

THE RUSSIAN EXPAT LEADING THE FIGHT TO PROTECT AMERICA

IN A WAR AGAINST HACKERS, DMITRI ALPEROVITCH AND CROWDSTRIKE ARE OUR SPECIAL FORCES (AND PUTIN'S WORST NIGHTMARE).

BY VICKY WARD OCT 24, 2016

f

3.1k

t six o'clock on the morning of May 6, Dmitri Alperovitch woke up in a Los Angeles hotel to an alarming email. Alperovitch is the thirty-six-year-old cofounder of the cybersecurity firm CrowdStrike, and late the previous night, his company had been asked by the Democratic National Committee to investigate a possible breach of its network. A CrowdStrike security expert had sent the DNC a proprietary software package, called Falcon, that monitors the networks of its clients in real time. Falcon "lit up," the email said, within ten seconds of being installed at the DNC: Russia was in the network.

 \bigcirc

ADVERTISEMENT - CONTINUE READING BELOW

 \square

Alperovitch, a slight man with a sharp, quick demeanor, called the analyst who had emailed the report. "Are we sure it's Russia?" he asked.



Christopher Leaman

The analyst said there was no doubt. Falcon had detected malicious software, or malware, that was stealing data and sending it to the same servers that had been used in a 2015 attack on the German Bundestag. The code and techniques used against the DNC resembled those from earlier attacks on the White House and the State Department. The analyst, a former intelligence officer, told Alperovitch that Falcon had identified not one but two Russian intruders: Cozy Bear, a group CrowdStrike's experts believed was affiliated with the FSB, Russia's answer to the CIA; and Fancy Bear, which they had linked to the GRU, Russian military intelligence.

that retraced the hackers' steps and pieced together the pathology of the breach. Over the next two weeks, they learned that Cozy Bear had been stealing emails from the DNC for more than a year. Fancy Bear, on the other hand, had been in the network for only a few weeks. Its target was the DNC research department, specifically the material that the committee was compiling on Donald Trump and other Republicans. Meanwhile, a CrowdStrike group called the Overwatch team used Falcon to monitor the hackers, a process known as shoulder-surfing.

Ultimately, the teams decided it was necessary to replace the software on every computer at the DNC. Until the network was clean, secrecy was vital. On the afternoon of Friday, June 10, all DNC employees were instructed to leave their laptops in the office. Alperovitch told me that a few people worried that Hillary Clinton, the presumptive Democratic nominee, was clearing house. "Those poor people thought they were getting fired," he says.





For the next two days, three CrowdStrike employees worked inside DNC headquarters, replacing the software and setting up new login credentials using what Alperovitch considers to be the most secure means of choosing a password: flipping through the dictionary at random. (After this article was posted online, Alperovitch noted that the passwords included random characters in addition to the words.) The Overwatch team kept an eye on Falcon to ensure there were no new intrusions. On Sunday night, once the operation was complete, Alperovitch took his team to celebrate at the Brazilian steakhouse Fogo de Chão.

ADVERTISEMENT - CONTINUE READING BELOW

A few people worried that Hillary Clinton, the presumptive Democratic nominee, was clearing house.

Hacking, like domestic abuse, is a crime that tends to induce shame. Companies such as Yahoo usually publicize their breaches only when the law requires it. For this reason, Alperovitch says, he expected that the DNC, too, would want to keep quiet.

By the time of the hack, however, Donald Trump's relationship to Russia had become an issue in the election. The DNC wanted to go public. At the committee's request, Alperovitch and Henry briefed a reporter from *The Washington Post* about the attack. On June 14, soon after the *Post* story publicly linked Fancy Bear with the Russian GRU and Cozy Bear with the FSB for the first time, Alperovitch published a detailed blog post about the attacks.

Alperovitch told me he was thrilled that the DNC decided to publicize Russia's involvement. "Having a client give us the ability to tell the full story" was a "milestone in the industry," he says. "Not just highlighting a rogue nation-state's actions but explaining what was taken and how and when. These stories are almost never told."

Cilluffo, the former special assistant to the president for homeland security, likens Alperovitch to Paul Revere: "Dmitri, as an individual, has played a significant role in elevating cybersecurity policy not only inside the private sector but more generally."



Christopher Leaman

When I met Alperovitch in late September, at his open-plan offices outside Washington, D.C., he explained that CrowdStrike was created to take advantage of a simple but central lesson he'd learned about stopping hackers. It's not enough, he says, to play defense with technology: "Otherwise the adversary will scale up and it becomes a game of numbers, which they will win." Instead, attribution is crucial: First you need to identify the perpetrator, then you need to discover what motivates the crime, and finally—most important—you need to figure out how to fight back.

ADVERTISEMENT - CONTINUE READING BELOW

Before Alperovitch founded CrowdStrike, the idea that attribution ought to be a central defense against hackers was viewed as heresy. In 2011, he was working in Atlanta as the chief threat officer at the antivirus software firm McAfee. While sifting through server logs in his apartment one night, he discovered evidence of a hacking campaign by the Chinese government. Eventually he learned that the campaign had been going on undetected for five years, and that the Chinese had compromised at least seventy-one companies and organizations, including thirteen defense contractors, three electronics firms, and the International Olympic Committee.

That the Chinese government had been stealing information from the private sector was a shock to the security industry and to many U. S. officials. Almost no one thought that foreign governments used the Internet for anything other than old-fashioned espionage. "This was not spy versus spy," says John Carlin, who was until recently the assistant attorney general for national security. The hacking was economic sabotage.

While Alperovitch was writing up his report on the breach, he received a call from Renee James, an executive at Intel, which had recently purchased McAfee. According to Alperovitch, James told him, "Dmitri, Intel has a lot of business in China. You cannot call out China in this report."

Alperovitch removed the word *China* from his analysis, calling the operation Shady Rat instead. He told me that James's intervention accelerated his plans to leave Intel. (James

Q

Alperovitch and George Kurtz, a former colleague, founded CrowdStrike as a direct response. The cybersecurity industry at the time, Alperovitch says, was "terrified of losing their ability to market products in China." Their new company would push the idea that hacking was a means, not an end. "We saw that no one's really focused on the adversary," Alperovitch told me. "No one's focusing exclusively on how can we actually identify them, attribute them, deter them from taking this action again." CrowdStrike's tagline encapsulated its philosophy: "You don't have a malware problem, you have an adversary problem."

perovitch's June 14 blog post garnered so much media attention that even its ebullient author felt slightly overwhelmed. Inevitably there were questions about the strange names his company had given the Russian hackers. As it happened, "Fancy Bear" and "Cozy Bear" were part of a coding system Alperovitch had created. Animals signified the hackers' country of origin: Russians were bears, Chinese were pandas, Iranians were kittens, and North Koreans were named for the chollima, a mythical winged horse. By company tradition, the analyst who discovers a new hacker gets to choose the first part of the nickname. Cozy Bear got its nickname because the letters *coz* appeared in its malware code. Fancy Bear, meanwhile, used malware that included the word *Sofacy*, which reminded the analyst who found it of the Iggy Azalea song "Fancy."

The day after the media maelstrom, the reporters were back with less friendly questions: Had Alperovitch gotten his facts right? Was he certain Russia was behind the DNC hacks? The doubts were prompted by the appearance of a blogger claiming to be from Eastern Europe who called himself Guccifer 2.0. Guccifer said that the breach was his, not Russia's. "DNC'S servers hacked by a lone hacker," he wrote in a blog post that included stolen files from the DNC. "I guess CrowdStrike customers should think twice about company's competence," Guccifer wrote. "Fuck CrowdStrike!!!!!!!!"

Guccifer said that the breach was his, not Russia's

Alperovitch was bewildered. In a career spanning nearly two decades, he had never made an incorrect attribution in public. "Did we miss something?" he asked CrowdStrike's forensics

ADVERTISEMENT - CONTINUE READING BELOW

Alperovitch had also never seen someone claim to be the only intruder on a site. "No hacker goes into the network and does a full forensic investigation," he told me. Being called out, he said, was "very shocking. It was clearly an attack on us as well as on the DNC."

Alperovitch initially thought that the leaks were standard espionage and that Guccifer's attacks on CrowdStrike were just a noisy reaction to being busted. "I thought, *Okay, they got really upset that they were caught,*" he said. But after documents from the DNC continued to leak, Alperovitch decided the situation was far worse than that. He concluded that the Russians wanted to use the leaked files to manipulate U. S. voters—a first. "It hit me that, holy crap, this is an influence operation. They're actually trying to inject themselves into the election," he said. "I believe that we may very well wake up on the morning the day after the election and find statements from Russian adversaries saying, 'Do not trust the result.' "

Q

s it turned out, many reporters found Guccifer's leaked documents too cumbersome to sift through, and some were nervous that files from the strange website might contain viruses. But on July 22, three days before the Democratic convention in Philadelphia, WikiLeaks dumped a massive cache of emails that had been stolen from the DNC. Unlike the leaks published by Guccifer, these were organized and easily searchable. Reporters soon found emails suggesting that the DNC leadership had favored Hillary Clinton in her primary race against Bernie Sanders, which led Debbie Wasserman Schultz, the DNC chair, along with three other officials, to resign.

Days later, Alperovitch got a call from a Reuters reporter asking whether the Democratic Congressional Campaign Committee had been hacked. CrowdStrike had, in fact, been working on a breach at the DCCC; once again, Alperovitch believed that Russia was responsible. Now, however, he suspected that only Fancy Bear was involved. A lawyer for the DCCC gave Alperovitch permission to confirm the leak and to name Russia as the suspected author.



Christopher Leaman

Two weeks later, files from the DCCC began to appear on Guccifer 2.0's website. This time he released information about Democratic congressional candidates who were running close races in Florida, Ohio, Illinois, and Pennsylvania. On August 12, he went further, publishing a spreadsheet that included the personal email addresses and phone numbers of nearly two hundred Democratic members of Congress.

Alperovitch was in New York when he read about the leak on Twitter. He and Henry were asked to join a conference call with Nancy Pelosi, the House minority leader, and the chair of the DCCC. Pelosi said she'd warned her colleagues to keep their phones away from their

the election.

ADVERTISEMENT - CONTINUE READING BELOW

"I remember getting off that call feeling completely outraged," he said. "I called up Shawn. I'm like, 'I can't believe the Russians are getting away with it. These are congresspeople. I can't believe that there's still no response from this government.' "

Alperovitch's friends in government told him privately that an official attribution so close to the election would look political. If the government named Russia, it would be accused of carrying water for Hillary Clinton. The explanations upset Alperovitch. The silence of the American government began to feel both familiar and dangerous. "It doesn't help us if two years from now someone gets indicted," he said. After Michelle Obama's passport was published online, on September 22, Alperovitch threw up his hands in exasperation. "That is Putin giving us the finger," he told me.

Q

systems. He was born in 1980 in Moscow, in an era when people were afraid to discuss politics even inside their homes. His father, Michael, was a nuclear physicist who barely escaped being sent to Chernobyl as part of a rescue mission in 1986. Many of Michael's close friends and colleagues died of radiation poisoning within months of flying to the burning power plant. The takeaway for Dmitri was that "life is cheap in the Soviet Union."

Michael also taught Dmitri to code. Without a computer at home, Dmitri practiced by writing down algorithms on paper. In 1990, his father was sent to Maryland as part of a nuclear-safety training program for scientists. Per Soviet custom, Dmitri stayed in the USSR to ensure that his parents didn't defect. He lived with his grandparents, and when his parents returned, after a year, they brought him his first computer, an IBM PC.

Without a computer at home, Dmitri practiced by writing down algorithms on paper

In 1994, his father was granted a visa to Canada, and a year later the family moved to Chattanooga, where Michael took a job with the Tennessee Valley Authority. The work was not particularly challenging, so Michael began studying cryptography on the side. While Dmitri was still in high school, he and his father started an encryption-technology business. Dmitri says he loved the beauty of the math but also saw cryptography's fatal flaw: "If someone stole your keys to encrypt the data, it didn't matter how secure the algorithms were."

Alperovitch studied computer science at Georgia Tech and went on to work at an antispam software firm. There he met a striking dark-haired computer geek named Phyllis Schneck. As a teenager, Schneck once showed her father that she could hack into the company where he worked as an engineer. Appalled, Dr. Schneck made his daughter promise never to do something like that again.



Phyllis Schneck learned how to hack when she was still a teenager. Today she serves as the chief cybersecurity official at the Department of Homeland Security.

Christopher Leaman

Fighting email spam taught Alperovitch a second crucial lesson. He discovered that every time he blocked a server, the spammers deployed a hundred new servers to take its place. Alperovitch realized that defense was about psychology, not technology.

ADVERTISEMENT - CONTINUE READING BELOW

To better understand his adversaries, Alperovitch posed as a Russian gangster on spam discussion forums, an experience he wrote up in a series of reports. One day he returned from lunch to a voice mail telling him to call the FBI immediately. He was terrified. "I was not a citizen yet," he told me.

As it happened, the bureau was interested in his work. The government was slowly waking up to the realization that the Internet was ripe for criminal exploitation: "the great price of the digital age," in John Carlin's words. In 2004, the bureau was hacked by Joseph Colon, a disgruntled IT consultant who gained "god-level" access to FBI files. Colon was eventually indicted, but his attack showed the government how vulnerable it was to cybercrime.

In 2005, Alperovitch flew to Pittsburgh to meet an FBI agent named Keith Mularski, who had been asked to lead an undercover operation against a vast Russian credit-card-theft syndicate. Mularski had no prior experience with the Internet; he relied on Alperovitch, whom he calls "a good guy and a friend," to teach him how to get into the forum and speak the lingo. Mularski's sting operation took two years, but it ultimately brought about fifty-six arrests.

belonging to human-rights activists in China had been breached. Google suspected the Chinese government. Alperovitch found that the breach was unprecedented in scale; it affected more than a dozen of McAfee's clients.

Three days after his discovery, Alperovitch was on a plane to Washington. He'd been asked to vet a paragraph in a speech by the secretary of state, Hillary Clinton. She'd decided, for the first time, to call out another country for a cyberattack. "In an interconnected world," she said, "an attack on one nation's networks can be an attack on all."



Hackers and Their Targets: Flying Kitten (Iran): Defense firms, Iranian dissidents; Deep Panda (China): Asian-policy experts in the U. S.; Silent Chollima (North Korea) Sony, South Korean firms

Tavis Coburn

Ξ

investigate a breach of its network. The company needed just two hours to identify North Korea as the adversary. Executives at Sony asked Alperovitch to go public with the information immediately, but it took the FBI another three weeks before it confirmed the attribution.

The delay still frustrates Alperovitch, who saw the long silence as a kind of disinformation. "Yesterday you had no idea. Today you're 100 percent certain. It wasn't credible." From the perspective of the government, however, the handling of the Sony hack was a triumph. "In twenty-six days we figured out it was North Korea," John Carlin told me. The attribution changed the focus, he said, from what Sony did wrong to how the government was going to respond to North Korea. As Phyllis Schneck, who now works at the Department of Homeland Security, told me, the government moves slowly because it cannot afford to be wrong: "Vendors like to be first. Government must be right."

ADVERTISEMENT - CONTINUE READING BELOW

Q

members of the Chinese People's Liberation Army had been indicted by a grand jury in Pennsylvania for stealing economic secrets from the computers of U. S. firms in the nuclear, solar, and metals industries. Carlin told me that the indictments were meant as "a giant No Trespass sign: Get off our lawn." But the indictment didn't stop the hackers. Alperovitch went on television to call for a stronger response. In April 2015, after President Obama signed an executive order threatening sanctions against the Chinese, Alperovitch received a call from the White House. "You should be happy," he was told. "You're the one who's been pushing for this."



Q

Six months later, just before the state visit, *The Washington Post* reported that the U. S. was considering making good on the executive order. A senior State Department official told me that Xi did not want to be embarrassed by an awkward visit. The Chinese sent over a negotiating team, and diplomats from both countries stayed up all night working out an agreement. During the state visit, Obama and Xi announced that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property" for the purpose of economic espionage. Since then, the Chinese burglaries have slowed dramatically.

his past March, Alperovitch hosted a cyber war game at the Moscone Center in San Francisco. Four teams of ten people—representing the government, the private sector, European and Australian allies, and the hackers—met for two hours to play the game. Shawn Henry; John Carlin; Chris Painter, coordinator for cyber issues at the State Department; and Chris Inglis, the former deputy director of the NSA, were all part of the government team. Executives from JPMorgan Chase and Microsoft represented the private sector. A former member of GCHQ, the British intelligence organization, was on the international team. Frank Cilluffo played a hacker. Ash Carter, the defense secretary, arrived halfway through and asked to play, but the game was already under way, so he was politely turned down.

The game's premise was that ISIS had hacked the databases of several state DMVs and their European counterparts. After a twenty-minute brainstorm, the government team said it was organizing a crisis-response group, speaking to the private sector, and sharing information with the Department of Homeland Security and the FBI. The private team said it was trying to get information from the government. The international team, meanwhile, complained that no one had briefed it—a mistake, Alperovitch said.

The adversary team then stood up and announced, "While the government team is deliberating and talking to the private sector, we're going to kill some people." It was a chilling moment that had real-life echoes for many people in the room. In June 2015, a Kosovar named Ardit Ferizi hacked an online retailer and passed the personal details of more than a thousand U. S. government and military officials to a member of ISIS, who in turn posted them on Twitter. —

he government's reluctance to name the Russians as the authors of the DNC and DCCC hacks made Alperovitch feel that the lessons of the war game—call out your enemy and respond swiftly—had been wasted. He continued to be told by his friends in government that it was politically impossible for the United States to issue an official response to Russia. Some, especially in the State Department, argued that the United States needed Russia's help in Syria and could not afford to ratchet up hostilities. Others said an attribution without a concrete response would be meaningless. Still others insisted that classified security concerns demanded consideration.

Alperovitch was deeply frustrated: He thought the government should tell the world what it knew. There is, of course, an element of the personal in his battle cry. "A lot of people who are born here don't appreciate the freedoms we have, the opportunities we have, because they've never had it any other way," he told me. "I have."

"A lot of people who are born here don't appreciate the freedoms we have."

The government's hesitation was soon overtaken by events. During the first week of October, while Alperovitch was on a rare vacation, in Italy, Russia pulled out of an arms-reduction pact after being accused by the U. S. of bombing indiscriminately in Syria. The same day, the U. S. halted talks with Russia about a Syrian ceasefire. On October 7, two days before the second presidential debate, Alperovitch got a phone call from a senior government official alerting him that a statement identifying Russia as the sponsor of the DNC attack would soon be released. (The statement, from the office of the director of national intelligence and the Department of Homeland Security, appeared later that day.) Once again, Alperovitch was thanked for pushing the government along.

nice that you have the DHS and DNI jointly putting the statement out on a Friday night, but the president coming out and saying, 'Mr. Putin, we know you're doing this, we find it unacceptable, and you have to stop' would be beneficial."

Less than a week later, after WikiLeaks released another cache of hacked emails—this time from John Podesta, Hillary Clinton's campaign chair—the White House announced that the president was considering a "proportional" response against Russia. Administration officials asked Alperovitch to attend a meeting to consider what to do. He was the only native Russian in the room. "You have to let them save face," he told the group. "Escalation will not end well."

MORE FROM ESQUIRE:



These Declassified CIA Maps Are Fantastic

Q