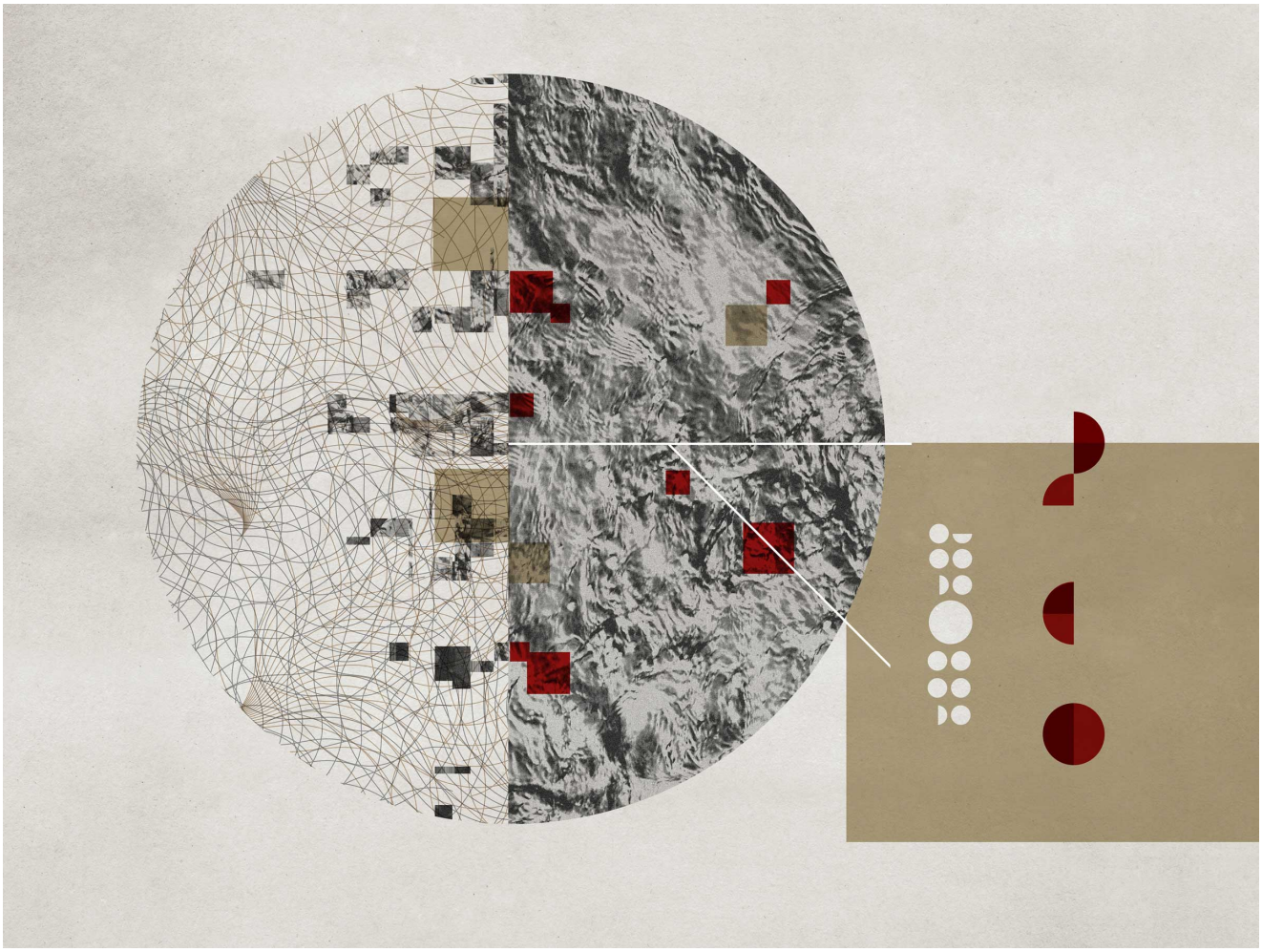
Inside the Hunt for Russia's Most Notorious Hacker

wired.com/2017/03/russian-hacker-spy-botnet/

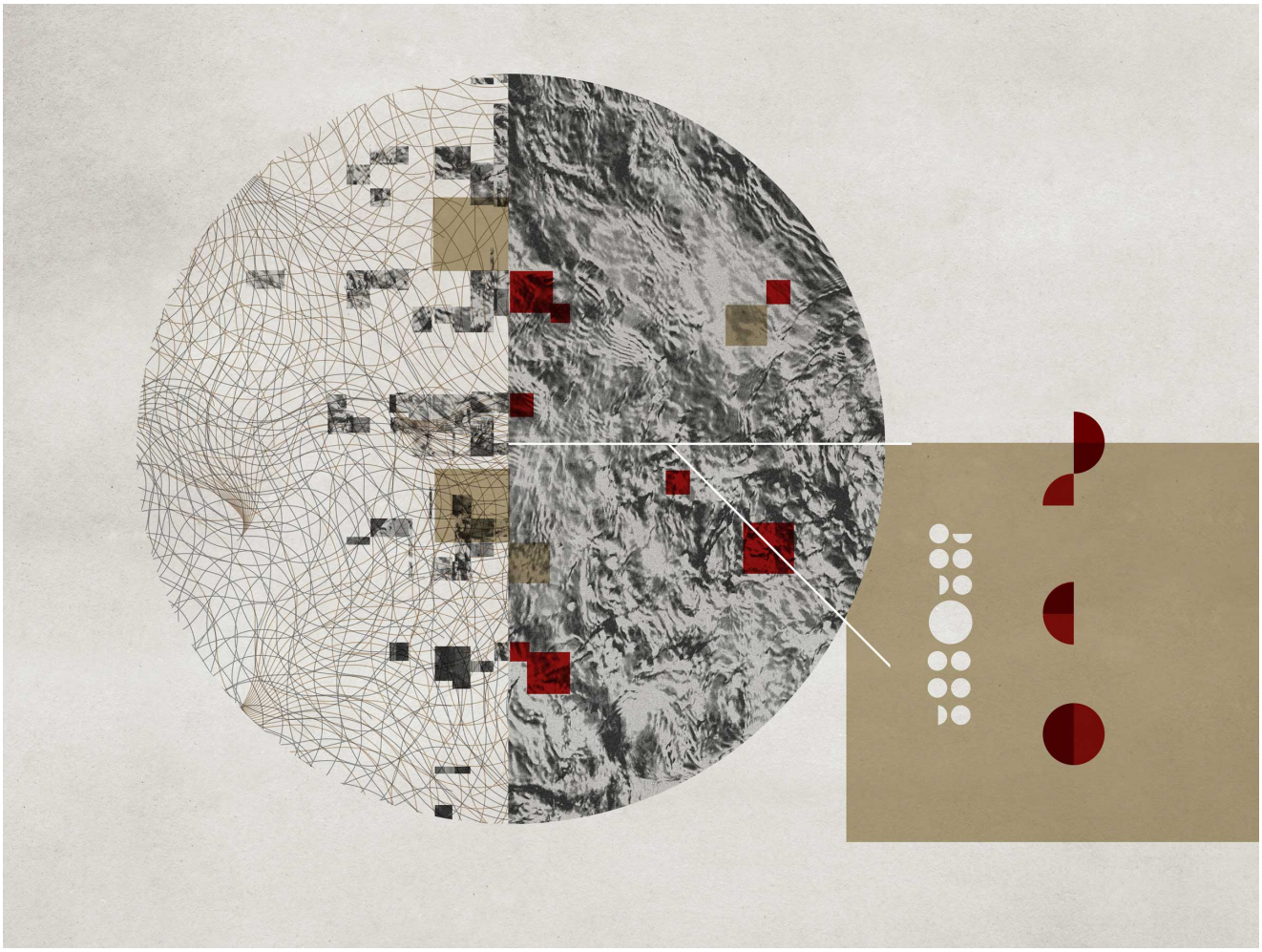
Garrett M. Graff March 21, 2017

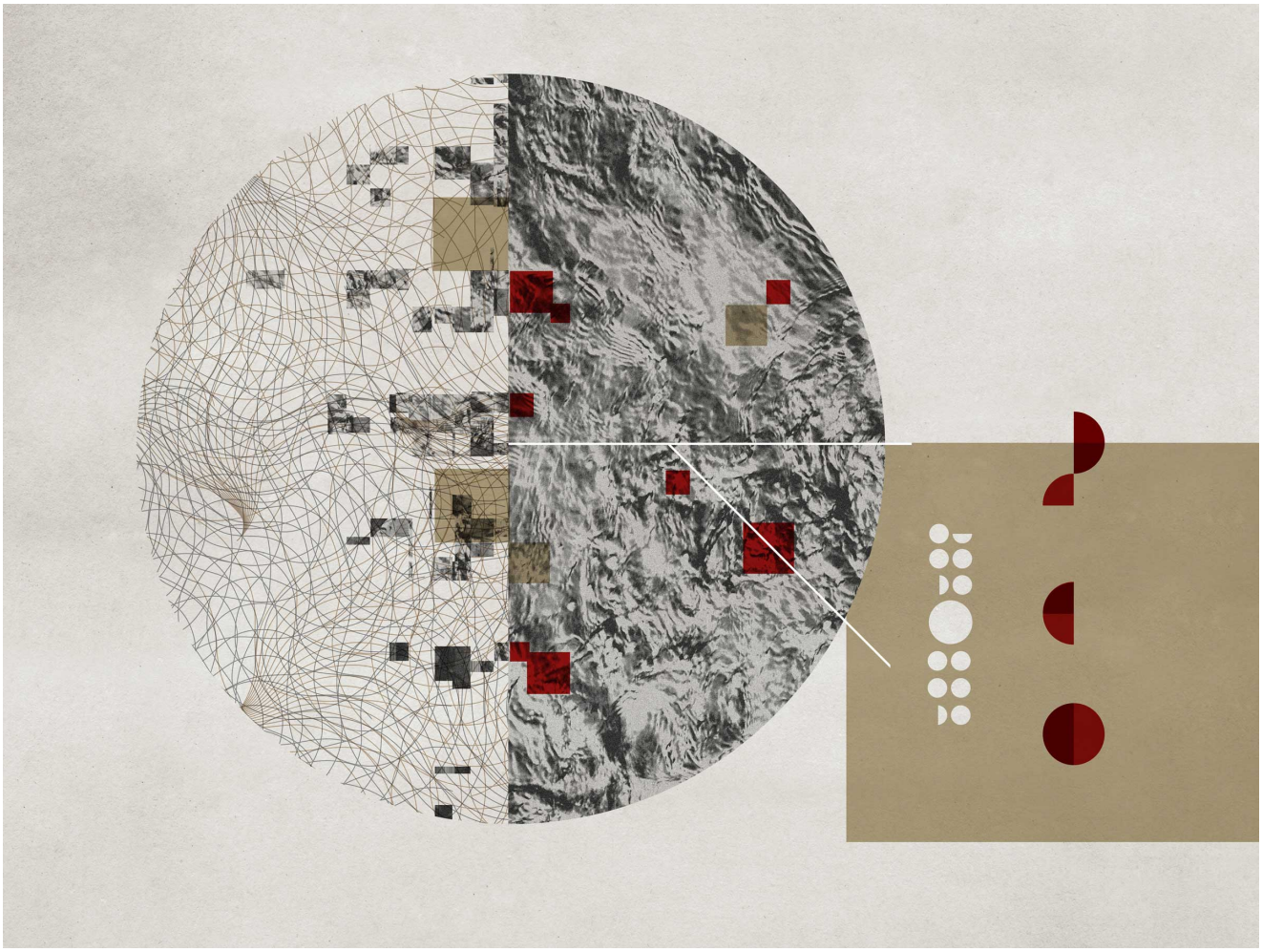


CHASING

THE

PHANTOM





Inside the Hunt

for Russia’s Most

Notorious Hacker

Inside the Hunt for Russia’s Most Notorious Hacker

by Garrett M. Graff | illustrations by Chad Hagen3.21.17

On the morning of December 30, the day after Barack Obama imposed sanctions on Russia for interfering in the 2016 US election, Tillmann Werner was sitting down to breakfast in Bonn, Germany. He spread some jam on a slice of rye bread, poured himself a cup of coffee, and settled in to check Twitter at his dining room table.

The news about the sanctions had broken overnight, so Werner, a researcher with the cybersecurity firm CrowdStrike, was still catching up on details. Following a link to an official statement, Werner saw that the White House had targeted a short parade’s worth of Russian names and institutions—two intelligence agencies, four senior intelligence officials, 35

diplomats, three tech companies, two hackers. Most of the details were a blur. Then Werner stopped scrolling. His eyes locked on one name buried among the targets: Evgeniy Mikhailovich Bogachev.

Werner, as it happened, knew quite a bit about Evgeniy Bogachev. He knew in precise, technical detail how Bogachev had managed to loot and terrorize the world's financial systems with impunity for years. He knew what it was like to do battle with him.

But Werner had no idea what role Bogachev might have played in the US election hack. Bogachev wasn't like the other targets—he was a bank robber. Maybe the most prolific bank robber in the world.
"What on earth is he doing on this list?" Werner wondered.

1

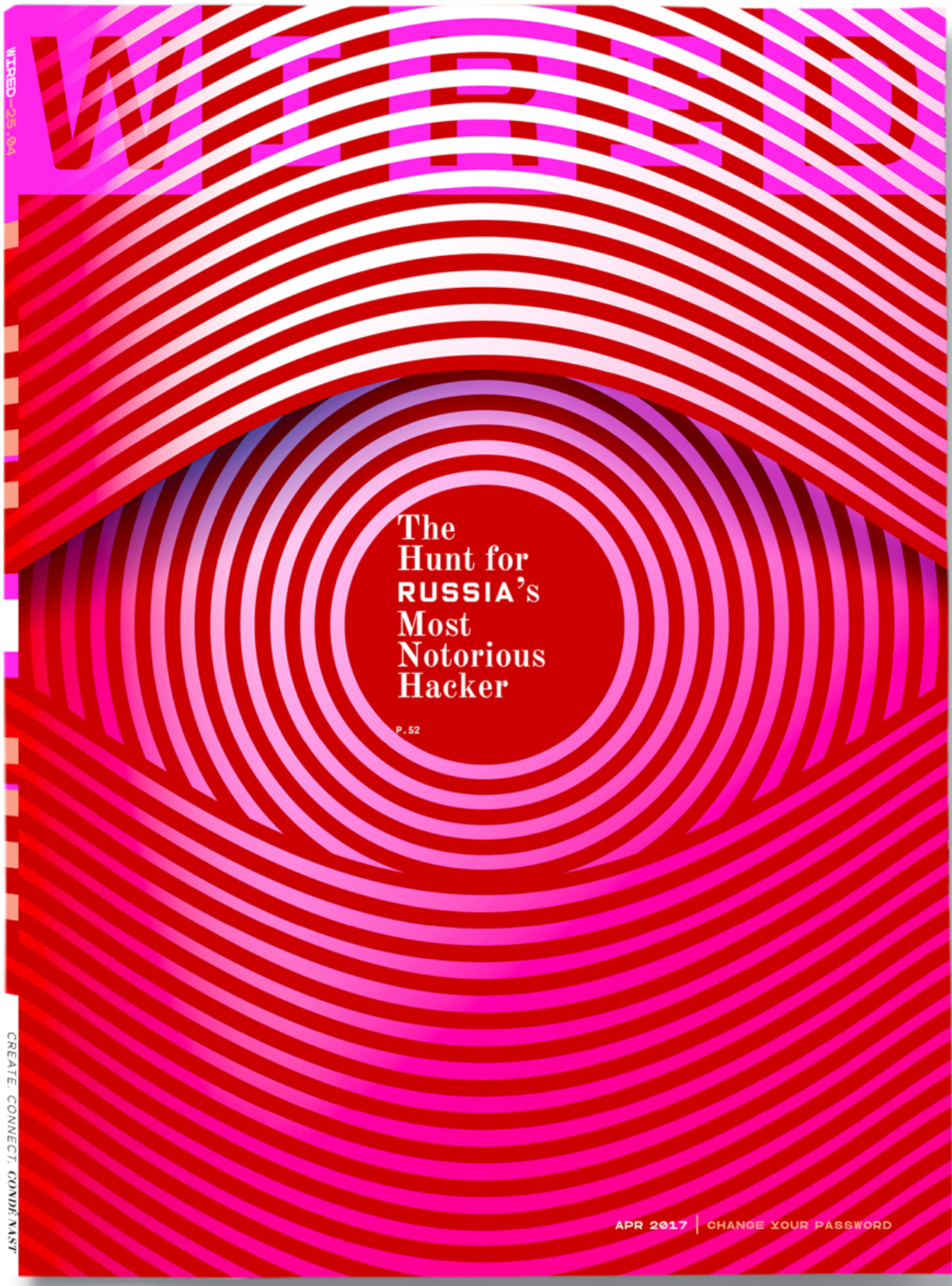
OMAHA

America's war with Russia's greatest cybercriminal began in the spring of 2009, when special agent James Craig, a rookie in the FBI's Omaha, Nebraska, field office, began looking into a strange pair of electronic thefts. A square-jawed former marine, Craig had been an agent for just six months, but his superiors tapped him for the case anyway, because of his background: For years, he'd been an IT guy for the FBI. One of his nicknames in college was "the silent geek."

While you log into seemingly secure websites, the malware modifies pages before they load, siphoning away your credentials and your account balance.

The leading victim in the case was a subsidiary of the payments-processing giant First Data, which lost $450,000 that May. That was quickly followed by a $100,000 theft from a client of the First National Bank of Omaha. What was odd, Craig noticed, was that the thefts seemed to have been executed from the victims' own IP addresses, using their own logins and passwords. Examining their computers, he saw that they were infected with the same malware: something called the Zeus Trojan horse.

In online security circles, Craig discovered, Zeus was notorious. Having first appeared in 2006, the malware had a reputation among both criminals and security experts as a masterpiece—smooth, effective, versatile. Its author was a phantom. He was only known online, where he went by the handle Slavik, or lucky12345, or a half-dozen other names.



April 2017. Subscribe to WIRED.

Zeus infected computers through fairly typical means: fake IRS emails, say, or illegitimate UPS shipping notices that tricked recipients into downloading a file. But once it was on your computer, Zeus let hackers play God: They could hijack websites and use a keystroke logger to record usernames, passwords, and PINs. Hackers could even modify login forms to request further valuable security information: a mother's maiden name, a Social Security number. The ruse is known as a "man in the browser" attack. While you sit at your computer logging into seemingly secure websites, the malware modifies pages before they load, siphoning away your credentials and your account balance. Only when you log in from a different computer do you even realize the money is gone.

By the time Craig started his investigation, Zeus had become the digital underground's malware of choice—the Microsoft Office of online fraud. Slavik was something rare in the malware world: a genuine professional. He regularly updated the Zeus code, beta-testing new features. His product was endlessly adaptable, with variants optimized for different kinds of attacks and targets. A computer infected with Zeus could even be folded into a botnet, a network of infected computers that can be harnessed together to run spam servers or distributed denial-of-service attacks, or send out more deceptive emails to spread the malware further.

But sometime shortly before Craig picked up his case in 2009, Slavik had begun to change tack. He started cultivating an inner circle of online criminals, providing a select group with a variant of his malware, called Jabber Zeus. It came equipped with a Jabber instant-message plug-in, allowing the group to communicate and coordinate attacks—like in the two Omaha thefts. Rather than rely on broad infection campaigns, they began to specifically target corporate accountants and people with access to financial systems.

As Slavik turned increasingly to organized crime, he dramatically narrowed his retail malware business. In 2010 he announced his "retirement" online and then released what security researchers came to call Zeus 2.1, an advanced version of his malware protected by an encryption key—effectively tying each copy to a specific user—with a price tag upwards of $10,000 per copy. Now, Slavik was only dealing with an elite, ambitious group of criminals.

"We had no idea how big this case was," Craig says. "The amount of activity from these guys was phenomenal." Other institutions began to come forward with losses and accounts of fraud. Lots of them. Craig realized that, from his desk in suburban Omaha, he was chasing a well-organized international criminal network. "The victims started falling out of the sky," Craig says. It dwarfed any other cybercrime the FBI had tackled before.

2

JABBER ZEUS

Craig's first major break in the case came in September 2009. With the help of some industry experts, he identified a New York–based server that seemed to play some sort of role in the Zeus network. He obtained a search warrant, and an FBI forensics team copied the server's data onto a hard drive, then overnighted it to Nebraska. When an engineer in Omaha examined the results, he sat in awe for a moment. The hard drive contained tens of thousands of lines of instant message chat logs in Russian and Ukrainian. Looking over at Craig, the engineer said: "You have their Jabber server."

This was the gang's whole digital operation—a road map to the entire case. The cybersecurity firm Mandiant dispatched an engineer to Omaha for months just to help untangle the Jabber Zeus code, while the FBI began cycling in agents from other regions on 30- or 90-day assignments. Linguists across the country pitched in to decipher the logs. "The slang was a challenge," Craig says.

One woman explained that she'd become a money mule after a job at a grocery store fell through, telling an agent: "I could strip, or I could do this."

The messages contained references to hundreds of victims, their stolen credentials scattered in English throughout the files. Craig and other agents started cold-calling institutions, telling them they had been hit by cyberfraud. He found that several businesses had terminated employees they suspected of the thefts—not realizing that the individuals' computers had been infected by malware and their logins stolen.

The case also expanded beyond the virtual world. In New York one day in 2009, three young women from Kazakhstan walked into the FBI field office there with a strange story. The women had come to the States to look for work and found themselves participating in a curious scheme: A man would drive them to a local bank and tell them to go inside and open a new account. They were to explain to the teller that they were students visiting for the summer. A few days later, the man had them return to the bank and withdraw all of the money in the account; they kept a small cut and passed the rest on to him. Agents pieced together that the women were "money mules": Their job was to cash out the funds that Slavik and his comrades had siphoned from legitimate accounts.

By the summer of 2010, New York investigators had put banks across the region on alert for suspicious cash-outs and told them to summon FBI agents as they occurred. The alert turned up dozens of mules withdrawing tens of thousands of dollars. Most were students or newly arrived immigrants in Brighton Beach. One woman explained that she'd become a mule after a job at a grocery store fell through, telling an agent: "I could strip, or I could do this." Another man explained that he'd be picked up at 9 am, do cash-out runs until 3 pm, and then spend the rest of the day at the beach. Most cash-outs ran around $9,000, just enough to stay under federal reporting limits. The mule would receive 5 to 10 percent of the total, with another cut going to the recruiter. The rest of the money would be sent overseas.

“The amount of organization these kids—they’re in their twenties—were able to pull together would’ve impressed any Fortune 100 company,” the FBI’s James Craig says.

The United States, moreover, was just one market in what investigators soon realized was a multinational reign of fraud. Officials traced similar mule routes in Romania, the Czech Republic, the United Kingdom, Ukraine, and Russia. All told, investigators could attribute around $70 million to $80 million in thefts to the group—but they suspected the total was far more than that.

Banks howled at the FBI to shut the fraud down and stanch the losses. Over the summer, New York agents began to close in on high-ranking recruiters and the scheme’s masterminds in the US. Two Moldovans were arrested at a Milwaukee hotel at 11 pm following a tip; one suspect in Boston tried to flee a raid on his girlfriend’s apartment and had to be rescued from the fire escape.

Meanwhile, Craig’s case in Omaha advanced against the broader Jabber Zeus gang. The FBI and the Justice Department had zeroed in on an area in eastern Ukraine around the city of Donetsk, where several of the Jabber Zeus leaders seemed to live. Alexey Bron, known online as “thehead,” specialized in moving the gang’s money around the world. Ivan Viktorvich Klepikov, who went by the moniker “petr0vich,” ran the group’s IT management, web hosting, and domain names. And Vyacheslav Igorevich Penchukov, a well-known local DJ who went by the nickname “tank,” managed the whole scheme, putting him second in command to Slavik. “The amount of organization these kids—they’re in their twenties—were able to pull together would’ve impressed any Fortune 100 company,” Craig says. The gang poured their huge profits into expensive cars (Penchukov had a penchant for high-end BMWs and Porsches, while Klepikov preferred Subaru WRX sports sedans), and the chat logs were filled with discussions of fancy vacations across Turkey, Crimea, and the United Arab Emirates.

By the fall of 2010, the FBI was ready to take down the network. As officials in Washington called a high-profile press conference, Craig found himself on a rickety 12-hour train ride across Ukraine to Donetsk, where he met up with agents from the country’s security service to raid tank’s and petr0vich’s homes. Standing in petr0vich’s living room, a Ukrainian agent told Craig to flash his FBI badge. “Show him it’s not just us,” he urged. Craig was stunned by the scene: The hacker, wearing a purple velvet smoking jacket, seemed unperturbed as agents searched his messy apartment in a Soviet-style concrete building; his wife held their baby in the kitchen, laughing with investigators. “This is the gang I’ve been chasing?” Craig thought. The raids lasted well into the night, and Craig didn’t return to his hotel until 3 am. He took nearly 20 terabytes of seized data back to Omaha.

With 39 arrests around the world—stretching across four nations—investigators managed to disrupt the network. But crucial players slipped away. One top mule recruiter in the US fled west, staying a step ahead of investigators in Las Vegas and Los Angeles before finally escaping the country inside a shipping container. More important, Slavik, the mastermind

himself, remained almost a complete cipher. Investigators assumed he was based in Russia. And once, in an online chat, they saw him reference that he was married. Other than that, they had nothing. The formal indictment referred to the creator of the Zeus malware using his online pseudonym. Craig didn't even know what his prime suspect looked like. "We have thousands of photos from tank, petr0vich—not once did we see Slavik's mug," Craig says. Soon even the criminal's online traces vanished. Slavik, whoever he was, went dark. And after seven years of chasing Jabber Zeus, James Craig moved on to other cases.

3

GAME NOT OVER

About a year after the FBI shut down the Jabber Zeus ring, the small community of online cybersecurity researchers who watch for malware and botnets began to notice a new variant of Zeus emerge. The malware's source code had been leaked online in 2011—perhaps purposefully, perhaps not—effectively turning Zeus into an open source project and setting off an explosion of new variants. But the version that caught the eyes of researchers was different: more powerful and more sophisticated, particularly in its approach to assembling botnets.

Until then, most botnets used a hub-and-spoke system—a hacker would program a single command server to distribute orders directly to infected machines, known as zombie computers. The undead army could then be directed to send out spam emails, distribute malware, or target websites for denial-of-service attacks. That hub-and-spoke design, though, made botnets relatively easy for law enforcement or security researchers to dismantle. If you could knock the command server offline, seize it, or disrupt a hacker's ability to communicate with it, you could usually break the botnet.

The gang's strategy represented an evolutionary leap in organized crime: Now they could do everything remotely, never touching a US jurisdiction.

This new Zeus variant, however, relied on both traditional command servers and peer-to-peer communication between zombie machines, making it extremely difficult to knock down. Infected machines kept a constantly updated list of other infected machines. If one device sensed that its connection with the command server had been interrupted, it would rely on the peer-to-peer network to find a new command server.

The network, in effect, was designed from the start to be takedown-proof; as soon as one command server was knocked offline, the botnet owner could just set up a new server somewhere else and redirect the peer-to-peer network to it. The new version became known as GameOver Zeus, after one of its file names, gameover2.php. The name also lent itself naturally to gallows humor: Once this thing infects your computer, went a joke among security experts, it's game over for your bank accounts.

As far as anyone could tell, GameOver Zeus was controlled by a very elite group of hackers—and the group's leader was Slavik. He had reemerged, more powerful than ever. Slavik's new crime ring came to be called the Business Club. A September 2011 internal announcement to the group—introducing members to a new suite of online tools for organizing money transfers and mules—concluded with a warm welcome to Slavik's select recipients: "We wish you all successful and productive work."

Like the Jabber Zeus network, the Business Club's prime directive was knocking over banks, which it did with even more ruthless inventiveness than its predecessor. The scheme was multipronged: First, the GameOver Zeus malware would steal a user's banking credentials, intercepting them as soon as someone with an infected computer logged into an online account. Then the Business Club would drain the bank account, transferring its funds into other accounts they controlled overseas. With the theft complete, the group would use its powerful botnet to hit the targeted financial institutions with a denial-of-service attack to distract bank employees and prevent customers from realizing their accounts had been emptied until after the money had cleared. On November 6, 2012, the FBI watched as the GameOver network stole $6.9 million in a single transaction, then hit the bank with a multiday denial-of-service attack.

Unlike the earlier Jabber Zeus gang, the more advanced network behind GameOver focused on larger six- and seven-figure bank thefts—a scale that made bank withdrawals in Brooklyn obsolete. Instead, they used the globe's interconnected banking system against itself, hiding their massive thefts inside the trillions of dollars of legitimate commerce that slosh around the world each day. Investigators specifically identified two areas in far eastern China, close to the Russian city of Vladivostok, from which mules funneled huge amounts of stolen money into Business Club accounts. The strategy, investigators realized, represented an evolutionary leap in organized crime: Bank robbers no longer had to have a footprint inside the US. Now they could do everything remotely, never touching a US jurisdiction. "That's all it takes to operate with impunity," says Leo Taddeo, a former top FBI official.

Chad Hagan

4

STOP THE BLEEDING

Banks weren't the gang's only targets. They also raided the accounts of nonfinancial businesses large and small, nonprofits, and even individuals. In October 2013, Slavik's group began deploying malware known as CryptoLocker, a form of ransomware that would encrypt the files upon an infected machine and force its owner to pay a small fee, say, $300 to $500, to unlock the files. It quickly became a favorite tool of the cybercrime ring, in part because it helped transform dead weight into profit. The trouble with building a massive botnet focused on high-level financial fraud, it turns out, is that most zombie computers don't connect to fat corporate accounts; Slavik and his associates found themselves with tens of thousands of mostly idle zombie machines. Though ransomware didn't yield huge amounts, it afforded the criminals a way to monetize these otherwise worthless infected computers.

The concept of ransomware had been around since the 1990s, but CryptoLocker took it mainstream. Typically arriving on a victim's machine under the cover of an unassuming email attachment, the Business Club's ransomware used strong encryption and forced victims to pay using bitcoin. It was embarrassing and inconvenient, but many relented. The Swansea, Massachusetts, police department grumpily ponied up $750 to get back one of its computers in November 2013; the virus "is so complicated and successful that you have to buy these bitcoins, which we had never heard of," Swansea police lieutenant Gregory Ryan told his local newspaper.

"When a bank gets attacked en masse—100 transactions a week—you stop caring about the specific malware and the individual attacks; you just need to stop the bleeding," says one Dutch security expert.

The following month, the security firm Dell SecureWorks estimated that as many as 250,000 machines worldwide had been infected with CryptoLocker that year. One researcher traced 771 ransoms that netted Slavik's crew a total of $1.1 million. "He was one of the first to realize how desperate people would be to regain access to their files," Brett Stone-Gross, a researcher with Dell SecureWorks at the time, says of Slavik. "He didn't charge an exorbitant amount, but he made a lot of money and created a new type of online crime."

As the GameOver network continued to gain strength, its operators kept adding revenue streams—renting out their network to other criminals to deliver malware and spam or to carry out projects like click fraud, ordering zombie machines to generate revenue by clicking on ads on fake websites.

With each passing week, the cost to banks, businesses, and individuals from GameOver grew. For businesses, the thefts could easily wipe out a year's profits, or worse. Domestically, victims ranged from a regional bank in north Florida to a Native American tribe in Washington state. As it haunted large swathes of the private sector, GameOver absorbed more and more of the efforts of the private cybersecurity industry. The sums involved were staggering. "I don't think anyone has a grasp of the full extent—one $5 million theft overshadows hundreds of smaller thefts," explains Michael Sandee, a security expert at the

Dutch firm Fox-IT. “When a bank gets attacked en masse—100 transactions a week—you stop caring about the specific malware and the individual attacks; you just need to stop the bleeding.”

Many tried. From 2011 through 2013, cybersecurity researchers and various firms mounted three attempts to take down GameOver Zeus. Three European security researchers teamed up to make a first assault in the spring of 2012. Slavik easily repelled their attack. Then, in March 2012, Microsoft’s Digital Crimes Unit took civil legal action against the network, relying upon US marshals to raid data centers in Illinois and Pennsylvania that housed Zeus command-and-control servers and aiming legal action against 39 individuals thought to be associated with the Zeus networks. (Slavik was first on the list.) But Microsoft’s plan failed to put a dent in GameOver. Instead it merely clued Slavik in to what investigators knew about his network and allowed him to refine his tactics.

5

ASSAULT

Botnet fighters are a small, proud group of engineers and security researchers—self-proclaimed “internet janitors” who work to keep online networks running smoothly. Within that group, Tillmann Werner—the tall, lanky German researcher with the security firm CrowdStrike—had become known for his flair and enthusiasm for the work. In February 2013 he seized control of the Kelihos botnet, an infamous malware network built on Viagra spam, live onstage during a presentation at the cybersecurity industry’s biggest conference. But Kelihos, he knew, was no GameOver Zeus. Werner had been watching GameOver since its inception, marveling at its strength and resilience.

In 2012 he had linked up with Stone-Gross—who was just a few months out of graduate school and was based in California—plus a few other researchers to map out an effort to attack GameOver. Working across two continents largely in their spare time, the men plotted their attack via online chat. They carefully studied the previous European effort, identifying where it had failed, and spent a year preparing their offensive.

At the peak of their attack, the researchers controlled 99 percent of Slavik’s network—but they’d overlooked a critical source of resilience in GameOver’s structure.

In January 2013, they were ready: They stocked up on pizza, assuming they were in for a long siege against Slavik’s network. (When you go against a botnet, Werner says, “you have one shot. It either goes right or wrong.”) Their plan was to reroute GameOver’s peer-to-peer network, centralize it, and then redirect the traffic to a new server under their control—a process known as “sinkholing.” In doing so, they hoped to sever the botnet’s communication link to Slavik. And at first, everything went well. Slavik showed no signs of fighting back, and Werner and Stone-Gross watched as more and more infected computers connected to their sinkhole by the hour.

At the peak of their attack, the researchers controlled 99 percent of Slavik's network—but they'd overlooked a critical source of resilience in GameOver's structure: a small subset of infected computers were still secretly communicating with Slavik's command servers. "We missed that there's a second layer of control," Stone-Gross says. By the second week, Slavik was able to push a software update to his whole network and reassert his authority. The researchers watched with dawning horror as a new version of GameOver Zeus propagated across the internet and Slavik's peer-to-peer network began to reassemble. "We immediately saw what happened—we'd completely neglected this other channel of communication," Werner says.

The researchers' ploy—nine months in the making—had failed. Slavik had won. In a trollish online chat with a Polish security team, he crowed about how all the efforts to seize his network had come to naught. "I don't think he thought it was possible to take down his botnet," Werner says. Dejected, the two researchers were eager to try again. But they needed help—from Pittsburgh.

6

PITTSBURGH

Over the past decade, the FBI's Pittsburgh field office has emerged as the source of the government's biggest cybercrime indictments, thanks in no small part to the head of the local cybersquad there, a onetime furniture salesman named J. Keith Mularski.

An excitable and gregarious agent who grew up around Pittsburgh, Mularski has become something of a celebrity in cybersecurity circles. He joined the FBI in the late '90s and spent his first seven years in the bureau working espionage and terrorism cases in Washington, DC. Jumping at the chance to return home to Pittsburgh, he joined a new cyber initiative there in 2005, despite the fact that he knew little about computers. Mularski trained on the job during a two-year undercover investigation chasing identity thieves deep in the online forum DarkMarket. Under the screen name Master Splyntr—a handle inspired by Teenage Mutant Ninja Turtles—Mularski managed to become a DarkMarket administrator, putting himself at the center of a burgeoning online criminal community. In his guise, he even chatted online with Slavik and reviewed an early version of the Zeus malware program. His DarkMarket access eventually helped investigators arrest 60 people across three continents.

Even after millions of dollars in thefts, neither the FBI nor the security industry had so much as a single Business Club member's name.

In the years that followed, the head of the Pittsburgh office decided to invest aggressively in combating cybercrime—a bet on its increasing importance. By 2014, the FBI agents in Mularski's squad, together with another squad assigned to a little-known Pittsburgh institution called the National Cyber-Forensics and Training Alliance, were prosecuting some of the Justice Department's biggest cases. Two of Mularski's agents, Elliott Peterson and

Steven J. Lampo, were chasing the hackers behind GameOver Zeus, even as their desk-mates simultaneously investigated a case that would ultimately indict five Chinese army hackers who had penetrated computer systems at Westinghouse, US Steel, and other companies to benefit Chinese industry.

The FBI's GameOver case had been under way for about a year by the time Werner and Stone-Gross offered to join forces with the Pittsburgh squad to take down Slavik's botnet. If they had approached any other law-enforcement agency, the response might have been different. Government cooperation with industry was still a relatively rare phenomenon; the Feds' style in cyber cases was, by reputation, to hoover up industry leads without sharing information. But the team in Pittsburgh was unusually practiced at collaboration, and they knew that the two researchers were the best in the field. "We jumped at the chance," Mularski says.

Both sides realized that in order to tackle the botnet, they needed to work on three simultaneous fronts. First, they had to figure out once and for all who was running GameOver—what investigators call "attribution"—and build up a criminal prosecution; even after millions of dollars in thefts, neither the FBI nor the security industry had so much as a single Business Club member's name. Second, they needed to take down the digital infrastructure of GameOver itself; that's where Werner and Stone-Gross came in. And third, they needed to disable the botnet's physical infrastructure by assembling court orders and enlisting the help of other governments to seize its servers across the globe. Once all that was done, they needed partners in the private sector to be ready with software updates and security patches to help recover infected computers the moment the good guys had control of the botnet. Absent any one of those moves, the next effort to take down GameOver Zeus was likely to fail just as the previous ones had.

The network was run through two password-protected British websites, which contained careful records, FAQs, and a "ticket" system for resolving technical issues.

With that, Mularski's squad began to stitch together an international partnership unlike anything the US government had ever undertaken, enlisting the UK's National Crime Agency, officials in Switzerland, the Netherlands, Ukraine, Luxembourg, and a dozen other countries, as well as industry experts at Microsoft, CrowdStrike, McAfee, Dell SecureWorks, and other companies.

First, to help nail down Slavik's identity and get intelligence on the Business Club, the FBI teamed up with Fox-IT, a Dutch outfit renowned for its expertise in cyber-forensics. The Dutch researchers got to work tracing old usernames and email addresses associated with Slavik's ring to piece together an understanding of how the group operated.

The Business Club, it turned out, was a loose confederation of about 50 criminals, who each paid an initiation fee to access GameOver's advanced control panels. The network was run through two password-protected British websites, Visitcoastweekend.com and

Work.businessclub.so, which contained careful records, FAQs, and a “ticket” system for resolving technical issues. When investigators got legal permission to penetrate the Business Club server, they found a highly detailed ledger tracking the group’s various ongoing frauds. “Everything radiated professionalism,” Fox-IT’s Michael Sandee explains. When it came to pinpointing the precise timing of transactions between financial institutions, he says, “they probably knew better than the banks.”

Chad Hagan

7

SPYWARE

One Day, after months of following leads, the investigators at Fox-IT got a tip from a source about an email address they might want to look into. It was one of many similar tips they'd chased down. "We had a lot of bread crumbs," Mularski says. But this one led to something vital: The team was able to trace the email address to a British server that Slavik used to run the Business Club's websites. More investigative work and more court orders eventually led authorities to Russian social media sites where the email address was connected to a real name: Evgeniy Mikhailovich Bogachev. At first it was meaningless to the group. It took weeks' more effort to realize that the name actually belonged to the phantom who had invented Zeus and created the Business Club.

Slavik, it turned out, was a 30-year-old who lived an upper-middle-class existence in Anapa, a Russian resort city on the Black Sea. Online photos showed that he enjoyed boating with his wife. The couple had a young daughter. One photo showed Bogachev posing in leopard-print pajamas and dark sunglasses, holding a large cat. The investigative team realized that he had written the first draft of Zeus when he was just 22 years old.

The team couldn't find specific evidence of a link between Bogachev and the Russian state, but some entity seemed to be feeding Slavik specific terms to search for in his vast network of zombie computers.

But that wasn't the most astounding revelation that the Dutch investigators turned up. As they continued their analysis, they noticed that someone at the helm of GameOver had been regularly searching tens of thousands of the botnet's infected computers in certain countries for things like email addresses belonging to Georgian intelligence officers or leaders of elite Turkish police units, or documents that bore markings designating classified Ukrainian secrets. Whoever it was was also searching for classified material linked to the Syrian conflict and Russian arms dealing. At some point, a light bulb went off. "These are espionage commands," Sandee says.

GameOver wasn't merely a sophisticated piece of criminal malware; it was a sophisticated intelligence-gathering tool. And as best as the investigators could determine, Bogachev was the only member of the Business Club who knew about this particular feature of the botnet. He appeared to be running a covert operation right under the noses of the world's most prolific bank robbers. The FBI and Fox-IT team couldn't find specific evidence of a link between Bogachev and the Russian state, but some entity seemed to be feeding Slavik specific terms to search for in his vast network of zombie computers. Bogachev, it appeared, was a Russian intelligence asset.

In March 2014, investigators could even watch as an international crisis played out live inside the snow globe of Bogachev's criminal botnet. Weeks after the Sochi Olympics, Russian forces seized the Ukrainian region of Crimea and began efforts to destabilize the country's eastern border. Right in step with the Russian campaign, Bogachev redirected a section of

his botnet to search for politically sensitive information on infected Ukrainian computers—trawling for intelligence that might help the Russians anticipate their adversaries' next moves.

The team was able to construct a tentative theory and history of Bogachev's spycraft. The apparent state connection helped explain why Bogachev had been able to operate a major criminal enterprise with such impunity, but it also shed new light on some of the milestones in the life of Zeus. The system that Slavik used to make his intelligence queries dated back approximately to the moment in 2010 when he faked his retirement and made access to his malware far more exclusive. Perhaps Slavik had appeared on the radar of the Russian security services at some point that year, and in exchange for a license to commit fraud without prosecution—outside Russia, of course—the state made certain demands. To carry them out with maximum efficacy and secrecy, Slavik asserted tighter control over his criminal network.

The discovery of Bogachev's likely intelligence ties introduced some trickiness to the operation to take down GameOver—especially when it came to the prospect of enlisting Russian cooperation. Otherwise, the plan was rumbling along. Now that the investigators had zeroed in on Bogachev, a grand jury could finally indict him as the mastermind behind GameOver Zeus. American prosecutors scrambled to bring together civil court orders to seize and disrupt the network. "When we were really running, we had nine people working this—and we only have 55 total," says Michael Comber of the US Attorney's office in Pittsburgh. Over a span of months, the team painstakingly went to internet service providers to ask permission to seize GameOver's existing proxy servers, ensuring that at the right moment, they could flip those servers and disable Slavik's control. Meanwhile, the Department of Homeland Security, Carnegie Mellon, and a number of antivirus companies readied themselves to help customers regain access to their infected computers. Weekly conference calls spanned continents as officials coordinated action in Britain, the US, and elsewhere.

By late spring 2014, as pro-Russian forces fought in Ukraine proper, the American-led forces got ready to move in on GameOver. They'd been plotting to take down the network for more than a year, carefully reverse-engineering the malware, covertly reading the criminal gang's chat logs to understand the group's psychology, and tracing the physical infrastructure of servers that allowed the network to propagate around the globe. "By this point, these researchers knew the malware better than the author," says Elliott Peterson, one of the lead FBI agents on the case. As Mularski recalls, the team checked off all the crucial boxes: "Criminally, we can do it. Civilly, we can do it. Technically we can do it." Working with a cast of dozens, communicating with more than 70 internet service providers and a dozen other law enforcement agencies from Canada to the United Kingdom to Japan to Italy, the team readied an attack to commence on Friday, May 30.

8

TAKEDOWN

The week leading up to the attack was a frantic scramble. When Werner and Stone-Gross arrived in Pittsburgh, Peterson had them over to his family's apartment, where his kids gawked at Werner and his German accent. Over dinner and Fathead beer, they took stock of their looming attempt. They were running way behind—Werner's code wasn't close to being ready. Over the rest of the week, as Werner and Stone-Gross raced to finish writing, another team assembled the last court orders, and still others ran herd on the ad hoc group of two dozen governments, companies, and consultants who were helping to take GameOver Zeus down. The White House had been briefed on the plan and was waiting for results. But the effort seemed to be coming apart at the seams.

For instance, the team had known for months that the GameOver botnet was controlled by a server in Canada. But then, just days before the attack, they discovered that there was a second command server in Ukraine. The realization made hearts drop. "If you're not even aware of the second box," Werner says, "how sure are you that there's not a third box?"

Bogachev readied for battle—wrestling for control of his network, testing it, redirecting traffic to new servers, and deciphering the Pittsburgh team's method of attack.

On Thursday, Stone-Gross carefully talked more than a dozen internet service providers through the procedures they needed to follow as the attack launched. At the last minute, one key service provider backed out, fearful that it would incur Slavik's wrath. Then, on Friday morning, Werner and Stone-Gross arrived at their office building on the banks of the Monongahela River to find that one of the operation's partners, McAfee, had prematurely published a blog post announcing the attack on the botnet, titled "It's 'Game Over' for Zeus and Cryptolocker."

After frantic calls to get the post taken down, the attack finally began. Canadian and Ukrainian authorities shut down GameOver's command servers, knocking each offline in turn. And Werner and Stone-Gross began redirecting the zombie computers into a carefully built "sinkhole" that would absorb the nefarious traffic, blocking the Business Club's access to its own systems. For hours, the attack went nowhere; the researchers struggled to figure out where the bugs lay in their code.

By 1 pm, their sinkhole had drawn in only about a hundred infected computers, an infinitesimal percentage of the botnet that had grown to as many as half a million machines. A line of officials stood behind Werner and Stone-Gross in a conference room, literally watching over their shoulders as the two engineers debugged their code. "Not to put any pressure on you," Mularski urged at one point, "but it'd be great if you could get it running."

Finally, by evening Pittsburgh time, the traffic to their sinkhole began to climb. On the other side of the world, Bogachev came online. The attack had interrupted his weekend. Perhaps he didn't think much of it at first, given that he had easily weathered other attempts to seize control of his botnet. "Right away, he's kicking the tires. He doesn't know what we've done," Peterson recalls. That night, yet again, Bogachev readied for battle—wrestling for control of his network, testing it, redirecting traffic to new servers, and deciphering the Pittsburgh team's method of attack. "It was cyber-hand-to-hand combat," recalls Pittsburgh US attorney David Hickton. "It was amazing to watch."

The team was able to monitor Bogachev's communication channels without his knowledge and knock out his Turkish proxy server. Then they watched as he tried to come back online using the anonymizing service Tor, desperate to get some visibility into his losses. Finally, after hours of losing battles, Slavik went silent. The attack, it appeared, was more than he had bargained for. The Pittsburgh team powered on through the night. "He must've realized it was law enforcement. It wasn't just the normal researcher attack," Stone-Gross says.

By Sunday night, nearly 60 hours in, the Pittsburgh team knew they'd won. On Monday, June 2, the FBI and Justice Department announced the takedown and unsealed a 14-count indictment against Bogachev.

Over the coming weeks, Slavik and the researchers continued to do occasional battle—Slavik timed one counterattack for a moment when Werner and Stone-Gross were presenting at a conference in Montreal—but ultimately the duo prevailed. Amazingly, more than two years later, the success has largely stuck: The botnet has never reassembled, though about 5,000 computers worldwide remain infected with Zeus malware. The industry partners are still maintaining the server sinkhole that's swallowing up the traffic from those infected computers.

For about a year after the attack, so-called account-takeover fraud all but disappeared in the US. Researchers and investigators had long assumed that dozens of gangs must have been responsible for the criminal onslaught that the industry endured between 2012 and 2014. But nearly all of the thefts came from just a small group of highly skilled criminals—the so-called Business Club. "You come into this and hear they're everywhere," Peterson says, "and actually it's a very tiny network, and they're much easier to disrupt than you think."

9

AFTER

In 2015, the State Department put a $3 million bounty on Bogachev's head, the highest reward the US has ever posted for a cybercriminal. But he remains at large. According to US intelligence sources, the government does not, in fact, suspect that Bogachev took part in the Russian campaign to influence the US election. Rather, the Obama administration included him in the sanctions to put pressure on the Russian government. The hope is that

the Russians might be willing to hand over Bogachev as a sign of good faith, since the botnet that made him so useful to them is defunct. Or maybe, with the added attention, someone will decide they want the $3 million reward and tip off the FBI.

The uncomfortable truth is that Bogachev and other Russian cybercriminals lie pretty far beyond America's reach.

But the uncomfortable truth is that Bogachev and other Russian cybercriminals lie pretty far beyond America's reach. The huge questions that linger over the GameOver case—like those surrounding Bogachev's precise relationship to Russian intelligence and the full tally of his thefts, which officials can only round to the nearest $100 million or so—foreshadow the challenges that face the analysts looking into the election hacks. Fortunately, the agents on the case have experience to draw from: The DNC breach is reportedly being investigated by the FBI's Pittsburgh office.

In the meantime, Mularski's squad and the cybersecurity industry have also moved on to new threats. The criminal tactics that were so novel when Bogachev helped pioneer them have now grown commonplace. The spread of ransomware is accelerating. And today's botnets—especially Mirai, a network of infected Internet of Things devices—are even more dangerous than Bogachev's creations.

Nobody knows what Bogachev himself might be cooking up next. Tips continue to arrive regularly in Pittsburgh regarding his whereabouts. But there are no real signs he has reemerged. At least not yet.

Garrett M. Graff *(@vermontgmg) wrote about James Clapper in issue 24.12.*

This article appears in the April issue. Subscribe now.