Inside the FBI, Russia, and Ukraine's failed cybercrime investigation

technologyreview.com/2021/07/08/1027999/fbi-russia-ukraine-cybercrime-investigation-ransomware/

Patrick Howell O'Neill

The American cops took the slower, cheaper train from Kyiv to Donetsk.

After repeatedly traveling between Ukraine and the United States, there were more comfortable ways to make this final, 400-mile journey. But the five FBI agents felt like luxury tourists compared to most travelers onboard. They could afford spacious private rooms while locals were sleeping 10 to a cabin. The train moved haltingly, past empty country and villages that, to the Americans at least, looked as if they'd been frozen in the Cold War.

The overnight trek was set to take 12 hours, but it had truly begun two years earlier, in 2008, at the FBI offices in Omaha, Nebraska. That's where the agents had started trying to understand a cybercrime explosion that was targeting Americans and pulling in millions of dollars from victims. At that point, with at least $79 million stolen, it was by far the biggest cybercrime case the FBI had ever seen. Even today, there are few to match its scale.

Bit by bit, the American investigators began to sketch a picture of the culprits. Soon Operation Trident Breach, as they called it, homed in on a highly advanced organized-crime operation that was based in Eastern Europe but had global reach. As evidence came in from around the world, the Bureau and its international partners slowly put names and faces to the gang and started plotting the next step.

As the train made its way across Ukraine, Jim Craig, who was leading his very first case with the FBI, couldn't sleep. He passed the time moving between his cabin and the drinks car, a baroque affair with velvet curtains. Craig stayed awake for the entire trip, staring out the window into the darkness as the country passed by.

For more than a year, Craig had traveled all over Ukraine to build a relationship between the American, Ukrainian, and Russian governments. It had been an unprecedented effort to work together and knock down the rapidly metastasizing cybercrime underworld. US agents exchanged intelligence with their Ukrainian and Russian counterparts, they drank together, and they planned a sweeping international law enforcement action.

That moment of unity is worth remembering today.

It would be a wild understatement to say that in the decade since Craig took that trip to Ukraine, cybercrime has grown dramatically. Last month, Joe Biden and Vladimir Putin made the ransomware crisis—which has struck governments, hospitals, and even a major American oil pipeline—a centerpiece of their first face-to-face summit. Now that critical infrastructure is being hit, the Americans are calling on Moscow to control the criminals within Russia's borders. During that meeting, in response to new pressure from Washington, Putin talked to Biden about doing more to track down cybercriminals.

"Criminal activity rising to the level of international summits shows you the degree to which the threat has grown," says Michael Daniel, the former White House cybersecurity coordinator for Barack Obama. "It also shows that the current international situation is not at equilibrium. It's not sustainable."

Days later, the head of Russia's FSB intelligence agency said the country would work with the United States to find and prosecute cybercriminals. Inside the White House, top American officials are figuring out what to do next. Some are deeply skeptical and think that Moscow would rather turn requests for help on cybercrime into recruiting opportunities than aid an American investigation.

To begin to understand why they are so concerned, we have to go back to the investigation that put Jim Craig on that train in Ukraine in 2010, and to the case that had him meeting Russian agents and planning raids in Moscow and other cities across multiple countries.

The operation was a unique chance to disrupt one of the world's most successful cybercrime gangs. It was an opportunity to put away some of the most important operators in the vast underground hacking economy operating in Russia and Ukraine. It was so important, in fact, that the agents began referring to September 29, 2010—the day of planned coordinated police raids in Ukraine, Russia, the United Kingdom, and the United States—as D-Day.

That was also the day when things went sideways.

Larger than life

Operation Trident Breach had dozens of targets worldwide. Three men were at the top of the list.

First was Evgeniy Bogachev, a prolific hacker known as “Slavik.” A Russian with a contradictory taste for anonymity and outrageous luxury, he wrote a piece of malware called Zeus. It infected computers with the goal of silently opening the door to people’s bank accounts. And it was a hit: simple, stealthy, effective, regularly updated, able to compromise all sorts of targets, and flexible enough to fit into any kind of cybercrime operation.

The investigation detailed how Bogachev had used Zeus to build an opaque cybercriminal empire with the kind of precision and ambition that felt more characteristic of a multinational corporation.

Second on Trident Breach’s list was one of Bogachev’s most important customers, Vyacheslav Penchukov. A Ukrainian known online as “Tank,” he ran his own criminal hacking crew using the Zeus malware, purchasing it from Bogachev for thousands of dollars per copy and raking in millions in profit. He’d assembled a crew that used a particularly tasty flavor of the program that integrated with the instant messaging software Jabber. It gave the hackers instant updates on their efforts: when an infection occurred, clients got a message and then moved the money as desired—as easy as that.

Related Story

Recovering from the SolarWinds hack could take 18 months

The head of the agency leading US efforts to fix a Russian hacking attack says rebuilding will take a very long time.

The third target was Maksim Yakubets, a Russian known as “Aqua,” who orchestrated a massive laundering operation. Using thousands of accomplices and front companies, he moved money stolen from hacked bank accounts back to Eastern Europe.

Tank’s crew ran out of Donetsk, a city of nearly a million people in southeast Ukraine. They would use Zeus to drain bank accounts and send the money to mules in the target countries, including the United States—who would then wire the proceeds to Ukraine.

The rise of this kind of professional operation, combining the nimble smarts of tech startups and the callousness of organized crime, might seem to have been inevitable. Today, the ransomware business makes headlines daily, and its hacker entrepreneurs rely on a whole sub-industry of white-glove criminal services. But in the mid-2000s, organizations like this were extremely unusual: the Zeus crew was a pioneer.

Tank was so closely involved in directing the inner workings of the scheme that for a time, the FBI thought he was in charge. It eventually became clear, however, that Tank was Slavik’s VIP customer—and apparently the only one who talked personally to Bogachev

himself.

Tank “would always be the first person to receive alerts,” says Jason Passwaters, a former FBI contractor who worked for years in both the US and Europe on the case. “Somebody would get popped, and it would be a particularly juicy one. He’d be the first to go into the bank account, say ‘We’ve got a good one,’ and then he’d pass it along to others to do the more manual work.”

Tank was no enigma to the feds. He had a family that was growing increasingly used to wealth and a very public side hustle as “DJ Slava Rich,” playing sweaty midnight raves drenched in neon lights. The agents hoped that the confidence to live so large would be his downfall.

Vodka diplomacy

To catch Tank, the FBI needed to expand its reach. The criminal operation they were targeting spanned the globe: there were victims and money mules in the United States and Europe, and the attacks were directed by kingpins and hackers across Ukraine and Russia. The FBI needed help from their counterparts in those two countries.

Securing those partnerships wasn’t easy. When Craig arrived in Kyiv, he was told that Russian FSB agents hadn’t set foot inside Ukraine since the Orange Revolution of 2004, when anticorruption protests reversed the country’s fraudulent presidential election results. But now he needed everyone in the same room.

Their inaugural in-person meeting took place at the boutique Opera Hotel in Kyiv. The conversations were tentative, mutual trust was low, and expectations were even lower. To Craig’s surprise, though, the four Russian agents who came were friendly and encouraging. They said they wanted to exchange information on hackers of interest and even offered to bring FBI agents into Russia to get a closer look at suspects.

The Americans explained that the driving engine of their investigation was a Jabber chat server they had located and started watching in 2009. It gave them a peek into the Zeus crew’s communications; details about operations and business deals appeared next to personal chatter about toys and expensive vacations that the crew had bought with the proceeds of their crimes.

> Passwaters saw a message he'd never forget. Another hacker had written to Tank: "You guys are fucked. The FBI is watching. I've seen the logs."

Passwaters—now a cofounder and executive at the American cybersecurity firm Intel 471, where Craig also works—says it was practically a full-time job to review the chat logs and share the information with the FSB and the SBU, Ukraine’s chief security and intelligence service.

In April 2010, as he was sifting through the data, Passwaters saw a message he'd never forget. Another hacker had written to Tank: "You guys are fucked. The FBI is watching. I've seen the logs."

Passwaters knew the logs in question were the ones he was reading at that exact moment—and that their existence was known only to a handful of agents. Somehow, they had been leaked. The agents suspected Ukrainian corruption.

"What was obvious was that someone within the unit privy to key details of the case had passed information on to the very cybercriminals that were being investigated," says one former SBU officer, who spoke to MIT Technology Review on the condition of anonymity. "Even the terminology used in their conversation was uncommon for cybercriminals and appeared to have come straight from a case file."

Tank's initial reaction was fear, especially at the possibility of being sent to the United States. But Passwaters remembers that the person who tipped Tank off then tried to calm him in another message: "This is the life we chose. Live by the sword, die by the sword."

Tank's next reaction was strange. Instead of immediately burning the server and moving operations elsewhere, as the FBI expected, he and his crew changed their nicknames but continued to use the compromised system for another month. Eventually, the server went dark. But by then, the investigation seemed to have gained unstoppable momentum.

> "This is the life we chose. Live by the sword, die by the sword."

In June 2010, about 20 officers from multiple countries met in the woods outside Kyiv at an outrageously opulent residence owned by SBU director Valeriy Khoroshkovsky. The house was often used by the agency to entertain its most important visitors. Everyone gathered in a lavish conference room to plan the particulars of D-Day. They discussed the suspects in detail, went over the roles each agency would play, and traded information about the operation's targets.

After a day of planning, the drinks started to flow. The group sat down to a multicourse dinner served with wine and vodka. No matter how much they drank, their glasses stayed full. Each person was obligated to give a toast during the marathon event. After the festivities, the SBU officers took their counterparts on a tour of the city. The Americans don't remember much about what they saw.

The next morning, despite the vodka ringing in their ears, the overall plan was clear enough. On September 29, police from five countries—the US, the UK, Ukraine, Russia, and the Netherlands—would simultaneously arrest dozens of suspects in an operation that promised to outshine all cybercrime investigations before it.

Headaches

The air was dark and malignant when Agent Craig and his team arrived in Donetsk on the train. Nearby, coal plants were burning, identifiable by the mark their smoke left on the sky. As the agents drove to the upscale Donbass Palace Hotel, Craig thought of the Russian border, just an hour away.

His mind turned to the Jabber Zeus victims he had met back in America. A woman in Illinois had her bank account drained while her husband was on life support; a small business in Seattle had lost all its money and shut its doors; a Catholic diocese in Chicago got hit, and a bank account operated by nuns was emptied. No one was spared.

When they arrived at their hotel, there was no time to rest. The Americans waited for the SBU—which was now in charge, since the operation was taking place in its own backyard—to give the green light.

But nothing happened. The Ukrainians pushed the date back again and again. The Americans started to wonder what was causing the delays. Was it the kind of dysfunction that can strike any complex law enforcement investigation, or was it something more worrying?

“We were supposed to be down there for two days,” says Craig. “We were down there for weeks. They kept delaying, delaying, delaying.”

The SBU said agents were trailing Tank around the city, watching closely as he moved between nightclubs and his apartment. Then, in early October, the Ukrainian surveillance team said they’d lost him.

The Americans were unhappy, and a little surprised. But they were also resigned to what they saw as the realities of working in Ukraine. The country had a notorious corruption problem. The running joke was that it was easy to find the SBU’s anticorruption unit—just look for the parking lot full of BMWs.

Although Tank was no longer in their sights, the Ukrainians were still tracking five of his lieutenants. The local police seemed ready to change gears. The SBU suddenly gave the green light, and the raids began.

Knock knock

It was the dead of night when Craig’s team made its first stop at the apartment of Ivan Klepikov, known as “petr0vich.” He was the crew’s systems administrator, handling technical duties behind the scenes—mundane but critical work that kept the criminal operation running.

The SBU’s heavily armed SWAT team breached Klepikov’s door but kept the unarmed Americans waiting outside the apartment. When Craig finally got inside, Klepikov was sitting comfortably in the living room in his underwear and a smoking jacket. The Ukrainians asked

Craig to introduce himself. The implied threat was that the cops might send Klepikov to the United States, which has much harsher criminal sentencing laws than most of the world. But the Ukrainian constitution forbids extradition of citizens. Klepikov's wife, meanwhile, held their baby in the kitchen and laughed as she spoke with other officers on the raid. Klepikov was taken into custody by police.

Next, the operation moved on to Tank's apartment. The same pattern took place: SBU officers went inside first, while the FBI agents waited outside. Once Craig was allowed in, Tank was missing and the apartment looked unnaturally clean—as though a maid had just been through, he thought. "It was quite obvious no one had been there for a few days," Craig says.

Related Story

How China turned a prize-winning iPhone hack against the Uyghurs

An attack that targeted Apple devices was used to spy on China's Muslim minority—and US officials claim it was developed at the country's top hacking competition.

He thought back to reports from just a few hours earlier, when the Ukrainian surveillance team said they were tracking Tank and had intelligence that the suspect had been at home recently. None of it seemed believable.

Five individuals were detained in Ukraine on that night, but when it came to Tank, who police alleged was in charge of the operation, they left empty-handed. And none of the five people arrested in Ukraine stayed in custody for long.

Somehow, the operation in Ukraine—a two-year international effort to catch the biggest cybercriminals on the FBI's radar—had gone sideways. Tank had slipped away while under SBU surveillance, while the other major players deftly avoided serious consequences for their crimes. Craig and his team were livid.

But if the situation in Ukraine was frustrating, things were even worse in Russia, where the FBI had no one on the ground. Trust between the Americans and Russians had never been very strong. Early in the investigation, the Russians had waved the FBI off Slavik's identity.

"They try to push you off target," Craig says. "But we play those games knowing what's going to happen. We're very loose with what we send them anyway, and even if you know something, you try to push it to them to see if they'll cooperate. And when they don't—oh, no surprise."

> A maddening mixture of corruption, rivalry, and stonewalling had left Operation Trident Breach without its top targets.

Even so, while the raids happened in Donetsk, the Americans hoped they would get a call from Russia about an FSB raid on the residence of Aqua, the money launderer Maksim Yakubets. Instead, there was silence.

The operation had its successes—dozens of lower-level operators were arrested across Ukraine, the United States, and the United Kingdom, including some of Tank's personal friends who helped move stolen money out of England. But a maddening mixture of corruption, rivalry, and stonewalling had left Operation Trident Breach without its top targets.

"It came down to D-Day, and we got ghosted," Craig says. "The SBU tried to communicate with [the Russians]. The FBI was making phone calls to the embassy in Moscow. It was complete silence. We ended up doing the operation anyway, without the FSB. It was months of silence. Nothing."

Well-connected criminals

Not everyone in the SBU drives a BMW.

After the raids, some Ukrainian officials, who were unhappy with the corruption and leaks happening within the country's security services, concluded that the 2010 Donetsk raid against Tank and the Jabber Zeus crew failed because of a tip from a corrupt SBU officer named Alexander Khodakovsky.

At the time, Khodakovsky was the chief of an SBU SWAT unit in Donetsk known as Alpha team. It was the same group that led the raids for Trident Breach. He also helped coordinate law enforcement across the region, which allowed him to tell suspects in advance to prepare for searches or destroy evidence, according to the former SBU officer who spoke to MIT Technology Review anonymously.

When Russia and Ukraine went to war in 2014, Khodakovsky defected. He became a leader in the self-proclaimed Donetsk People's Republic, which NATO says receives financial and military aid from Moscow.

The problem wasn't just one corrupt officer, though. The Ukrainian investigation into—and legal proceedings against—Tank and his crew continued after the raids. But they were carefully handled to make sure he stayed free, the former SBU officer explains.

"Through his corrupt links among SBU management, Tank arranged that all further legal proceedings against him were conducted by the SBU Donetsk field office instead of SBU HQ in Kyiv, and eventually managed to have the case discontinued there," the former officer says. The SBU, FBI, and FSB did not respond to requests for comment.

> "It came down to D-Day, and we got ghosted."
>
> *Jim Craig*

Tank, it emerged, was deeply entangled with Ukrainian officials linked to Russia's government—including Ukraine's former president Viktor Yanukovych, who was ousted in 2014.

Yanukovych's youngest son, Viktor Jr., was the godfather to Tank's daughter. Yanukovych Jr. died in 2015 when his Volkswagen minivan fell through the ice on a lake in Russia, and his father remains in exile there after being convicted of treason by a Ukrainian court.

When Yanukovych fled east, Tank moved west to Kyiv, where he is believed to represent some of the former president's interests, along with his own business ventures.

"Through this association with the president's family, Tank managed to develop corrupt links into the top tiers of Ukrainian government, including law enforcement," the SBU officer explains.

Ever since Yanukovych was deposed, Ukraine's new leadership has turned more decisively toward the West.

"The reality is corruption is a major challenge to stopping cybercrime, and it can go up pretty high," Passwaters says. "But after more than 10 years working with Ukrainians to combat cybercrime, I can say there are plenty of really good people in the trenches silently working on the right side of this fight. They are key."

Warmer relations with Washington were a major catalyst for the ongoing war in eastern Ukraine. Now, as Kyiv tries to join NATO, one of the conditions of membership is eliminating corruption. The country has lately cooperated with Americans on cybercrime investigations to a degree that would have been unimaginable in 2010. But corruption is still widespread.

"Ukraine overall is more active in combating cybercrime in recent years," says the former SBU officer. "But only when we see criminals really getting punished would I say that the situation has changed at its root. Now, very often we see public relations stunts that do not result in cybercriminals' ceasing their activities. Announcing some takedowns, conducting some searches, but then releasing everyone involved and letting them continue operating is not a proper way of tackling cybercrime."

And Tank's links to power have not gone away. Enmeshed with the powerful Yanukovych family, which is itself closely aligned with Russia, he remains free.

A looming threat

On June 23, FSB chief Alexander Bortnikov was quoted as saying his agency would work with the Americans to track down criminal hackers. It didn't take long for two particular Russian names to come up.

Even after the 2010 raids took down a big chunk of his business, Bogachev continued to be a prominent cybercrime entrepreneur. He put together a new crime ring called the Business Club; it soon grew into a behemoth, stealing more than $100 million that was divided among its members. The group moved from hacking bank accounts to deploying some of the first modern ransomware, with a tool called CryptoLocker, by 2013. Once again, Bogachev was at the center of the evolution of a new kind of cybercrime.

Around the same time, researchers from the Dutch cybersecurity firm Fox-IT who were looking closely at Bogachev's malware saw that it was not just attacking targets at random. The malware was also quietly looking for information on military services, intelligence agencies, and police in countries including Georgia, Turkey, Syria, and Ukraine—close neighbors and geopolitical rivals to Russia. It became clear that he wasn't just working from inside Russia, but his malware actually hunted for intelligence on Moscow's behalf.

Related Story

The $1 billion Russian cyber company that the US says hacks for Moscow

Washington has sanctioned Russian cybersecurity firm Positive Technologies. US intelligence reports claim it provides hacking tools and runs operations for the Kremlin.

The exact details of Bogachev's relationship with Russian intelligence agencies is unknown, but experts say it looks as if those authorities used his worldwide network of more than 1 million hacked computers as a powerful spying tool.

Today, the FBI offers a $3 million reward for information leading to Bogachev's arrest. It's a small fraction of the total amount he's stolen, but the second-highest reward for a hacker ever. He remains free.

Weeks after the Russians went silent during the Donetsk raids, a search warrant was belatedly executed in Moscow on Maksim Yakubets. The Russians shared only a fraction of the information the Americans asked for, Craig says. So in 2019, the FBI offered a $5 million reward for Yakubets' arrest, officially topping the bounty on Bogachev as the Americans' biggest reward for a hacker.

Even with such a price tag on his head, Yakubets has remained free and even expanded his operations. He's now wanted for running his own cybercrime empire—a group he branded Evil Corp. According to a 2019 indictment, it is responsible for at least $100 million in theft. In the two years since, that number has grown: today, the syndicate is one of the world's top ransomware gangs.

And, like Bogachev, Yakubets seems to be doing more than just profit-seeking. According to the US Treasury Department, which has imposed sanctions on Evil Corp, he had begun working for the Russian FSB by 2017. "To bolster its malicious cyber operations, the FSB cultivates and co-opts criminal hackers," the 2019 sanctions announcement said, "enabling them to engage in disruptive ransomware attacks and phishing campaigns."

Given this—and the history of Trident Breach—Washington officials were deeply skeptical when Bortnikov offered the FSB's assistance. Few in the US government believe what Moscow says, and vice versa. But still, there is some hope in Washington that the calculus driving the Kremlin's decisions is changing.

Related Story

Could the ransomware crisis force action against Russia?

Moscow's blind eye toward cybercriminals has made escalating attacks inevitable, say experts. But changing the approach is easier said than done.

"We feel like we have emerged from this trip with a common strategy with our allies," said US national security advisor Jake Sullivan in a press conference following the Biden-Putin summit, "As well as having laid down some clear markers with Russia, some clear expectations, and also communicated to them the capacities that we have should they choose not to take action against criminals who are attacking our critical infrastructure from Russian soil."

Translation: The White House is applying pressure on the Kremlin as never before. But how much does that change the math for Moscow? From President Biden down, the Americans have never devoted as much energy, money, and staff resources to fighting hacking as they are doing today. Now the Americans are wondering if they could actually see the FSB make arrests.

A sacrificial lamb or two from the Russians is one thing, but what would it take to actually solve the problem of cybercrime? What will Washington do to follow through, and how much pain is Moscow willing to endure?

"There have been some tactical wins over the years, but to this day I still see some of the same folks pop up again and again," Passwaters says. "We call them the 'old wolves' of cybercrime. I personally think that if Tank, Aqua, and Slavik had been nabbed in 2010, things would look quite a bit different today. But the reality is cybercrime will continue to be a massive problem until it is accepted as the serious national security threat that it is."