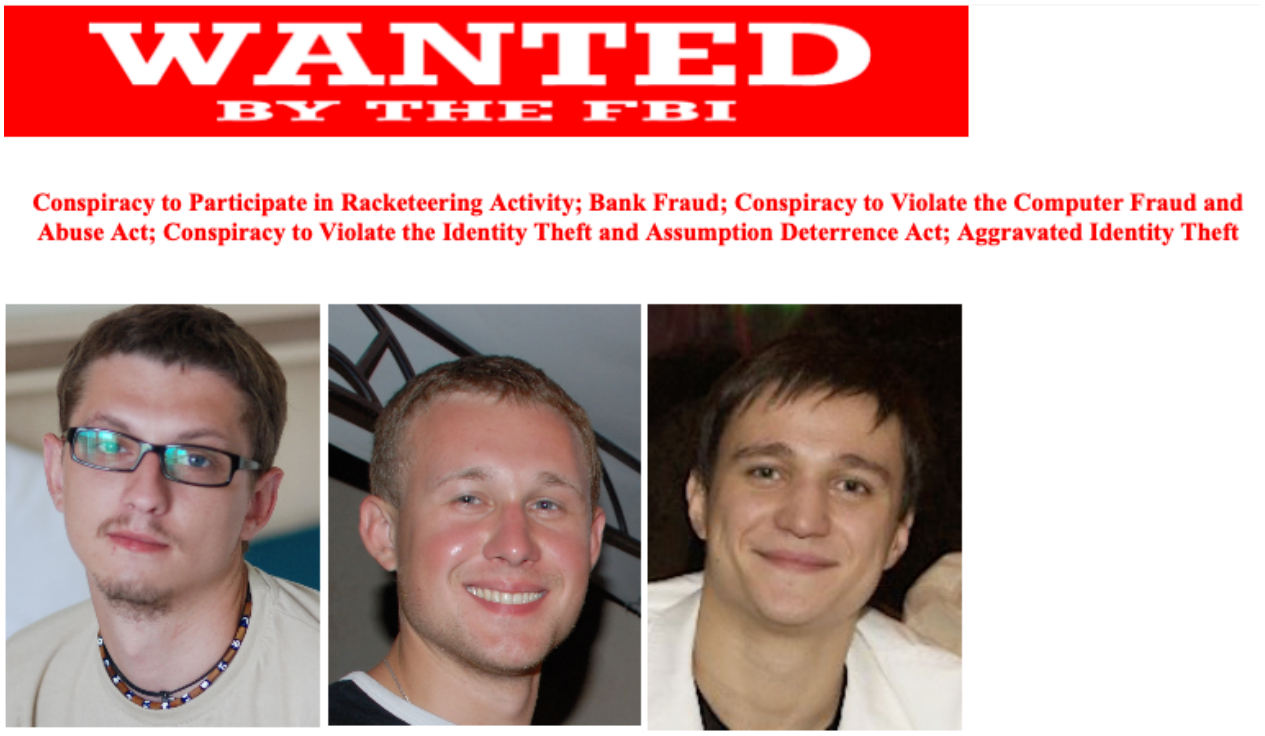
Top Zeus Botnet Suspect “Tank” Arrested in Geneva

krebsonsecurity.com/2022/11/top-zeus-botnet-suspect-tank-arrested-in-geneva/

Vyacheslav “Tank” Penchukov, the accused 40-year-old Ukrainian leader of a prolific cybercriminal group that stole tens of millions of dollars from small to mid-sized businesses in the United States and Europe, has been arrested in Switzerland, according to multiple sources.



Wanted Ukrainian cybercrime suspect Vyacheslav “Tank” Penchukov (right) was arrested in Geneva, Switzerland. Tank was the day-to-day manager of a cybercriminal group that stole tens of millions of dollars from small to mid-sized businesses.

Penchukov was named in a 2014 indictment by the **U.S. Department of Justice** as a top figure in the **JabberZeus Crew**, a small but potent cybercriminal collective from Ukraine and Russia that attacked victim companies with a powerful, custom-made version of the **Zeus** banking trojan.

The **U.S. Federal Bureau of Investigation** (FBI) declined to comment for this story. But according to multiple sources, Penchukov was arrested in Geneva, Switzerland roughly three weeks ago as he was traveling to meet up with his wife there.

Penchukov is from Donetsk, a traditionally Russia-leaning region in Eastern Ukraine that was recently annexed by Russia. In his hometown, Penchukov was a well-known deejay ("DJ Slava Rich") who enjoyed being seen riding around in his high-end BMWs and Porsches. More recently, Penchukov has been investing quite a bit in local businesses.

The JabberZeus crew's name is derived from the malware they used, which was configured to send them a Jabber instant message each time a new victim entered a one-time password code into a phishing page mimicking their bank. The JabberZeus gang targeted mostly small to mid-sized businesses, and they were an early pioneer of so-called "man-in-the-browser" attacks, malware that can silently siphon any data that victims submit via a web-based form.

Once inside a victim company's bank accounts, the crooks would modify the firm's payroll to add dozens of "**money mules**," people recruited through work-at-home schemes to handle bank transfers. The mules in turn would forward any stolen payroll deposits — minus their commissions — via wire transfer overseas.

Tank, a.k.a. "DJ Slava Rich," seen here performing as a DJ in Ukraine in an undated photo from social media.

The JabberZeus malware was custom-made for the crime group by the alleged author of the Zeus trojan — **Evgeniy Mikhailovich Bogachev**, a top Russian cybercriminal with a $3 million bounty on his head from the FBI. Bogachev is accused of running the Gameover Zeus botnet, a massive crime machine of 500,000 to 1 million infected PCs that was used for large DDoS attacks and for spreading Cryptolocker — a peer-to-peer ransomware threat that was years ahead of its time.

Investigators knew Bogachev and JabberZeus were linked because for many years they were reading the private Jabber chats between and among members of the JabberZeus crew, and Bogachev's monitored aliases were in semi-regular contact with the group about updates to the malware.

Gary Warner, director of research in computer forensics at the University of Alabama at Birmingham, noted in his blog from 2014 that Tank told co-conspirators in a JabberZeus chat on July 22, 2009 that his daughter, **Miloslava**, had been born and gave her birth weight.

"A search of Ukrainian birth records only showed one girl named Miloslava with that birth weight born on that day," Warner wrote. This was enough to positively identify Tank as Penchukov, Warner said.

Ultimately, Penchukov's political connections helped him evade prosecution by Ukrainian cybercrime investigators for many years. The late son of former Ukrainian President **Victor Yanukovych** (Victor Yanukovych Jr.) would serve as godfather to Tank's daughter Miloslava. Through his connections to the Yanukovych family, Tank was able to establish contact with key insiders in top tiers of the Ukrainian government, including law enforcement.

Sources briefed on the investigation into Penchukov said that in 2010 — at a time when the Security Service of Ukraine (SBU) was preparing to serve search warrants on Tank and his crew — Tank received a tip that the SBU was coming to raid his home. That warning gave Tank ample time to destroy important evidence against the group, and to avoid being home when the raids happened. Those sources also said Tank used his contacts to have the investigation into his crew moved to a different unit that was headed by his corrupt SBU contact.

Writing for *Technology Review*, **Patrick Howell O'Neil** recounted how SBU agents in 2010 were trailing Tank around the city, watching closely as he moved between nightclubs and his apartment.

"In early October, the Ukrainian surveillance team said they'd lost him," he wrote. "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."

AUTHOR'S NOTE/BACKGROUND

I first encountered Tank and the JabberZeus crew roughly 14 years ago as a reporter for *The Washington Post*, after a trusted source confided that he'd secretly gained access to the group's private Jabber conversations.

From reading those discussions each day, it became clear Tank was nominally in charge of the Ukrainian crew, and that he spent much of his time overseeing the activities of the money mule recruiters — which were an integral part of their victim cashout scheme.

It was soon discovered that the phony corporate websites the money mule recruiters used to manage new hires had a security weakness that allowed anyone who signed up at the portal to view messages for every other user. A scraping tool was built to harvest these money mule recruitment messages, and at the height of the JabberZeus gang's activity in 2010 that scraper was monitoring messages on close to a dozen different money mule recruitment sites, each managing hundreds of "employees."

Each mule was given busy work or menial tasks for a few days or weeks prior to being asked to handle money transfers. I believe this was an effort to weed out unreliable money mules. After all, those who showed up late for work tended to cost the crooks a lot of money, as the victim's bank would usually try to reverse any transfers that hadn't already been withdrawn by the mules.

When it came time to transfer stolen funds, the recruiters would send a message through the fake company website saying something like: "Good morning [mule name here]. Our client — XYZ Corp. — is sending you some money today. Please visit your bank now and withdraw this payment in cash, and then wire the funds in equal payments — minus your commission — to these three individuals in Eastern Europe."

Only, in every case the company mentioned as the "client" was in fact a small business whose payroll accounts they'd already hacked into.

So, each day for several years my morning routine went as follows: Make a pot of coffee; shuffle over to the computer and view the messages Tank and his co-conspirators had sent to their money mules over the previous 12-24 hours; look up the victim company names in Google; pick up the phone to warn each that they were in the process of being robbed by the Russian Cyber Mob.

My spiel on all of these calls was more or less the same: "You probably have no idea who I am, but here's all my contact info and what I do. Your payroll accounts have been hacked, and you're about to lose a great deal of money. You should contact your bank immediately and have them put a hold on any pending transfers before it's too late. Feel free to call me back afterwards if you want more information about how I know all this, but for now please just call or visit your bank."

In many instances, my call would come in just minutes or hours before an unauthorized payroll batch was processed by the victim company's bank, and some of those notifications prevented what otherwise would have been enormous losses — often several times the amount of the organization's normal weekly payroll. At some point I stopped counting how many tens of thousands of dollars those calls saved victims, but over several years it was probably in the millions.

Just as often, the victim company would suspect that I was somehow involved in the robbery, and soon after alerting them I would receive a call from an FBI agent or from a police officer in the victim's hometown. Those were always interesting conversations.

Collectively, these notifications to victims led to dozens of stories over several years about small businesses battling their financial institutions to recover their losses. I never wrote about a single victim that wasn't okay with my calling attention to their plight and to the sophistication of the threat facing other companies.

This incessant meddling on my part very much aggravated Tank, who on more than one occasion expressed mystification as to how I knew so much about their operations and victims. Here's a snippet from one of their Jabber chats in 2009, after I'd written a story for The Washington Post about their efforts to steal $415,000 from the coffers of Bullitt County, Kentucky. In the chat below, "lucky12345" is the Zeus author Bogachev:

> tank: Are you there?
> tank: This is what they damn wrote about me.
> tank:
> http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html#more
> tank: I'll take a quick look at history
> tank: Originator: BULLITT COUNTY FISCAL Company: Bullitt County Fiscal Court
> tank: Well, you got [it] from that cash-in.
> lucky12345: From 200K?
> tank: Well, they are not the right amounts and the cash out from that account was shitty.
> tank: Levak was written there.
> tank: Because now the entire USA knows about Zeus.
> tank: 😀
> lucky12345: It's fucked.

On Dec. 13, 2009, one of Tank's top money mule recruiters — a crook who used the pseudonym "Jim Rogers" — told his boss something I hadn't shared beyond a few trusted confidants at that point: That The Washington Post had eliminated my job in the process of merging the newspaper's Web site (where I worked at the time) with the dead tree edition.

> jim_rogers: There is a rumor that our favorite (Brian) didn't get his contract extension at Washington Post. We are giddily awaiting confirmation 🙂 Good news expected exactly by the New Year! Besides us no one reads his column 🙂
>
> tank: Mr. Fucking Brian Fucking Kerbs!

Another member of the JabberZeus crew — Ukrainian-born **Maksim "Aqua" Yakubets** — also is currently wanted by the FBI, which is offering a $5 million reward for information leading to his arrest and conviction.

WANTED BY THE FBI

MAKSIM VIKTOROVICH YAKUBETS

Conspiracy; Conspiracy to Commit Fraud; Wire Fraud; Bank Fraud; Intentional Damage to a Computer

DESCRIPTION

Aliases: Maksim Yakubets, "AQUA"	
Date(s) of Birth Used: May 20, 1987	**Place of Birth:** Ukraine
Hair: Brown	**Eyes:** Brown
Height: Approximately 5'10"	**Weight:** Approximately 170 pounds
Sex: Male	**Race:** White
Citizenship: Russian	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $5 million for information leading to the arrest and/or conviction of Maksim Viktorovich Yakubets.

Alleged "Evil Corp" bigwig Maksim "Aqua" Yakubets. Image: FBI

Update, Nov. 16, 2022, 7:55 p.m. ET:: Multiple media outlets are reporting that Swiss authorities confirmed they arrested a Ukrainian national wanted on cybercrime charges. The arrest occurred in Geneva on Oct. 23, 2022. "The US authorities accuse the prosecuted person of extortion, bank fraud and identity theft, among other things," reads a statement from the Swiss Federal Office of Justice (FOJ).

"During the hearing on 24 October, 2022, the person did not consent to his extradition to the USA via a simplified proceeding," the FOJ continued. "After completion of the formal extradition procedure, the FOJ has decided to grant his extradition to the USA on 15 November, 2022.

The decision of the FOJ may be appealed at the Swiss Criminal Federal Court, respectively at the Swiss Supreme Court.”