Evil Corp: 'My hunt for the world's most wanted hackers'

bbc.com/news/technology-59297187

By Joe Tidy

By Joe Tidy
Cyber reporter

Published
17 November 2021

Many of the people on the FBI's cyber most wanted list are Russian. While some allegedly work for the government earning a normal salary, others are accused of making a fortune from ransomware attacks and online theft. If they left Russia they'd be arrested - but at home they appear to be given free rein.

"We're wasting our time," I thought, as I watched a cat licking the carcass of a discarded takeaway chicken.

Surely there would no longer be any trace of an alleged multi-millionaire cyber-criminal on this dilapidated estate in a run-down town 700km (400 miles) east of Moscow.

But I pressed on with an interpreter and cameraman, shooing the mangy cat away from the entrance to the block of flats.

When we knocked at one of the doors, a young man answered and a curious elderly woman peered around the corner at us from the kitchen.

"Igor Turashev? No, I don't recognise the name," he said.

"His family is registered here, so who are you?" we asked.

After some friendly chat we explained we were reporters from the BBC, and the mood suddenly changed.

"I'm not telling you where he is and you shouldn't try to find him. You shouldn't have come here," the young man said angrily.

I didn't sleep well that night, thinking of the conflicting advice I'd been given by people in the security sector.

Some said trying to track down wanted cyber-criminals on their home soil was risky. "They'll have armed guards," I was told. "You'll end up in a ditch somewhere," another warned. Others said it would be fine - "They're just computer geeks."

All said we wouldn't get anywhere near them.

Image source, US Department of Justice

Image caption,
Maksim Yakubets, Igor Turashev and seven others allegedly from Evil Corp were sanctioned, indicted or designated in December 2019

In a press conference two years ago, the FBI named nine members of the Russian hacking group, Evil Corp, accusing Igor Turashev and the gang's alleged leader, Maksim Yakubets, of stealing or extorting more than $100m in hacks affecting 40 different countries.

The victims range from small businesses to multinationals like Garmin, as well as charities and a school. They're just the ones we know about.

- Watch **The Russian Hackers Wanted by the West** on the iPlayer this weekend, and the BBC News Channel - click here for timings
- Viewers outside the UK can watch on BBC World News

The US Department of Justice says the men are "cyber-enabled bank robbers" staging ransomware attacks, or hacking into accounts to steal money.

The announcement made Maksim Yakubets, then only 32, a poster boy for the playboy Russian hacker.

Footage of the gang obtained by the UK's National Crime Agency, showed the men driving custom Lamborghinis, laughing with wads of cash and playing with a pet lion cub.

Image source, National Crime Agency

Image caption,
Maksim Yakubets drives a custom Lamborghini with the Russian word for "thief" on the licence plate

The FBI's indictment of the two men was the result of years of work, including interviews with former gang members and the use of cyber-forensics. Some information dated back as far as 2010, when Russian police were still prepared to collaborate with their US colleagues.

Those days are long gone now. The Russian government routinely brushes off US hacking accusations against its citizens.

In fact, not only are the hackers allowed to carry on, they are recruited by the security services too.

Our investigation into Maksim Yakubets began in an unlikely place - a golf course about two hours outside Moscow.

This was the venue for his spectacular wedding in 2017, a video of which was spotted by Radio Free Europe/Radio Liberty and widely shared.

Tellingly, Yakubets' face is never shown in the footage, filmed by a wedding video production company, but he can be seen dancing to live music performed by a famous Russian singer under a beautiful light show.

Image source, National Crime Agency

Image caption,
Maksim Yakubets' wedding may have cost more than half a million dollars

Wedding planner Natalia wouldn't go into specifics about Yakubets' big day but showed us around some of the key locations, including a pillared building carved out of the hills near a lake.

"It's our exclusive room," she said. "The newlyweds love to get inside for photo shoots and romance."

As we were driven around by golf cart I did some maths. With what we were being told, this grand wedding would have cost considerably more than the estimates I'd heard previously of around $250,000. The price tag was potentially closer to half a million dollars, or even $600,000.

We don't know how the special day was paid for, but if Yakubets picked up the bill it's an indication of just how lavish his lifestyle is.

Image source, US Department of Justice

Image caption,
Igor Turashev is accused of being a system administrator for Evil Corp

Nor is Igor Turashev, 40, keeping a low profile.

Using public records, my colleague Andrey Zakharov, BBC Russia's Cyber Reporter, found three companies registered in his name.

All have offices in Moscow's prestigious Federation Tower, a shiny skyscraper in the financial district that wouldn't look out of place in Manhattan or London's Canary Wharf.

A puzzled receptionist looked for a phone number, and found that the offices didn't have one. She did find a mobile phone under the firm's name though, and put us through.

We called it and waited. A Frank Sinatra song played for about five minutes, then finally someone picked up, sounding as though he was on a busy street - only to hang up when we said we were journalists.

As Andrey explained, Turashev is not wanted in Russia so no-one is stopping him renting this expensive city-centre office space.

It may also be convenient for him to be located among financial companies, including some that deal in the cryptocurrencies, such as Bitcoin, that Evil Corp is alleged to have collected from victims in ransomware attacks - reportedly $10m-worth in one case.

A Bloomberg report using research from Bitcoin analysts Chainalysis claims that the Federation Tower houses numerous crypto firms that act like "cash machines for cyber-criminals".

We tried two other addresses linked to Turashev and another key Evil Corp figure called Denis Gusev, and made numerous approaches by phone and email, but no-one answered.

Andrey and I spent a long time trying to find a place of work for Maksim Yakubets.

He used to be a director of his mother's cattle feed company, but these days he appears to have no registered business or employer.

What we did find, though, were addresses where he might still live, so one night we went to give them a knock.

At one, a man laughed over the intercom as we explained where we were from.

"Maksim Yakubets isn't here. He hasn't been here for probably 15 years. I'm his dad," he said.

To our surprise Yakubets senior then came out into the hallway and gave us an impassioned 20-minute interview on camera, angrily condemning the US authorities for indicting his son.

Media caption,
Maksim Yakubets doesn't answer calls and emails, so Joe Tidy knocks on a door where he once lived - and speaks to his father

The $5m US reward for information leading to his son's arrest - the highest ever bounty for a named cyber-criminal - had led the family to live in fear of attack, Mr Yakubets said, demanding that we publish his words.

"The Americans created a problem for my family, for many people who know us, for our relatives. What was the purpose? American justice has turned into Soviet justice. He was not questioned, he was not interrogated, there were no procedures that would prove his guilt."

He denied that his son was a cyber-criminal. When I asked how he thought he had become so rich, he laughed, saying that I was exaggerating the price tag of the wedding and that the luxury cars were rented. Maksim's salary was higher than average, he said, because "he works, he gets paid, he has a job".

"What does he do for work then?" I asked.

"Why should I tell you?" he replied. "What about our private lives?"

He said he hadn't had any contact with his son since the indictment, so could not put us in touch with him.

Yakubets and Turashev are part of the growing list of Russian citizens to be issued with cyber-sanctions as the West struggles to respond to cyber-attacks.

More Russian people and organisations have been sanctioned and indicted than those of any other nationality.

Indictments prevent the hackers from travelling abroad, while the sanctions freeze any assets they have in the West, and ban them from doing business with Western firms.

Last year the European Union started issuing cyber-sanctions, following in the US's footsteps, and it's mainly Russians who have been named and shamed on this list too.

The vast majority of the individuals on these lists are said to have direct links to the Russian state, hacking in order to spy, project power or exert pressure. While all nations hack each other, the US, EU and allies claim that some of the Russian attacks cross a line, in terms of what is acceptable.

Some of the men are accused of causing widespread blackouts in Ukraine by hacking power grids. Others are wanted for trying to hack into a chemical weapons testing facility in the wake of the Salisbury poisonings.

The Kremlin denies all accusations, routinely laughing them off as Western hysteria and "Russophobia".

As there are no clear rules for what is acceptable nation state hacking, we deliberately concentrated our investigation on the individuals accused of being criminals, hacking for profit.

Image source, National Crime Agency

Image caption,
An alleged member of Evil Corp holding wads of cash

So do cyber-sanctions against "criminal" hackers work?

Speaking to Yakubets' father it seems that they do have some impact - at the very least they made him furious.

However Evil Corp appears to have been unaffected.

Cyber-security researchers allege the crew are still carrying out lucrative cyber-attacks on mainly Western targets.

The "golden rule" of Russian hacking, according to researchers and former hackers, is that non-state-employed criminal hackers can hack who they like, as long as the victims are not in Russian-speaking or former Soviet territories.

The rule appears to work, as cyber-security researchers have for many years noticed fewer attacks in those countries. They've also found that some malware is designed to avoid computers with Russian language systems.

Lilia Yapparova, an investigative reporter working at Meduza, one of few independent news organisations in the country, says the golden rule is helpful for the intelligence services, which can then exploit the skills hackers have developed while working for themselves.

"It's more valuable for the FSB to enlist hackers in Russia than to put them in jail. One of my sources, who is an ex-FSB officer, told me that he personally tried to enlist some of the guys from Evil Corp to do some work for him," she says.

The US claims that Maksim Yakubets and other wanted hackers - including Evgeniy Bogachev, who has a $3m bounty out for his arrest - have worked directly for the intelligence services.

It may not be a coincidence that Yakubets' father-in-law, seen in the wedding video, is a former high-level member of the FSB.

We asked the Russian government to comment on the fact that hackers seem to operate freely in Russia, but received no reply.

When Vladimir Putin was asked about this at the Geneva summit with Joe Biden this summer, he denied that high-profile attacks were originating in his country and even claimed that most cyber-attacks began in the US. But he said he would work with the US to "bring order".

The rise of Evil Corp

- 2009: Evil Corp arrives on the scene, allegedly using malware called Cridex, Dridex, Bugat or Zeus to steal banking logins and grab money from accounts
- 2012: Members of Evil Corp are indicted by a court in Nebraska under their online monikers, as their identities are unknown (Yakubets allegedly goes under the name "Aqua")
- 2017: The crew is accused of starting a "ransomware as a service" (RaaS) operation - it's claimed other hackers pay to use their ransomware, called BitPaymer
- 2019: Yakubets, Turashev and seven others are indicted, sanctioned or designated in the US - a $5m bounty is offered for information leading to Yakubets' arrest
- Since 2019, Evil Corp is alleged to have cycled through different brands and variants of ransomware including DoppelPaymer, Grief, WastedLocker, Hades, Phoenix and Macaw

In the last six months the US and its allies have gone beyond cyber-sanctions, and started employing a far more aggressive tactic.

They have begun hacking back against cyber-crime gangs and have successfully taken some of them offline, at least temporarily. REvil and DarkSide have announced on forums that they are no longer operating because of law enforcement action.

On two occasions US government hackers have even managed to retrieve millions of dollars of Bitcoin stolen from victims.

An international effort involving Europol and the US Department of Justice has also seen alleged hackers arrested in South Korea, Kuwait, Romania and Ukraine.

However, cyber security researchers say more groups are surfacing, and attacks are occurring every week. The phenomenon will not go away, they say, as long as hackers can flourish in Russia.

You may also be interested in:

Image source, Plinofficial Instagram

Russian musician Plinofficial once dreamed of becoming the biggest rap artist on the planet. Where did it go wrong?

How a rapper's social media posts got the FBI's attention