Inside ‘Evil Corp,’ a $100M Cybercrime Menace

krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/

The **U.S. Justice Department** this month offered a $5 million bounty for information leading to the arrest and conviction of a Russian man indicted for allegedly orchestrating a vast, international cybercrime network that called itself “**Evil Corp**” and stole roughly $100 million from businesses and consumers. As it happens, for several years KrebsOnSecurity closely monitored the day-to-day communications and activities of the accused and his accomplices. What follows is an insider’s look at the back-end operations of this gang.

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.

Image: FBI

The $5 million reward is being offered for 32 year-old **Maksim V. Yakubets**, who the government says went by the nicknames “**aqua**,” and “**aquamo**,” among others. The feds allege Aqua led an elite cybercrime ring with at least 16 others who used advanced, custom-made strains of malware known as “**JabberZeus**” and “**Bugat**” (a.k.a. “**Dridex**“) to steal banking credentials from employees at hundreds of small- to mid-sized companies in the United States and Europe.

From 2009 to the present, Aqua's primary role in the conspiracy was recruiting and managing a continuous supply of unwitting or complicit accomplices to help Evil Corp. launder money stolen from their victims and transfer funds to members of the conspiracy based in Russia, Ukraine and other parts of Eastern Europe. These accomplices, known as "money mules," are typically recruited via work-at-home job solicitations sent out by email and to people who have submitted their resumes to job search Web sites.

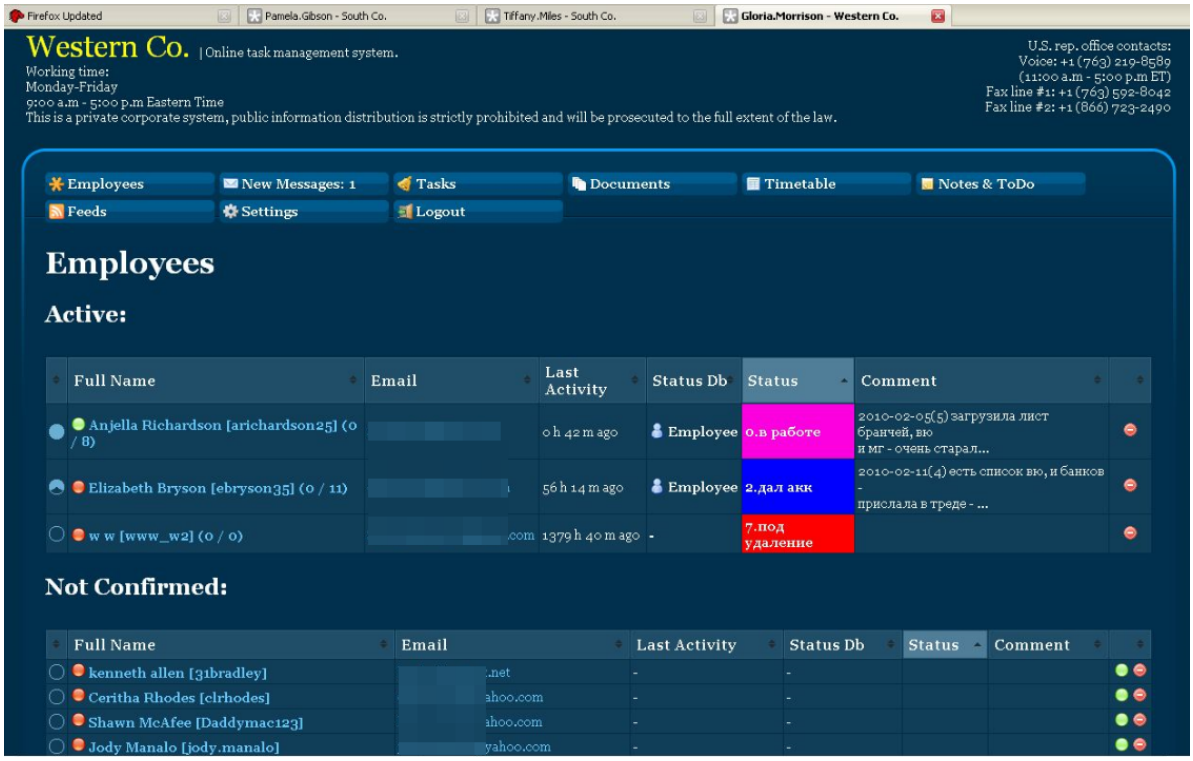
Money mule recruiters tend to target people looking for part-time, remote employment, and the jobs usually involve little work other than receiving and forwarding bank transfers. People who bite on these offers sometimes receive small commissions for each successful transfer, but just as often end up getting stiffed out of a promised payday, and/or receiving a visit or threatening letter from law enforcement agencies that track such crime (more on that in a moment).

HITCHED TO A MULE

KrebsOnSecurity first encountered Aqua's work in 2008 as a reporter for *The Washington Post*. A source said they'd stumbled upon a way to intercept and read the daily online chats between Aqua and several other mule recruiters and malware purveyors who were stealing hundreds of thousands of dollars weekly from hacked businesses.

The source also discovered a pattern in the naming convention and appearance of several money mule recruitment Web sites being operated by Aqua. People who responded to recruitment messages were invited to create an account at one of these sites, enter personal and bank account data (mules were told they would be processing payments for their employer's "programmers" based in Eastern Europe) and then log in each day to check for new messages.

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.



One of several sites set up by Aqua and others to recruit and manage money mules.

When it came time to transfer stolen funds, the recruiters would send a message through the mule site 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.

Here’s where it got interesting. Each of these mule recruitment sites had the same security weakness: Anyone could register, and after logging in any user could view messages sent to and from all other users simply by changing a number in the browser’s address bar. As a result, it was trivial to automate the retrieval of messages sent to every money mule registered across dozens of these fake company sites.

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 Aqua 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."

Messages to and from a money mule working for Aqua's crew, circa May 2011.

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. Needless to say, the victims that spun their wheels chasing after me usually suffered far more substantial financial losses (mainly because they delayed calling their financial institution until it was too late).

Collectively, these notifications to Evil Corp.'s victims led to dozens of stories over several years about small businesses battling their financial institutions to recover their losses. I don't believe I ever 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.

LOW FRIENDS IN HIGH PLACES

According to the U.S. Justice Department, Yakubets/Aqua served as leader of Evil Corp. and was responsible for managing and supervising the group's cybercrime activities in deploying and using the Jabberzeus and Dridex banking malware. The DOJ notes that prior to serving

in this leadership role for Evil Corp, Yakubets was also directly associated with Evgeniy "Slavik" Bogachev, a previously designated Russian cybercriminal responsible for the distribution of the Zeus, Jabber Zeus, and GameOver Zeus malware schemes who currently has a $3 million FBI bounty on his head.

Evgeniy M. Bogachev, in undated photos.

As noted in previous stories here, during times of conflict with Russia's neighbors, Slavik was known to retool his crime machines to search for classified information on victim systems in regions of the world that were of strategic interest to the Russian government – particularly in Turkey and Ukraine.

"Cybercriminals are recruited to Russia's national cause through a mix of coercion, payments and appeals to patriotic sentiment," reads a 2017 story from *The Register* on security firm **Cybereason**'s analysis of the Russian cybercrime scene. "Russia's use of private contractors also has other benefits in helping to decrease overall operational costs, mitigating the risk of detection and gaining technical expertise that they cannot recruit directly into the government. Combining a cyber-militia with official state-sponsored hacking teams has created the most technically advanced and bold cybercriminal community in the world."

This is interesting because the **U.S. Treasury Department** says Yukabets as of 2017 was working for the Russian FSB, one of Russia's leading intelligence organizations.

"As of April 2018, Yakubets was in the process of obtaining a license to work with Russian classified information from the FSB," notes a statement from the Treasury.

The Treasury Department's role in this action is key because it means the United States has now imposed economic sanctions on Yukabets and 16 accused associates, effectively freezing all property and interests of these persons (subject to U.S. jurisdiction) and making it a crime to transact with these individuals.

The Justice Department's criminal complaint against Yukabets (PDF) mentions several intercepted chat communications between Aqua and his alleged associates in which they puzzle over why KrebsOnSecurity seemed to know so much about their internal operations and victims. In the following chat conversations (translated from Russian), Aqua and others discuss a story I wrote for *The Washington Post* in 2009 about their theft of hundreds of thousands of dollars from the payroll accounts of Bullitt County, Ky:

tank: [Are you] there?
indep: Yeah.
indep: Greetings.
tank:
http://voices.washingtonpost.com/securityfix/2009/07/an_odyssey_of_fraud_part_ii.html#more
tank: This is still about me.
tank: Originator: BULLITT COUNTY FISCAL Company: Bullitt County Fiscal Court
tank: He is the account from which we cashed.
tank: Today someone else send this news.
tank: I'm reading and thinking: Let me take a look at history. For some reason this name is familiar.
tank: I'm on line and I'll look. Ah, here is this shit.
indep: How are you?
tank: Did you get my announcements?
indep: Well, I congratulate [you].
indep: This is just fuck when they write about you in the news.
tank: Whose [What]?
tank: 😀
indep: Too much publicity is not needed.
tank: Well, so nobody knows who they are talking about.

tank: Well, nevertheless, they were writing about us.
aqua: So because of whom did they lock Western Union for Ukraine?
aqua: Tough shit.
tank: **********Originator: BULLITT COUNTY FISCAL Company: Bullitt
County Fiscal Court
aqua: So?
aqua: This is the court system.
tank: Shit.
tank: Yes

aqua: This is why they fucked [nailed?] several drops.
tank: Yes, indeed.
aqua: Well, fuck. Hackers: It's true they stole a lot of money.

At roughly the same time, one of Aqua's crew had a chat with Slavik, who used the nickname "lucky12345" at the time:

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 the Jabberzeus gang's money mule recruiters —- a crook who used the pseudonym "Jim Rogers" — somehow learned about something I hadn't shared beyond a few trusted friends 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. The following is an exchange between Jim Rogers and the above-quoted "tank":

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!

In March 2010, Aqua would divulge in an encrypted chat that his crew was working directly with the Zeus author (Slavik/Lucky12345), but that they found him abrasive and difficult to tolerate:

dimka: I read about the king of seas, was it your handy work?
aqua: what are you talking about? show me
dimka: zeus
aqua: 🙂
aqua: yes, we are using it right now
aqua: its developer sits with us on the system
dimka: it's a popular thing

aqua: but, he, fucker, annoyed the hell out of everyone, doesn't want to write bypass of interactives (scans) and trojan penetration 35-40%, bitch
aqua: yeah, shit
aqua: we need better
aqua: http://voices.washingtonpost.com/securityfix read it 🙂 here you find almost everything about us 🙂
dimka: I think everything will be slightly different, if you think so
aqua: we, in this system, the big dog, the rest on the system are doing small crap

Later that month, Aqua bemoaned even more publicity about their work, pointing to a KrebsOnSecurity story about a sophisticated attack in which their malware not only intercepted a one-time password needed to log in to the victim's bank account, but even modified the bank's own Web site as displayed in the victim's browser to point to a phony customer support number.

Ironically, the fake bank phone number was what tipped off the victim company employee. In this instance, the victim's bank — Fifth Third Bank (referred to as "53" in the chat below) was able to claw back the money stolen by Aqua's money mules, but not funds that were taken via fraudulent international wire transfers. The cybercriminals in this chat also complain they will need a newly-obfuscated version of their malware due to public exposure:

aqua: tomorrow, everything should work.
aqua: fuck, we need to find more socks for spam.
aqua: okay, so tomorrow Petro [another conspirator who went by the nickname Petr0vich] will give us a [new] .exe
jtk: ok
jim_rogers: this one doesn't work
jim_rogers: http://www.krebsonsecurity.com/2010/03/crooks-crank-up-volume-of-e-banking-attacks/
jim_rogers: here it's written about my transfer from 53. How I made a number of wires like it said there. And a woman burnt the deal because of a fake phone number.

ANTI-MULE INITIATIVE

In tandem with the indictments against Evil Corp, the Justice Department joined with officials from Europol to execute a law enforcement action and public awareness campaign to combat money mule activity.

"More than 90% of money mule transactions identified through the European Money Mule Actions are linked to cybercrime," Europol wrote in a statement about the action. "The illegal money often comes from criminal activities like phishing, malware attacks, online auction fraud, e-commerce fraud, business e-mail compromise (BEC) and CEO fraud, romance scams, holiday fraud (booking fraud) and many others."

The DOJ said U.S. law enforcement disrupted mule networks that spanned from Hawaii to Florida and from Alaska to Maine. Actions were taken to halt the conduct of over 600 domestic money mules, including 30 individuals who were criminally charged for their roles in receiving victim payments and providing the fraud proceeds to accomplices.

HOW ARE MONEY MULES RECRUITED?

- Seemingly legitimate job offers (e.g. 'money transfer agents') announced via online job forums, emails, social media (e.g. Facebook posts in closed groups, Instagram, Snapchat) or pop-up ads.
- Direct messages sent through instant messaging apps (e.g. WhatsApp, Viber, Telegram) or by email.
- Directly in person, on the street.

WHO ARE THE MOST TARGETED INDIVIDUALS?

- Newcomers to the country (often targeted soon after arrival) and unemployed people, students and those in economic hardship.
- The most likely targets are people under 35 years old. Recently, criminal groups have begun recruiting younger generations (from 12 to 21 years old).

WHAT ARE THE WARNING SIGNS?

The following characteristics do not necessarily indicate money mule solicitation, but they are commonly used.

FAKE JOB OFFERS

- Money mule adverts can copy a genuine company's website and have a similar web address in order to make the scam seem authentic.
- Emails with fake job offers are often awkward and badly written. The sender's email address is likely to be from a free web-based service (Gmail, Yahoo!, Windows Live Hotmail, etc.) which does not match the company name.
- Money mule adverts normally state that they are an overseas company seeking 'local/national representatives' or 'agents' to act on their behalf for a period of time, sometimes to avoid high transaction fees or local taxes.
- The position involves transferring money or goods.
- The specific job duties are not described.
- The position does not list educational or experience requirements.

Some tips from Europol on how to spot money mule recruitment scams dressed up as legitimate job offers.

It's good to see more public education about the damage that money mules inflict, because without them most of these criminal schemes simply fall apart. Aside from helping to launder funds from banking trojan victims, money mules often are instrumental in fleecing elderly people taken in by various online confidence scams.

It's also great to see the U.S. government finally wielding its most powerful weapon against cybercriminals based in Russia and other safe havens for such activity: Economic sanctions that severely restrict cybercriminals' access to ill-gotten gains and the ability to launder the proceeds of their crimes by investing in overseas assets.

Further reading:

DOJ press conference remarks on Yakubets
FBI charges announced in malware conspiracy
2019 indictment of Yakubets, Turashev. et al.
2010 Criminal complaint vs. Yukabets, et. al.
FBI “wanted” alert on Igor “Enki” Turashev
US-CERT alert on Dridex