

Forum:[Hack Forums](#)

Thread: [{Hacks, Scams, and Exploits} - #5 - Zeus - The God Of Banking Malware](#)

Pr0m3th3us - July 19, 2026, 7:39 am

Preface

Lets be real here....online banking changed everything for most of us. Before it existed, robbing a bank meant walking in with a firearm, demanding cash, and hoping you made it out before the cops showed up. After it existed, for some of us all you needed was a computer, some patience, and the right piece of code. No firearm, no getaway car, no witnesses. The money just moved. This is the story of a young Russian coder who figured that out before almost anyone else, built a tool so effective it was eventually described by the FBI as the most sophisticated botnet they had ever attempted to disrupt, and who to this day has never been arrested, never faced trial, and is presumably still living comfortably on the Black Sea coast of Russia with a \$3 million bounty on his head. Fucking brilliant.

The Hacks

This wild story starts in 2006 with a piece of malware nobody recognized. A user on the tech support forum techsupportguy.com posted a sample of strange code they'd found on a family member's computer, and security researchers who picked it up couldn't identify it. They named it WSNPoem after a directory string found in the code. What it did was straightforward but effective, it crawled silently through infected machines, hunted for stored usernames and passwords, and reported everything back to whoever deployed it, with a particular appetite for online banking credentials. Nobody knew who wrote it. A Russian group called UpLevel was rumored to be behind it, but that was speculation. What became clear over the following months, as updated versions emerged under new names, first PRG, then Zbot...was that a single author was driving this, constantly iterating, constantly improving. That author was a twenty-two-year-old Russian coder operating under the handle Slavik. The creator and main developer of the original Zeus was Evgeniy Bogachev, also known as "lucky12345" and "slavik."

By 2008 the malware had a name Slavik himself had given it...Zeus. The name wasn't accidental, Zeus is the king of the Greek gods, ruler of Mount Olympus, and Slavik wanted a single botnet that ruled them all. What separated Zeus from the banking malware that had come before it was the business model wrapped around it. Slavik wasn't just using it to rob people himself, he was selling it as a crimeware kit on underground forums, a DIY banking Trojan package complete with a builder tool that let buyers configure their own botnet without needing serious technical skills. By spring 2009 it was estimated that around 5,000 different customers had purchased copies of Zeus. He was charging around \$3,000 per copy for the base kit, with premium modules on top, a form-grabber for Firefox at \$2,000, a backconnect module at \$1,500 that routed all traced transactions back to the victim's own machine, and the Jabber chat notifier at \$500 which would fire an instant message to the operator the moment an infected machine logged into a bank account with a significant balance, delivering live credentials and two-factor authentication codes in real time. The top-tier virtual networking module cost \$10,000 and gave operators full remote control of the infected machine, letting them tunnel all their traffic through the victim's own internet connection so the bank saw a login from the customer's home, not from Russia.

The people deploying Zeus ranged from lone fraudsters to organized phishing groups. Two of the

biggest were Rock Phish, who had been running sophisticated bank-impersonation phishing campaigns since 2005, and their successors Avalanche, who adopted Zeus and layered it on top of their existing phishing infrastructure, hitting victims with a double threat, a fake login page to capture credentials if they clicked, and Zeus silently waiting in the background to capture credentials if they didn't. Slavik himself ran a tighter inner circle he called the Business Club, a hand-selected team of six specialists covering tech support, malware development, and money mule recruitment. Money mules were the critical human layer of the operation, ordinary people recruited through fake job postings on sites like Craigslist, told they were doing clerical work, and asked to receive transfers and forward them onward while keeping a small percentage. Most had no idea they were laundering stolen funds. Many ended up prosecuted for it anyway. One documented case from June 2009 showed how precisely the crew operated, they targeted the county treasurer of Bullitt County, Kentucky, infected her machine with JabberZeus, obtained her banking credentials and email login, used the backconnect module to make their activity appear to originate from her own computer, reset the judge's credentials through the treasurer's access, and in under ten minutes created twenty-five fake payroll employees and transferred \$415,000 out of the court's account to waiting money mules across the country.

Slavik's real identity remained unknown to investigators for years. The FBI first indicted him in August 2012 under the alias lucky12345, charging him with conspiracy to participate in racketeering activity, bank fraud, conspiracy to violate the Computer Fraud and Abuse Act, conspiracy to violate the Identity Theft and Assumption Deterrence Act, and aggravated identity theft. They didn't know his real name yet, the breakthrough came later. Bogachev was identified as the head of the GameOver Zeus network by cross-referencing the IP address used to access his email, which had been provided by a tipster, with the IP used to administer the botnet, although he had used a VPN to obscure his activity. On May 19, 2014, Bogachev was indicted in his true name by a federal grand jury in the Western District of Pennsylvania on charges of conspiracy, computer fraud, wire fraud, bank fraud, and money laundering. His real name was Evgeniy Mikhailovich Bogachev, thirty years old, residing in Anapa, Russia, on the northern coast of the Black Sea. The SpyEye crew, who had tried to compete with and ultimately absorb Zeus, also went down around this time, security researchers have variously attributed the Zeus source code leak to Bogachev or Aleksandr Panin, the creator of SpyEye. Panin, hacker handle "Gribodemon" was arrested on holiday in the Dominican Republic, extradited to the US, and sentenced to nine years. His SpyEye co-operator Hamza Bendelladj, a 27 year old Algerian, received fifteen years. Bogachev himself has never been arrested. He remains on the FBI's Cyber Most Wanted list with a \$3 million reward, at the time of its issuance, the largest reward ever offered for a cybercriminal in history.

Impact

The scale of damage Zeus caused across its entire lifespan is difficult to fully quantify because the malware was sold to thousands of different operators who carried out their own independent campaigns. What the FBI was able to document is significant enough on its own. GameOver Zeus is believed responsible for more than one million computer infections, resulting in financial losses of more than \$100 million from businesses and consumers in the US and worldwide, with the scheme causing more than \$100 million in damages. The ransomware layer added further damage, an additional \$27 million extracted through CryptoLocker infections delivered through the same botnet infrastructure. Individual victims ranged from ordinary people who lost their savings to organizations with no obvious security profile, A Kentucky court, a Catholic religious order, schools, small businesses, and a Massachusetts police department that paid \$750 in ransom just to get their own systems back.

The broader financial sector bore enormous collateral damage. Banks spent heavily on upgraded authentication systems, fraud detection, and customer remediation as Zeus attacks scaled up. The "man-in-the-browser" technique Zeus pioneered was particularly damaging because it bypassed almost every conventional security measure, even customers who did everything right, used strong

passwords, logged in from home on their own computer, were still vulnerable if Zeus was already on that machine. For the money mule layer of the operation, the human cost was real, interviews with former money mules allowed the FBI to begin to understand GameOver Zeus's botnet infrastructure, meaning ordinary people who thought they were doing data entry jobs ended up being both victims and inadvertent witnesses in one of the largest cybercrime prosecutions in US history.

What Changed

The takedown operation, codenamed "Operation Tovar" was a landmark event in how law enforcement approached large-scale botnet disruption. Operation Tovar began on May 30 and was completed within four to five hours. The operation was a sinkholing attack that cut off communication between the bots and their command servers, redirecting the communication towards government-controlled servers. Law enforcement in Canada, France, Germany, Luxembourg, the Netherlands, Ukraine, and the United Kingdom began seizing key GameOver Zeus servers simultaneously. The private sector involvement was equally unprecedented. Microsoft, Dell SecureWorks, CrowdStrike, Symantec, McAfee, F-Secure, and a dozen other organizations coordinated with the FBI in real time. The FBI described GameOver Zeus as the most sophisticated botnet they and their allies had ever attempted to disrupt, and the operation represented the largest fusion of law enforcement and industry partnership ever undertaken in support of an FBI cyber operation.

The legal framework around cybercrime was also significantly shaped by the Zeus prosecutions. The charges brought against Bogachev included racketeering, computer fraud, wire fraud, bank fraud, money laundering, aggravated identity theft. They established a template for prosecuting malware authors not just as hackers but as organized crime operators, which carried dramatically heavier sentencing exposure. The money mule prosecutions that ran alongside Zeus cases contributed to a broader law enforcement push to treat mule recruitment networks as criminal enterprises rather than isolated incidents. On the defensive side, Zeus accelerated the industry-wide adoption of behavioral analytics in banking fraud detection, systems that analyze not just what credentials a user provides but how they type, what device they use, where they are, and whether their behavior matches historical patterns. The man-in-the-browser attack surface Zeus exploited pushed banks toward out-of-band transaction verification, confirming transfers through a separate channel like SMS or a dedicated app rather than within the same browser session the malware could intercept. Less than two months after Operation Tovar was executed, a new strain of GameOver Zeus was discovered, named newGOZ, which lacked peer-to-peer capabilities but otherwise shared ninety percent of its codebase with the original, a reminder that taking down the infrastructure doesn't erase the code and as long as Bogachev remains free in Russia, the story isn't really over.

Sources

Darknet Diaries Ep. 111 — Zeus: <https://darknetdiaries.com/episode/111/>

Darknet Diaries Ep. 111 Transcript: <https://darknetdiaries.com/transcript/111/>

FBI Most Wanted — Evgeniy Mikhailovich Bogachev:

<https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev>

DOJ Press Release — Operation Tovar / Gameover Zeus Disruption (2014):

<https://www.justice.gov/archives/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware>

DOJ Press Release — \$3 Million Reward for Bogachev:

<https://www.justice.gov/usao-wdpa/pr/reward-announced-cyber-fugitive>

Wikipedia — Gameover Zeus: https://en.wikipedia.org/wiki/Gameover_Zeus

IBTimes — GameOver Zeus Disrupted:

<https://www.ibtimes.com/gameover-zeus-disrupted-evgeniy-mikhailovich-bogachev-put-fbis-cybers->

[most-wanted-list-1593947](#)

Bitdefender — FBI's Most Wanted Cybercriminal \$3M for lucky12345:

<https://www.bitdefender.com/en-us/blog/hotforsecurity/fbis-most-wanted-cybercriminal-3-million-for-lucky12345>

Newsweek — FBI Issues \$3 Million Bounty for Russian Hacker:

<https://www.newsweek.com/fbi-issues-3-million-bounty-russian-hacker-309288>

TIME — Evgeniy Mikhailovich Bogachev \$3 Million Reward:

<https://time.com/3721250/russian-hacker-bogachev/>

AfterDawn — US Identifies Russian Linked to CryptoLocker and GameOver Zeus:

https://www.afterdawn.com/news/article.cfm/2014/06/02/fbi-evgeniy_bogachev-wanted-zeus-cryptolocker

Full disclosure: I used Claude to help me locate sources to go over, I read the articles, I listened and re-listened to "Darknet Diaries" podcast while doing this write-up, as he was an inspiration. I used Claude to go over my write-up for grammar errors, punctuation (im really bad about using apostrophes), and cleaning up the overall writing but keeping my writing style instead of changing it so much i couldn't recognize it. I also told it to point out if i made errors in reporting in my write up. ChatGPT was used for the Image.