’d become familiar with over his years of tracking booter services: Who might know any of the pseudonymous hackers selling access to Mirai?

Not long after starting the investigation, his team in the Anchorage office got a lead on one good source. They’d managed to obtain a complete sample of the Mirai code from an infected device and found that it phoned home to a command-and-control server hosted by the DDoS mitigation firm BackConnect. Peterson knew that name. He’d been hunting the vDOS crew when BackConnect came under attack from Mirai’s rival; in an apparent act of self-defense, the company had used a BGP hijack to pull vDOS’s infrastructure offline—a rogue move that had nearly derailed Peterson’s vDOS investigation.

So he made a few calls to BackConnect’s management to ask about the company’s BGP hijack and the Mirai server they were hosting—which had since moved elsewhere—and whether they had any contact with whoever controlled it. BackConnect’s staff said they didn’t, but suggested someone who might: One of their acquaintances from a company called ProTraf Solutions, Paras Jha, seemed to have had contact with whoever was behind Mirai.

After all, Paras had received an extortion email from someone launching the Mirai attacks—neither Peterson norBack-Connect knew that Paras had sent that email himself—and they’d heard he’d chatted with a Mirai handler known as Ristorini.

So Peterson called ProTraf’s phone number and left a voicemail. Paras called him back. Peterson remembers that Paras matched his polite, friendly tone and calmly explained that yes, he had been in

touch with Ristorini in online chats. But he had no idea of the real identity of the person who'd tried extorting one of his former customers.

Paras kept the conversation short but said he'd be sure to keep asking around and would be in touch soon to help in any way he could when he'd learned more. Then he hung up and immediately called Dalton and Josiah to tell them the FBI was on their trail.

This time, their emergency meeting was steeped in panic: They needed to ditch Mirai, *now.*

Dalton suggested they simply take down Mirai's infrastructure, wipe the command-and-control and loader servers, and destroy the hard drive of every computer they'd ever used to manage it. "Lay as low as possible, kill the whole thing, shred our drives," as he put it. Then they could quietly move on to their more promising click fraud business.

Paras had another idea: How about they release the Mirai source code into the wild? If they posted it publicly on Hack Forums, it would be adopted by every DDoS-happy hacker in the world, just as Qbot had once been. They could disappear into that crowd, making it vastly harder for this nosy Alaskan FBI agent or anyone else to identify the original Mirai amid the flood of copycat attacks.

Dalton vehemently disagreed. He argued that releasing the source code would only draw more attention to Mirai, cause more damage, and make law enforcement all the more intent on finding the botnet's original creators.

The call devolved into a full-blown shouting match, the first the three friends had ever really had. Dalton screamed at Paras not to release the code. Paras remained unmoved. Josiah, meanwhile, listened impassively, stuck between his friends, unable to break the tie.
When they hung up, they had agreed that their Mirai adventure was over. But they remained split on what to do with its source code.

So Paras acted on his own. A couple of months earlier, he had created a new sock-puppet account on Hack Forums as another potential profile for Mirai's mastermind: He'd called this one Anna-Senpai, named after the villain of the Japanese animated show *Shimoneta,* or "Dirty Joke," in keeping with Mirai's anime-loving cover persona.

> **"We'll do it a few times," Josiah thought. "We'll cause trouble for a little bit, and then we'll just forget about it. We'll stop."**

Now, in late September, he logged in again as Anna-Senpai to post a stunning announcement. "I made my money, there's lots of eyes looking at IOT now, so it's time to GTFO," he wrote. "So today, I have an amazing release for you." The post then linked to download pages for Mirai's source code, along with a tutorial detailing how anyone could use it to create their own massive, self-spreading, internet-of-things attack tool. He added in a separate post that Anna-Senpai was now on the run, fleeing their home in France for a non-extradition country.

Paras had just dumped the recipe for a superweapon into a mosh pit. Beyond throwing up a smoke screen to ward off the FBI, it was also a final, epic troll: away to shake the internet ant farm, this time on a global scale, and watch the ants scramble.

The Hack Forums community responded accordingly, showering him with praise and admiring Mirai's polished programming. Several users wrote that it had to be the work of professionals, not the forum's typical teenage wannabes. "Your a fucking legend," one user wrote. "Leak of the year," wrote another.

Within days, one user responded that they'd successfully used the source code to create their own Mirai botnet of 30,000 devices. Another chimed in to say theirs had reached 86,000 machines. "The glorious copy paste will happen," wrote another appreciative hacker. "IoT botnets will spread like wildfire."

"Best haxoring tool of all time! Gonna take down eribody!" wrote another Hack Forums fan, summing up the gleeful mood. "I've always wanted a botnet that can DDoS de planet!"

Peterson was deeply dismayed to see the Mirai code dumped online, a move he saw as appallingly reckless. But rather than be thrown off, as Paras had intended, Peterson had the immediate thought: Had his poking around inspired this? Did his conversation with Paras have something to do with it?

Not long after Anna-Senpai's Mirai release, Peterson got another break in the case: Some university researchers working with the anti-DDoS group Big Pipes told him they'd found a clue in the logs of their honeypot machines, designed to monitor internet scanning. Two months earlier, on August 1, they'd been able to see that a kind of proto-Mirai scanning tool, perhaps the earliest version of the botnet's reconnaissance code, had probed their devices from a US-based IP address.

Peterson contacted the IP's hosting company to request the identity behind it and got a subscriber name: Josiah White. The other cofounder of ProTraf solutions.

The FBI agent called ProTraf again and this time spoke to Josiah on the phone, projecting his same friendly tone. Josiah, trying to sound professional but caught off guard by Peterson's discovery, nervously admitted that yes, he'd "done some scanning." Scanning the internet, after all, isn't a crime. Then he begged off answering any more questions and hung up the phone.

Peterson had been fascinated and even impressed by the Mirai team's operational security: the careful layering of proxies, the dead ends he reached as he traced those connections, the "doxes" he found for Mirai's handler accounts, all of which seemed to lead him astray. But now, just weeks into his investigation, he knew that Josiah's early scanning slipup had allowed him to sidestep all of that obfuscation and misdirection. His team began sending a flurry of legal requests to the email and internet service providers for every account associated with the throwaway profiles Paras had created for Mirai, as well as those of Paras and Josiah themselves and ProTraf Solutions.

As Peterson dug through Hack Forums, he noticed, too, that there was another interesting account that sometimes chimed in on Anna-Senpai's posts—someone called Fireswap. Often they seemed to be defending Mirai's creators and taking shots at critics of their source code. So Peterson sent a legal request to Hack Forums for Fireswap's email address—fireswap1337@gmail.com—and then asked Google for that user's subscriber metadata.

Looking through logins on Fireswap's Google account, registered to someone named Bob Jenkins, he could see they came from the same VPN or proxy server IP address that had carefully been used to create the fake Mirai doxes—sometimes just minutes apart. But then, in some cases, "Jenkins" had a different IP: the same one that Paras had used to connect to his ProTraf email account.

Paras had never suspected that an investigator would think to look into the burner account he'd created solely to cheerlead for himself on Hack Forums and take swipes at detractors. Now it had become the missing link tying him to Mirai.

Peterson still hadn't heard of Dalton Norman. But he now believed he'd found Mirai's two creators. The end of their cybercriminal careers was already in sight. But the chaos they'd invited onto the internet was just beginning.

Once it was fully unleashed and reproducing in the wild, Mirai didn't immediately break the internet. It took three weeks.

On the morning of October 21, 2016, Allison Nixon was just getting down to work in Flashpoint's office, an old garment factory on the desolate western edge of Midtown Manhattan, when a colleague pointed out to her that something was seriously wrong with the internet.

Specifically, its phone book was broken. The domain name system is the mechanism that translates human readable domain names into the IP addresses that actually route internet traffic to the computers where services are hosted. DNS is what allows you to remember "Google.com" instead of 2001:4860:4000:0:0:0:0:0, for instance, as the way to tell your browser to load up a search engine.

On that morning, the DNS of dozens of websites seemed to be crippled. Internet users across the US were typing names into browsers that needed to be translated into numbers, and the translators had been knocked out cold. "Something big is happening," Nixon remembers a colleague saying to her. "We need to figure out what's going on."

As Nixon's team tried sending DNS requests to some of the affected sites—the same sprawling collection of news sites, social media, streaming services, banking sites, and dozens of other major services that Scott Shapiro and millions of other users were trying in vain to reach—they saw that all the sites used the same New Hampshire–based DNS provider, a firm called Dyn. Although it wasn't yet clear to Nixon at the time, no fewer than 175,000 websites were offline.

Searching for a root cause for this unfolding internet collapse, she checked the attack logs generated by her "sad" DVRs—by now her team had several of them serving as bait. Sure enough, she could see that a Mirai variant, one of the many copycats that had sprouted in the weeks since Paras leaked the source code, had been relentlessly bombarding the Dyn DNS server for Sony's PlayStation gaming network. The attack's effects had apparently spilled over to take down Dyn's entire DNS system. Someone was using their copycat botnet to troll a video game company—typical Hack Forums behavior—and the collateral damage was the worst internet outage the world had ever seen.

The nihilistic, teen-angst-fueled, mega-DDoS that Nixon had always warned about had finally arrived. "We had worked for such a long time in preparation for that day that it was kind of vindicating," Nixon says. "On another level, it was super, *super* stressful."

Shortly after the attack on Dyn started, Nixon managed to reach someone at Dyn and share the evidence pointing to Mirai, a suspect Dyn only had an inkling of until that point. Dyn staffers, at that moment, were anxious but still confident that they could handle the problem and get their servers back online.

It was around the same time, still before 9 am eastern, that Dyn truly began to implode.

DNS records are designed to work like a kind of hierarchical phone tree. Major services like Google and Comcast have their own DNS servers ready to answer computers requesting the IP address of a domain, and they only periodically check in with an "authoritative" DNS provider—in this case, Dyn—to make sure the addresses they're handing out haven't changed. Some services check in multiple times a minute, while others refer to their last update of DNS data for hours before refreshing it.

Within minutes of the Mirai attack striking, Dyn was already in trouble, as DNS servers set to check in every 15, 30, or 60 seconds for new DNS records pounded the company's overwhelmed authoritative servers. When they didn't get an answer, they'd ask again—and again and again. They were designed to *expect* answers, after all: An authoritative DNS provider as large as Dyn had never gone down before.

But as time passed and Dyn's servers stayed down, the chorus of DNS requests began to include major services that check in only every hour. And then the ones that check in every two hours. And three. All now joining the mob incessantly hammering on Dyn's doors. Some internet services had even designed their DNS systems to automatically spin up new DNS servers to ask for answers when their existing ones didn't get a response, multiplying the barrage of queries.

"Once the cascading failure started, that's when everyone got very, very nervous," says one person who was working at Dyn on the day of the attack. "Before that, the graphs looked awkward, but they didn't look catastrophic. But then they tipped over an edge as major services couldn't get responses, and the numbers started shooting up to the right."

The Mirai attack, in other words, had set off a chain reaction. The internet's IP address directory system was DDoSing itself.

At the same time, Dyn began to experience a kind of parallel, human DDoS attack, as people began demanding answers in almost the same cascading structure. Angry corporate customers with comatose websites started bombarding Dyn's phone lines. When management couldn't answer their questions, they echoed them down the org chart to engineers who were already entirely overwhelmed. "When the ratio of management and client services people looking for answers versus the number of people who can provide any answers starts to explode," the Dyn staffer remembers, "that's when it really starts to feel like chaos."

Compounding the problem was a coincidence of almost comic timing: A team of Dyn staffers was, on that very day, waiting for Oracle to sign the paperwork to close a deal to acquire their company, reportedly for more than $600 million. No one wanted to be remembered as the middle manager who failed to keep the internet online on this momentous occasion—the first day that the new bosses were watching. And through all of this corporate panic ran an undercurrent of rumors that China or Russia was responsible, that they were up against an all-powerful state-sponsored hacking operation.

Those rumors were short-lived. So, by some measures, was the outage. By that afternoon, Dyn had managed to get the attack under control and had started sending DNS responses piecemeal to its clients, quieting the different networks clamoring for answers from its servers, one by one.

But the damage left in the wake of the Dyn outage lasted longer. The total economic cost of a major fraction of the global internet falling offline for half a day is difficult to measure. Sony, whose PlayStation Network was the attack's original target, reported an estimated net revenue loss of $2.7 million. Following the attack, there were projections that, for a time, Dyn lost roughly 8 percent of its contracted web domains—more than 14,000 total—and millions in future revenue.

Josiah was walking through a dark hallway, still trying to get a shirt over his head, when he found a flashlight—and a gun—pointing at his face.

As Paras, Dalton, and Josiah watched a botnet built with their code break the internet's backbone, they had an array of reactions. Paras remembers being shocked that it was so easy: The Mirai clone that had carried out the attack had hit Dyn with fewer than 100,000 devices, just a fraction of the size of their original botnet. Dalton felt a grim "I told you so" sense of confirmation that he'd been right about the hazards of releasing the source code, along with the stress of knowing it was sure to draw more heat—but he also noted, with a hint of pride, that whoever carried out this internet-shaking attack hadn't even updated their code. "There was no innovation at all," he says.

Josiah, who had already had the closest brush with the FBI among the three young men, was perhaps the most troubled. By then, his family had moved out of the Pennsylvania countryside into a three-story house in the nearby town of Washington. That's where, from the basement-level storage room he now used as his work area, he read about the Dyn disaster, silent with dread and amazement.

As for Elliott Peterson, he spent the day in the FBI's Anchorage office, fielding calls from every agency and official imaginable. Over the course of a month, his case had grown from a cybersecurity industry curiosity into an international clusterfuck, a subject of urgent interest for the Department of Homeland Security and for reporters asking questions in a White House press conference.

No one yet knew who had made the copycat Mirai that had attacked Dyn. But Peterson was confident he already knew who had created Mirai and handed the code to those attackers. It was time to pay Josiah and Paras a visit.

It was just before 6 am, long before the sun would rise on that mid-January morning, when Josiah heard the banging on his front door.

For two months, he had been waiting for the raid. He was now keeping a nocturnal schedule, working at his computer with Paras and Dalton until 3 or 4 in the morning before sleeping until 8 am and then heading into his father's computer repair shop. But that night, having finally gone to bed after 4 am, he still lay awake, his mind racing with anxiety.

As the banging started and his older brother hurried upstairs from their shared basement-level bedroom, Josiah went into the storage room and quickly switched off his computers. All three of the Mirai creators

had been careful to do their hacking on remote servers and to connect to them only from ephemeral virtual machines that ran on their own PCs. So he figured that switching the computers off would erase any lingering data in memory. Then, before turning off his phone, he sent a message to Paras using the encrypted messaging app Signal: “911.”

Josiah slipped on a pair of sweatpants and grabbed a T-shirt. He climbed the stairs and was walking through a dark hallway, still trying to get the shirt over his head, when he found a flashlight—or rather, he’d later learn, a gun with a flashlight attached to it—pointing at his face. “Drop the shirt,” he remembers an agent saying.

Josiah was herded onto his front porch, still shirtless, in the cold Western Pennsylvania winter air, where the rest of his family was already being held. Black Suburbans filled the street. And there was Elliott Peterson, on the porch, greeting Josiah in his weirdly gregarious tone. “Oh hi, Josiah. I was hoping we wouldn’t meet under these circumstances,” Josiah remembers him saying. “But here I am.”

After leaving Josiah’s flabbergasted family shivering in the cold for several long minutes, the agents brought them all back inside. As they searched the house, Josiah managed to get fully dressed and sat in the living room. But even once he’d warmed up, he still couldn’t stop shaking. As his secret life finally came crashing into his family life, he remembers feeling especially embarrassed that he’d left the storage room the FBI was searching so untidy.

Aside from Peterson, Josiah could see that local Pittsburgh FBI officials had joined the raid—as had French special intelligence officers. He’d later learn that French law enforcement had also raided the home of a certain innocent patsy in France with a server filled with anime.

After a couple hours of searching, the agents hauled away Josiah’s computers, hard drives, and phone, and Peterson asked Josiah and his parents to come into the dining room to talk. “You probably know why I’m here,” Peterson said. Josiah responded that he could guess.

The conversation lasted about half an hour. Peterson brought up the Mirai scanning server, and Josiah deflected again, confessing to nothing. The FBI agent warned Josiah not to tell anyone about the search—not knowing that Josiah had already sent his “911” warning to Paras. Then he left.

In the silence that followed, Josiah’s parents told him it was time to come clean. During an excruciating 30-minute car ride to their computer repair shop to start the workday, Josiah confessed everything. His parents listened, stone-faced, too scared for their son’s future to even be angry.

Finally, his father responded: They would have to entrust Josiah’s fate to God.

The raid on Paras' home came the next day. Peterson had hoped for simultaneous searches but decided he should be present at both, so he spent the hours after leaving Josiah's house driving more than 350 miles across Pennsylvania into New Jersey.

At 6 am, Paras heard the same banging on the front door of his family's house, where he was home from Rutgers for winter break. Thanks to Josiah's warning, this second raid had far less of an intimidating effect than the first: Paras had carefully cleaned up any evidence on his computers and turned them off long before the FBI agents arrived. In an attempt to find any storage devices Paras had hidden, the agents brought along an electronics-sniffing dog—trained to smell the glue used in computer hardware components. Paras remembers it wanted to play with his family's dog, a comical moment that helped dispel any shock and awe.

When Paras saw Peterson in person, his first response was annoyance that this chipper FBI agent had come all the way from Alaska to turn his home upside down. Peterson asked Paras whether Josiah had told him about his search of Josiah's house the previous day. Peterson assumed Josiah had stayed silent, as instructed, and he hoped to plant a sense of betrayal in Paras that his friend hadn't given him a heads-up.

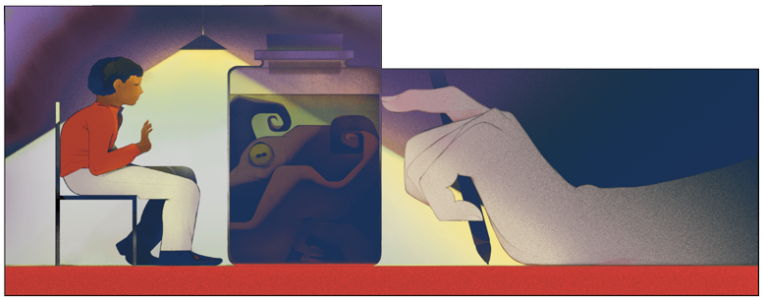
But Paras instead smiled and said that yes, Josiah had warned him, surprising Peterson. And like his friend the day before, Paras refused to confess to anything related to Mirai.

Paras' family was deeply shaken by the intrusion. But when the agents left, he assured his parents that it was all a misunderstanding, that he had no idea why this Alaskan FBI agent seemed so fixated on him. He hadn't done anything wrong.

Paras, Josiah, and Dalton discussed the raids, and they came to an extremely optimistic conclusion: that the feds didn't seem to have anything on them. The searches had been a scare tactic, they agreed, and they had failed.

On the same day the FBI searched Paras' home, Brian Krebs had published a bombshell article suggesting that Paras, potentially with Josiah's help, was the most likely identity behind Anna-Senpai. Krebs was working his own sources to piece together many of the same connections the FBI had drawn. But Paras had denied the accusation in a response to Krebs, and the three hackers, armed with the incredible hubris of youth, blew off the article as circumstantial evidence. After all, the FBI had already taken their shot and seemed to have gotten nothing that could prove their guilt.

As the months passed and they remained free, they made a brazen decision: They would continue their pivot into the click fraud scheme.



This new venture was turning out to be far more lucrative than Mirai, to a degree that even they had never imagined. To avoid ties to their overexposed botnet, they had begun building a new one, this time focused on devices primarily in the US, given that they could make the most money selling access to American computers to generate clicks on American ads. By the spring of 2017, they were quietly pulling in $50,000 a month in revenue, paid out in cryptocurrency by a business partner who seemed to be Eastern European.

Paras and Josiah mostly socked away the money, waiting for an opportunity to try to launder it through a legitimate business—though by then they'd finally given up and killed ProTraf. Dalton was less careful. He spent tens of thousands of dollars on splurges like a 70-inch flatscreen TV for his parents—he told them he'd made the money trading crypto—and upgrades to his home computer, a gaming desktop surrounded by transparent tubes of red coolant to prevent it from overheating as he supercharged its performance.

Even as the three hackers left Mirai behind, their code continued to plague the global internet. Mirai attacks hit the UK banks Lloyds Banking Group and Barclays, intermittently tearing Lloyds offline while Barclays repelled the onslaught. Another struck the primary mobile telecom provider for Liberia with about 500 gigabits a second of traffic, taking down much of the West African country's connectivity.

But Mirai, and its many malicious progeny, were no longer its creators' problem. The three young men had now, finally, hit their stride with a truly profitable and stealthy form of cybercrime. Dalton made a prediction to himself: "In a year, we'll either be rich," he thought, "or we'll be in jail."

Only months later did Josiah hear from Elliott Peterson again. The FBI agent asked him to come to Anchorage to talk. Prosecutors were suggesting a reverse proffer session, where they would lay out the evidence against him. By this point Josiah had a lawyer, who recommended that he take the meeting—and not tell his friends. This time he didn't.
In the summer of 2017, Josiah and his mother flew to Anchorage. The 10-hour flight was only the second time he'd ever been on a plane. On the morning of the meeting with prosecutors, he arrived at the Anchorage Department of Justice building in a suit, his mind nearly paralyzed with anxiety. Peterson was there, and he greeted Josiah and his mother, suggesting fun activities they should check out while they were in town, as if this were a family vacation.

The Alaskan assistant US attorney who had taken on the Mirai case, a young prosecutor named Adam Alexander with a background in charging violent crimes and child exploitation, launched into a PowerPoint presentation projected on a screen in the front of the conference room. He began by displaying the sentencing guidelines for violations of the Computer Fraud and Abuse Act, showing how the prison time scaled up based on the amount of damage caused.

For the millions of dollars in damage Josiah might be held responsible for, Alexander suggested, he was facing as much as six or seven years in prison for his first offense.

Alexander began to detail the evidence they had against him. First, they had his connection to the early Mirai scanning server. Then it went further: On occasion, it turned out, Josiah had let his guard down in small but revealing ways, checking on the IP address of another Mirai server directly from his home computer rather than using a remote virtual machine that would leave no trace on his PC.

And then there were text messages he and Paras had exchanged during his pre-Mirai DDoS takedowns of Rutgers' network.

"Were you still smashing?" Josiah had written to Paras at one point.

"No. Phone is insecure," Paras had wisely responded. But then, minutes later, he had asked for Josiah's help in launching another attack: the barely coded "Admiral can you execute my command?" message.

After more than an hour, they took a break. Josiah's lawyer told him and his mother that he strongly advised they seek a plea deal and that Josiah cooperate with the FBI—that he "shouldn't push his luck." Josiah, terrified by the looming threat of years in prison that had been slowly materializing since his first call with Peterson, immediately agreed.

When they reconvened in a different, much smaller conference room, Josiah told Peterson and Alexander he was ready to negotiate a deal. They responded that he'd first need to tell them the full, true story of his crimes. To their relief, he began to detail the entire Mirai conspiracy. The FBI agent and prosecutor were intrigued to learn more about the key role played by Dalton, who hadn't until then been a target of their investigation. And they were amazed to hear that the Mirai crew was now, even after their raids, engaged in an entirely new click fraud botnet scheme. They had known nothing about it.

> **When the feds finally arrived before dawn, Dalton was relieved. They found him in his boxer shorts, wrapped in a pink blanket on a beanbag, watching *Star Wars*.**

Peterson and Alexander told Josiah that if he wanted any chance of a plea deal—still without any promise of avoiding prison—he'd have to fully cooperate. That meant helping to collect evidence on his friends.

Josiah, now in survival mode, was ready to do what it took to stay out of prison. By the time he flew back to Pennsylvania, he was a federal informant.

Dalton and Paras could tell Josiah was acting strangely. He'd never been aloof or a step behind on any technical questions before. Now, on their group calls, he was quieter and would inexplicably ask them to break down how their criminal enterprise worked in unusual detail.

They had their suspicions and did their best to discuss their conspiracy using only convoluted code words and hypotheticals. But they couldn't bring themselves to violate the unspoken terms of their friendship by confronting Josiah or cutting him out of their deal. "We both knew something was up," Dalton says. "But we didn't have any proof. I didn't want to fuck him over just because I was sketched out." After all, this was their old friend, the legendary LiteSpeed, the one to whom they owed so much for advancing their careers as botnet masters.

As for Josiah, he says his years of working in his family's computer repair shop had helped prepare him for his new role as a double agent. "When you work in retail, you're used to putting on a face," he says, "talking to people how they want to be talked to."

A few weeks later, Paras got his own call from Peterson, with his own offer of a meeting in Anchorage. Paras told Dalton about the invitation—but not Josiah, whom he'd begun to distrust. They agreed that it made sense for Paras to meet with this FBI agent and see exactly what the feds had on them.

Over the six months since the raid of his home, Paras had remained in denial, putting on a defiant face but quietly living in a state of latent terror. His family had never again discussed the traumatic violation of their home by federal agents, instead pretending it had never happened. They were "going through the motions of being a family," as Paras puts it, "but there's this cloud hanging over everyone's head."

The cloud of silence remained in place as Paras and his father flew to Anchorage. Along with Paras' lawyer, they met with Peterson and Alexander in the same Department of Justice conference room and got the same cheery hiking tips from Peterson. Paras tried to maintain an implacable expression as the prosecutor threw one damning piece of evidence after another onto the screen, laying out his crimes in front of his father. They showed Paras' connections to the Mirai handles and to Anna-Senpai, and his Fireswap burner account.

Still, Paras told himself that the case was far from clear-cut. Then Alexander played for the room a series of audio recordings of the three hackers explicitly discussing their new click fraud venture. One conversation, from a night when Paras and Dalton had been drinking and let down their guard, was particularly incriminating. For Paras, it was the first confirmation of Josiah's betrayal.

Just as with Josiah, the meeting paused for a break after an hour. Paras, his father, and his lawyer walked across the street from the prosecutor's office into a small park of paper birch trees in front of the Anchorage Museum. It was a dismally cold, cloudy day, though Paras says his anxiety had reached a degree where he was disassociating, barely aware of his surroundings.

Paras' lawyer leveled with him: It sounded very much like he was guilty of the crimes that he had, until then, denied even to his own attorney. Standing there in the park, Paras finally broke. Huddling with his father and lawyer, he confessed, tears flowing as he unlocked the shame, guilt, and fear that he'd kept bottled for months.

He asked his father to cut ties with him, begged him to let him face whatever punishment he had brought on himself alone. His father responded in a voice as broken as Paras' own: He could never do that.

Instead, he and the lawyer both told Paras that there was no other way out now. His only chance to save himself was to do whatever the FBI and the prosecutors asked of him.

Unbeknownst to them, Peterson and Alexander had watched the three men speaking from the window across the street. From Paras' body language, they could tell they'd made a breakthrough.

When Paras came back inside, he was a different person, his defenses down. "You're in a hole, Paras," Peterson told him. "It's time to stop digging." He was ready to cooperate.

Alexander asked him whether he had told anyone that he was coming to Alaska, and he admitted that he'd told Dalton. So Alexander and Peterson asked Paras to call Dalton now, on the spot, on speakerphone, and tell him that he had nothing to worry about.

Paras did as he was told. Dalton picked up the call. And as the FBI and prosecutors sat around the table intently listening, Paras assured Dalton that it was just as they'd thought: The feds had nothing on them.

When it was Dalton's turn to be raided, Peterson practically scheduled it with him. a few weeks before the bang on the door, Yahoo had mistakenly sent Dalton a letter stating that his old email address had been the subject of a legal request. For more information, it read, he should contact FBI special agent Elliott Peterson.

So Dalton preemptively called the FBI agent who'd now been stalking them for nearly a year. Josiah and Paras, playing their roles as supportive friends, listened in. Peterson picked up the phone, said hello, and immediately apologized. "I wasn't planning on us talking for a couple weeks," he explained.

When Dalton claimed not to know who Peterson was or why his emails were being read, the FBI agent laughed out loud. "We're going to have a great opportunity to have a chat," he said in the most aggressive version of his usual genial tone. He ended the call by confirming with Dalton that he was still living at home, despite having now started college, implying he didn't want to search Dalton's parents' house if he had moved into a dormitory. "We try to be minimally invasive."

Dalton hung up with Peterson. "What the fuck was that?" he said to Josiah and Paras, who were still on the group call.

"Your ass," Paras responded.

For the next three weeks, Dalton was stricken with nausea-inducing anxiety and a sense of "impending doom." When the feds finally arrived before dawn, he says, he was actually relieved. They found him in his boxer shorts, wrapped in a pink blanket on a beanbag, watching *Star Wars.*

During the search, Dalton says, his anxiety evaporated—thanks to his early swatting experience, it wasn't his first time having law enforcement point a gun at him—and he did his best to show the feds that he wasn't impressed. He napped on a couch during the FBI's search. When Peterson tried to interview him, he gave him nothing.

In fact, with plenty of time to prepare before they arrived, Dalton had physically destroyed all his most sensitive hard drives. The agents found his beloved water-cooled PC torn apart, its red coolant spilled across his bedroom floor like blood. He'd carefully cached another drive that stored all the bitcoins earned from their click fraud scheme inside a cat food container, fully hidden by kibble. Since the container was transparent, the searching agents didn't think to look inside.

Just as with Paras and Josiah, Peterson told Dalton not to tell anyone about the search. But Dalton, loyal to the end, tried to send a coded message to Paras that he'd been raided, too: He repeatedly toggled the status of his account on the Steam video game network on and off in Morse code, spelling "FBI."

Paras saw Dalton's account blinking. But he never got the message. Of course, even if he had, he'd already been working with the FBI for months to collect evidence on his friend.

Dalton soon took his own trip to Anchorage, where he and his parents sat through Peterson and Alexander's third and final Mirai reverse proffer presentation. Through an hour of damning chat logs and audio recordings, Dalton showed no emotion. But when it was over, he knew there was no use resisting. They had everything.

When Dalton reluctantly agreed to cooperate, Peterson didn't ask him to keep their arrangement secret from Josiah and Paras. This time, he phoned the other two. All four of them joined the call.

After months of paranoia, Peterson wanted to clear the air, to tell them that they were no longer cooperating against one another. They would now all be working together. Josiah remembers it almost like a reunion: meeting each other again now that they were all on the other side.

In the call, Josiah and Paras seemed relieved to finally be able to speak honestly to each other and Dalton after months of subterfuge. Dalton agreed, in a defeated tone, that yes, he was on board. They would give up all their hacking tools and dismantle the click fraud botnet, and Dalton would forfeit the hidden hard drive full of their bitcoins. But Peterson remembers that Dalton remained quiet and formal, seemingly still processing his anger and shame at having been cornered by the FBI and surveilled by his friends.

It was only late one night, a few days after Dalton got home to New Orleans, that he allowed the full reality of his situation to catch up with him. He was facing a felony conviction. He was going to have to work as a federal informant. And he was still likely to end up in prison. It felt hopeless.

The person he chose to call to talk this over with, strangely, wasn't Josiah or Paras, but Peterson. He was trapped, he told the FBI agent in tears. His life was over.

For the next hour, Peterson, sitting in his living room in Anchorage, found himself back in his "dean of men" role, comforting and counseling the young cybercriminal who'd so recently been the target of his investigation.

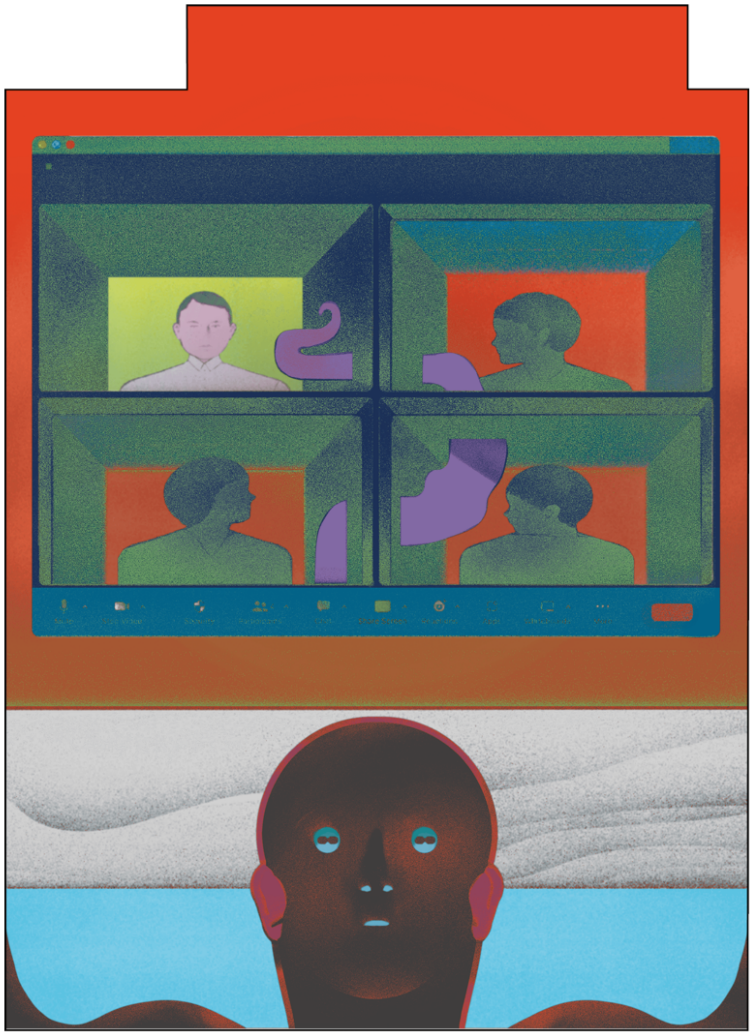
Peterson asked Dalton about his hopes for the future—the "where do you see yourself in five years" question of every guidance counselor. Dalton confessed that beneath his old, secret belief that cybercrime could be his only path in life, he still hoped that someday he might be able to have a normal, successful job in technology. Peterson told him that was still possible.

"He was super nice," Dalton says. "Far nicer than he ever needed to be."

Peterson said he couldn't promise Dalton that it would all be OK. There was still the possibility of spending years in prison. Regardless, Peterson reassured Dalton, he could still go to college. He could still do something rewarding with his talents. His life was not over.

The young men's lawyers had each warned them that, to have any hope of avoiding prison, they would need to go above and beyond in their cooperation with the FBI and prosecutors. So once they found themselves on the same team again, Josiah, Dalton, and Paras threw themselves into working with law enforcement with the same obsessive energy that they'd once put into conquering the internet of things.

All three were still deeply embedded in the cybercriminal community—in fact, Mirai had turned the personae that Paras had created into celebrities. So to start, they began helping the FBI target their old associates. It was Paras, the Mirai creator who had opened Pandora's box by publishing the botnet's source code, who found himself most actively working undercover to take down Mirai's copycats.



Because he still controlled the Anna-Senpai handle, Paras was tasked with reaching out to the creator of one especially prolific Mirai knockoff. The copycat botnet was controlled by a hacker who lived near Portland, Oregon. He'd been brash enough to reveal his location to Anna-Senpai in their chats, and even to invite Mirai's creator to hang out if he were ever in town. Paras took him up on the offer.
At that point, Peterson and Alexander had been tracking the suspect and believed they knew his identity. But he appeared to have no fixed address—he seemed to have developed a serious drug problem and had admitted to using meth in his chats with Anna-Senpai—and instead roamed around the city from house to house with little more than a backpack and the laptop he used to manage his botnet.

After Paras flew to Portland, he suggested to the target of their sting that they meet at his hotel. Sure enough, the hacker turned up, and the two botnet admins spent a few hours in Paras' room there, swapping stories and hacking tricks, and even inviting other hacker associates to join the conversation via Skype. Meanwhile, Peterson and other FBI agents recorded the meeting—with eavesdropping techniques they declined to describe—from another room across the hallway.

Eventually the young Portland hacker suggested they head to a nearby Little Caesars to eat. When he and Paras walked out of the room, he carelessly left his laptop open and didn't even bother to close the video chat session with his hacker friends. Those friends were still watching through the laptop's webcam when Peterson and another agent came into the room and seized the computer as evidence. Less than an hour later, the agents stepped out of a black van in the hotel parking lot and arrested their target as he and Paras returned from their lunch.

After that Portland sting, some of the hackers who had just watched the accidental livestream of the hotel raid accused Paras of acting as the FBI's snitch. But Paras pointed out that it hadn't been his idea to meet up—or even to conveniently go out for pizza—arguing that maybe *he* was in fact the one who had been set up.

The explanation was convincing enough that Paras managed to pull off subsequent undercover operations against multiple other cybercriminal suspects across the country. He says he hardly relished his role in those stings. But nor did he feel much guilt. "I mean, honestly, it was exhilarating," he says. "It felt like something out of a movie."

The FBI and the Justice Department declined to share all of the details of the investigations that Paras and the other two Mirai creators helped them pursue. But Peterson summarizes them: "We arrested people, and we worked other cases against IoT botnets, and we shut down other botnets where arrests weren't feasible," he says. "We just did really interesting work."

After a few months, when they had run out of undercover cases, Peterson began to give the team different kinds of tasks, many of them with no direct relationship to Mirai or their old contacts. They were grateful to find they were no longer acting as informants, so much as Peterson's new group of technical analysts.

They started helping the FBI agent with jobs like reverse engineering malware and analyzing logs to identify botnet victims. They built a software tool that parsed the blockchain to trace cybercriminal cryptocurrency. In early 2018, when hackers began to exploit server software known as Memcached to amplify their DDoS attacks, the Mirai team figured out how to scan for vulnerable servers that enabled those attacks so that the FBI could warn the servers' owners and help remove a new kind of DDoS ammunition from the internet.

Josiah says that, in this new role, he couldn't help but apply the same technical perfectionism he had always prided himself on. "I enjoy being the best at this sort of stuff," he says. "I thought, 'If we're going to work on this, it damn well better work right.' "

Paras says that, at first, he had immersed himself in Peterson's assignments—even the harrowing undercover ones—mostly on his lawyer's advice and as a distraction from his lingering guilt and shame."To prevent myself from feeling things," as Paras puts it. But over time, he found that he was able to look at

the work more squarely—and to even get some gratification from the good he felt he was now doing. Peterson's comment to him in Alaska, that he should stop digging the hole he was in, had stuck. The work for Peterson felt like "the opposite of digging," as he puts it. "I wanted to put as much distance as possible between who I am now and who I was then," he says.

Eventually, when the Mirai crew talked among themselves about their motivation to work with Peterson, Paras says, it went beyond self-interested survival to a sense of actual atonement for the harm they'd done. "It was like, OK, what is our path to redemption?" he says. "Maybe this is the start."

The FBI, of course, has a long, unsavory record of exploiting informants and cooperating defendants—many of whom are put in dangerous situations, made to entrap innocent associates, or end up feeling abandoned or used by their handlers. The three Mirai hackers felt they were an exception.

As the months passed, they say, they came to see Peterson as a kind of mentor. He seemed to show real concern for their futures. The strange friendliness he'd displayed while hunting them, they felt, was not an aggressive front but an actual expression of his humanity. "We were very lucky that we got Elliott," says Dalton. "He literally saved my life."

The US criminal justice system has a history of notoriously harsh sentences for hackers. In 2010, Albert Gonzalez was sentenced to 20 years in prison for stealing tens of millions of debit and credit card numbers from retailer networks when he was in his mid-twenties. In 2017, Russian cybercriminal Roman Seleznev, arrested on vacation at the Maldives airport, was sentenced to 27 years for his own massive theft of credit card data. Even Hector Monsegur, a front man for the rampaging hacktivist group LulzSec who flipped on his friends and served as a federal informant for more than two years, was jailed for seven months—longer than some other members of LulzSec in the United Kingdom he had informed on.

So it was almost a radical act when the prosecutors in the case of Mirai, the botnet behind several of the biggest cyberattacks in history, asked the judge to sentence its creators to a total of zero days in prison. Adam Alexander, the Alaskan assistant US attorney who had flipped each of the three hackers with PowerPoint presentations full of evidence against them, explains that his decision was based in part on the fact that none of them had prior criminal history or substance abuse problems that might have led them to fall back into old habits. Unlike many defendants, they had strong family support networks holding them accountable. Most importantly, by the time their sentencing was approaching in the fall of 2018, they had done more than a thousand hours of work for Peterson, what Alexander described in a letter to the judge as "extensive and exceptional" cooperation. "They were kind of gleefully willing to break the internet," Alexander says. "But would putting any of the three of these young men in prison for 18 to 36 months, and then wiping our hands of them, have more meaningfully assured that we could prevent future criminal conduct? I didn't actually think so then, and I still don't think so today."

Instead, he asked the court to sentence Josiah, Dalton, and Paras to 2,500 hours of community service each over the following five years. They would carry out that work with the same FBI agent who had supervised their presentence cooperation period: Elliott Peterson.

In an Anchorage courtroom roughly two years after Mirai had obliterated Brian Krebs' website, a judge handed down that sentence—community service, no prison time—to the three 21-and 22-year-olds, along with debts of between $115,000 and $127,000 each in restitution. "You're young, you have a lot to give to society … and you have a lot of talent and skill," a judge told the three men in his Anchorage courtroom that fall day. "I hope you use it for good." (Paras would face separate charges in New Jersey

for his attacks on Rutgers, where prosecutors vehemently argued that he deserved prison time. Alexander intervened, countering that Paras' cooperation with prosecutors and the FBI in Alaska should be factored into his sentencing in that case, too. The New Jersey judge ultimately agreed, sentencing Paras to nearly $9 million more in restitution and six months of confinement at his parents' home, but no jail time.)

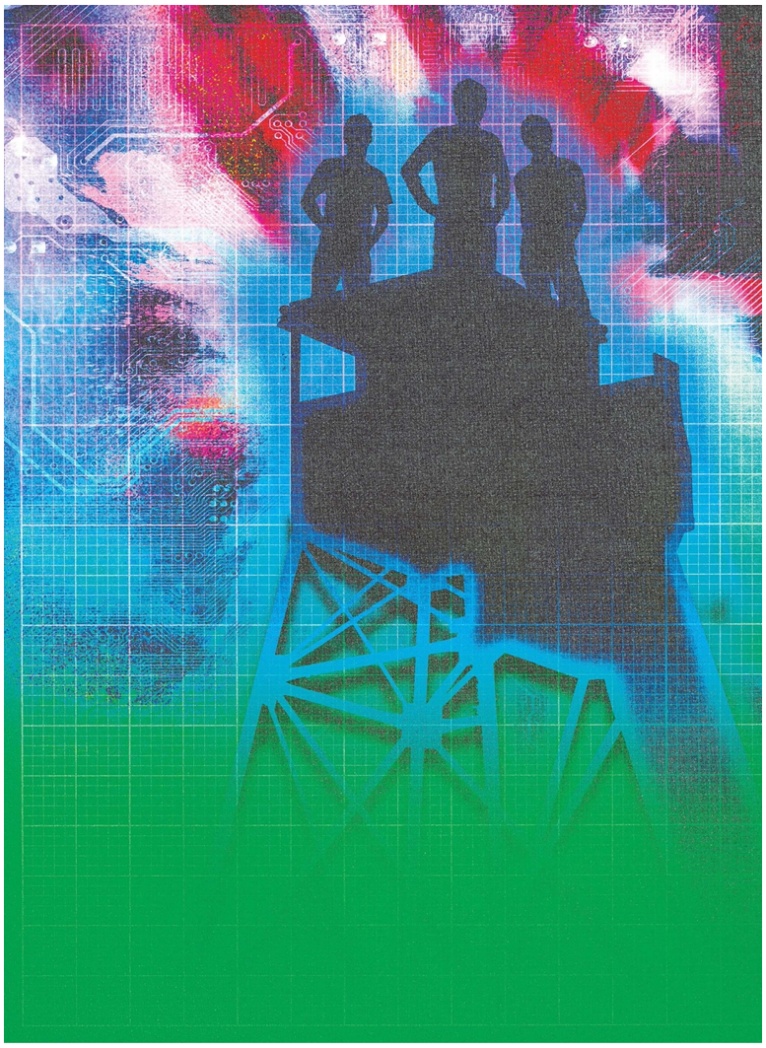
On this visit to Alaska, when Peterson again suggested local activities, the Mirai crew actually took him up on it. That evening they ate together at a local indie theater restaurant, the Bear Tooth Grill, where they also caught a screening of a documentary about Google's Go-playing AI—just some notorious hackers and the FBI agent who hunted them down, out for dinner and a movie.

Not long into their five-year community service stint, Peterson says he began to sense that his three unlikely protégés were beginning to outgrow him—that he couldn't find enough technical tasks worthy of their talents. So he asked the Big Pipes anti-DDoS group he'd helped create with Allison Nixon if anyone there had work for them to do. Nixon raised her hand.

When Peterson had first started overseeing "the kids"—as they came to be known within Big Pipes—Nixon had wanted nothing to do with them. She'd spent long enough lurking in the Hack Forums cesspool to be familiar with the toxicity that flowed freely there and had even been personally harassed by some of the Mirai team's old associates. "They're not nice people," she says of that scene. "You don't want them to know your name."
But after seeing that Peterson had worked with Paras, Josiah, and Dalton for more than a year and was still willing to vouch for them, she decided to take a chance and met them on a video call. She found the three young hackers—including the notorious Josiah "LiteSpeed" White, whom she'd tracked for nearly his entire career—polite and eager to please.

She did, in fact, need their programming help: She had an idea for a new kind of honeypot that would be far more versatile than her "sad DVR." She wanted to create a system where security researchers or analysts could load up any internet-of-thing device's firmware in a virtual environment to catch new malware variants.

The tool they built together was called Watchtower. It used a newer technology called QEMU containerization to spin up quarantined, full-fledged simulations of DVRs, waiting to be infected. The Mirai team had designed their internet-of-things malware to detect when it loaded on a software simulation of a gadget rather than the real thing and to kill its processes rather than give a researcher any information. But WatchTower's honeypot was designed to look like a real device in every way that malware could check—a seamless, virtual panopticon in which to observe malware and intercept its master's commands.



“It was brilliantly done,” says Larry Cashdollar, a security researcher at Akamai who says the company used Watchtower to obtain and analyze countless new samples of IoT malware. Eventually Nixon and her Mirai team added in data contributed from other researchers and members of her Big Pipes DDoS working group, including machines that acted as honeypots for reflection attacks and DNS data to identify targeted domains, integrating it all into a real-time DDoS analysis dashboard. By 2020, they had added a list of domain keywords to identify attacks on political or voting system targets, and the tool’s results were used to monitor for DDoS attacks throughout that year’s election—helping them prepare for any democracy-disrupting “big one” that many in the security community still feared.

As for Brian Krebs, when he found out that the three Mirai creators had escaped jail time and were now essentially working as whitehat security researchers, he was initially perturbed by what he saw as a lack of accountability.

“Trust the process,” he remembers Nixon telling him. “What process?” Krebs says he responded. “This doesn’t look like justice to me.”

But as time passed and he continued to learn from Nixon and others about the good work Paras, Josiah, and Dalton were doing, he says he slowly changed his mind. “When I was able to hear about some of the things they came up with, it was encouraging,” he says. “I guess that it’s the best of all possible outcomes.”

When Nixon moved from Flashpoint to a job at a new security firm, Unit 221B, she lobbied the company to hire her Watchtower team. By that time, Paras had gotten a job writing code for a semiconductor company. But Josiah and Dalton both began working for Nixon full time as security researchers on contract, on top of their community service work.

Of course, even as the Mirai crew joined the legitimate security industry, many of the new botnets that they were now monitoring with Watchtower were, in fact, variants of their own monstrous creation. Like Josiah’s Qbot code before it, Mirai had become the best, cleanest code base for anyone trying to build their own massive collection of hacked machines, and all manner of digital miscreants proceeded to pick it apart, repurposing its components to wreak havoc. “There are pieces of Mirai everywhere now,” says Chad Seaman, a security researcher at Akamai and an early member of the Big Pipes working group.

Companies still face near-constant attacks from Mirai descendants, Seaman says. Because those botnets are generally still fighting over the same vast but splintered collection of vulnerable internet-of-things devices, none of them is nearly as big as the original Mirai. Nor has any of Mirai’s progeny ever again managed to surprise defenders to the degree Mirai did.

But their attacks still plague the internet, adding to the millions of dollars a year that companies pay in DDoS protection. “The arsonists have turned over a new leaf,” Akamai’s Seaman summarizes. “The wildfires continue to rage.”

EPILOGUE

In the years after he sat in his Connecticut home and watched his digital life implode, Scott Shapiro became a kind of Mirai fanatic. The Yale Law professor eventually read the source code that Paras published on Hack Forums, printing it out, poring over its mechanics, and marveling at its well-polished design. Years later, he would write a case study of Mirai in his book *Fancy Bear Goes Phishing,* which tells a history of the internet through a series of extraordinary hacking events.

Among other things, Shapiro now sees the Mirai case as a rare model of actual restorative justice in cybercriminal law. It shows, he argues, a positive alternative to putting young hackers in prison when, in many cases, their online behavior contrasts so sharply with their real-world selves. Yes, the internet can seduce good people into doing bad things. But perhaps the split personalities it creates also leaves more room for redemption in the offline world. Perhaps it even means more cybercriminals like the Mirai crew can be reformed and put to work fixing the problems they caused. “This was an experiment. It worked out really well,” Shapiro says. “I would like to see more of it.”

One afternoon in early December of 2021, three years into the Mirai creators’ five years of probation, Shapiro invited Josiah, Paras, Dalton, and Elliott Peterson to speak to his Yale cybersecurity law class over Zoom. It would be the first time the four of them had appeared together in a semipublic setting other than a courtroom.

At first, Peterson did most of the talking, telling the story of the case and his investigation in a 45-minute presentation. Then he finished and the group took questions from the students.

One asked how this group of young adults with no criminal records had justified to themselves carrying out such epic acts of digital disruption. Paras answered for all of them, explaining how incremental it had all felt, how easy it had been to graduate from commandeering hundreds of hacked computers to thousands to hundreds of thousands, with no one to tell them where to draw the line. “There was never a leap,” he says. “Just one step after another.”

> **They had simply never faced an obstacle to their hacking careers that they hadn’t been able to surmount. They had come to feel almost invincible.**

Another student asked how they had kept going for so long—how they believed they could evade the FBI even after they had been raided. This time it was Dalton who answered, overcoming his anxiety at speaking in front of crowds, in part thanks to better treatments that have helped to alleviate his stutter. He explained to the class that they had simply never faced an obstacle to their hacking careers that they hadn’t been able to surmount—that, like teenagers who have no experience of aging or death and therefore believe they’ll live forever, they had come to feel almost invincible.

Throughout the presentation, Shapiro says, he was struck by the youthful nervousness of the three Mirai creators and the fact that, even as they spoke, they never turned on their webcams. The hacker threat that he’d once been sure must be the Russians, that had felt so large and powerful, was just these “young boys,” he realized. “Young boys who don’t want to show their faces.”

Paras would later explain to me that he wasn’t exactly trying to hide. He just doesn’t want to associate his face with Mirai anymore. He’s since lost more than 30 pounds, ditched his glasses, grown a trim beard; he’d prefer to let his old image, the pudgy bespectacled kid pictured in Brian Krebs’ story about Anna-Senpai, be the one tied to Mirai.

As of the end of October, all three of the Mirai hackers’ periods of probation have ended. Paras Jha and Josiah White work together for a high-frequency financial trading company. Dalton Norman still holds his job working for Allison Nixon at Unit 221B. But they all plan to continue maintaining and updating Watchtower, perhaps their most lasting contribution to undoing some of the damage they’ve done.

“I’m grateful for the chance to try to put the genie back in the bottle,” Josiah says.

He also admits that’s probably impossible. Even now, he and Dalton and Paras know that fragments of the monster they built still haunt the internet. Mirai no longer comes from the future. Instead, it stubbornly hangs on from the past. Someday, they hope to leave it there.

ANDY GREENBERG *is a* WIRED *senior writer. He is the author, most recently, of* Tracers in the Dark: The Global Hunt for the Crime Lords of Cryptocurrency.

SOURCE IMAGES: GETTY IMAGES; ILLUSTRATIONS BY JOONHO BRIAN KO; CHRISTOPH DERNBACH/GETTY IMAGES; FBI; ALLISON NIXON; DANIEL ROSENBAUM/REDUX; GUY JORDAN/LONDON SCHOOL OF ECONOMICS