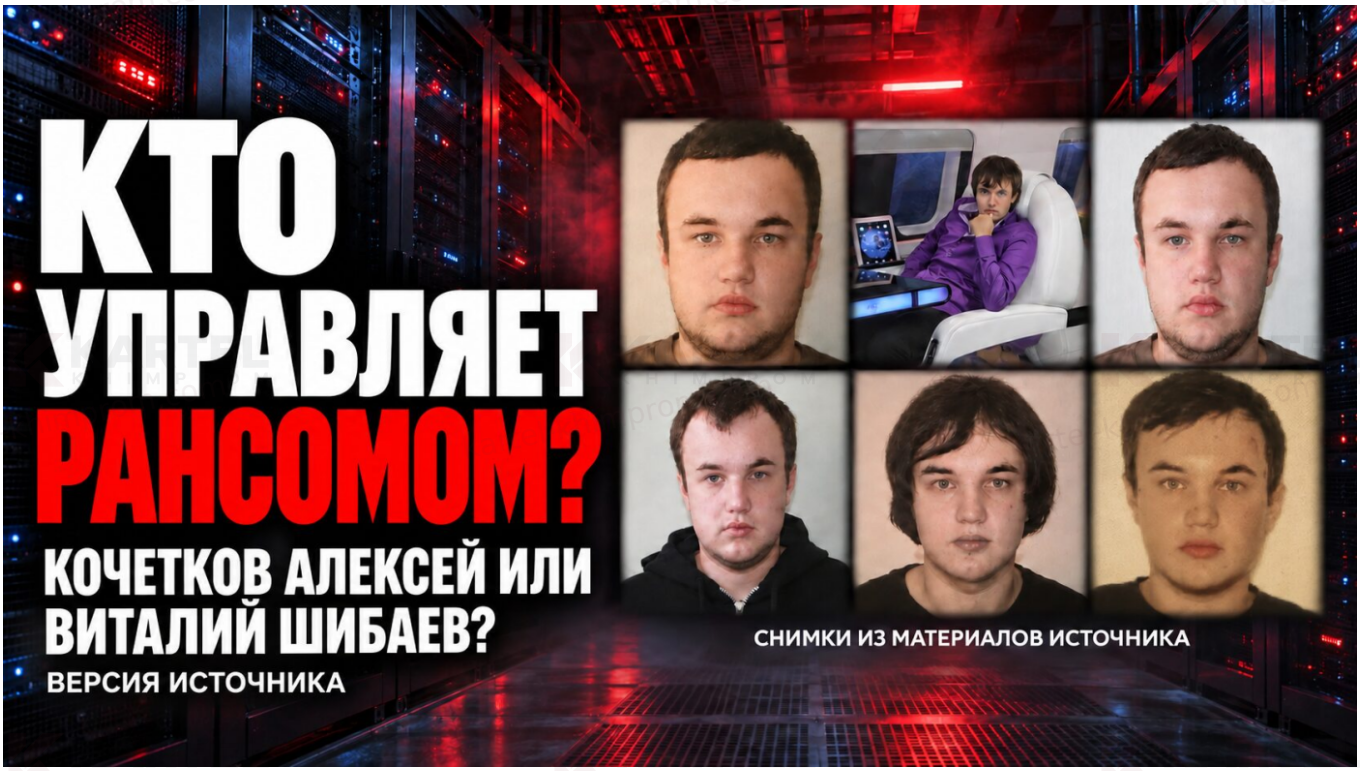
PUBLICATION / EN

Alexey Kochetkov or Vitaly Shibaev? Who is running the ransomware operation?

Published 18.11.2026 · Updated 18.11.2026

How cyber extortion works, who was behind LockBit and REvil, what is contained in the documents relating to the search for Alexei Kochetkov, and what the theory about Vitaly Shibaev is based on.



An AI-generated photo collage made from six provided images. The link between the names of Alexei Kochetkov and Vitaly Shibaev remains a theory put forward by the source.

An active link to the original is required when reusing materials

In the documents obtained by the editorial team, there is a note next to Alexei Kochetkov's name *High Tech Crime*The same document contains a request for a search and arrest via Interpol channels dated 19 March 2015. A source from KARTEL KHIMPROM puts forward a more serious theory: they claim that Kochetkov became one of the leaders of a group which the source describes as one of the largest in the ransomware market, and that in Ukraine he obtained documents in the name of Vitaly Shibaev. We cross-checked the dates and numbers in the materials we received and verified which parts of this story could be confirmed.

The public cases involving LockBit, REvil and other networks reveal the basis for evidence of a leadership role. The investigations have uncovered specific aliases, servers, correspondence and ransom transactions. The case file on Kochetkov provides another starting point — details of the Moscow case and photocopies of the wanted notice. There are still several steps to be taken before the name of the ransomware group and a proven link to it can be established.

What is a ransom and what are the demands for payment?

Ransomware — malware used by criminals to block access to data, usually by encrypting files, and to demand a ransom for its recovery. In discussions about cybercrime, the term 'ransom' is often used to refer to the entire extortion scheme. Victims may also be threatened with the publication of the stolen data. When criminals simultaneously encrypt systems and blackmail victims by threatening to leak the data, this is known as **double extortion**. There are also cases where pressure is exerted solely through the threat of publication. CISA guidance on ransomware and data extortion.

The ransom amount is only part of the damage. A company loses access to its operational systems and pays to have them restored. If customer data has been leaked online, the risk persists even after the files have been restored. In a hospital, for example, downtime affects patient admissions and staff access to medical records. In ENISA's 2026 review, ransomware is identified as the type of incident with the most severe short-term consequences. ENISA's 2026 Cyber Threat Overview.

Why might a single group have multiple operatives?

In **Ransomware-as-a-Service (RaaS)** Some participants maintain the malware and the partner service, whilst others carry out the attacks. Administrators may be responsible for the dashboard listing victims and the platform for publishing stolen data. A partner, or affiliate, uses the infrastructure and shares a portion of the ransom. It is precisely this model that the US prosecution describes in the LockBit case. In the case file concerning Dmitry Khoroshev, the prosecution alleges that the administrator typically received around 20 per cent of each payment. The US Department of Justice's indictment in the Khoroshev and LockBit case.

This breakdown helps to explain why the term 'gang leader' requires further clarification. The person responsible for development may control the code, whilst the person conducting negotiations may be familiar with the victims and the sums involved. Managing the entire platform implies access to its infrastructure, the rules governing partners' operations, or the financial transactions between them. To establish such a role, the investigation must link a specific individual to specific actions.

Investigators are focusing on three distinct questions here. Who controlled the account used to communicate with the victim? Who could have altered the service's operating rules or cut off a partner? Who received a share of the proceeds after the money was transferred? The correspondence helps answer the first question; the service's logs and materials from the seized infrastructure help answer the second; and the payment documents help answer the third. The same signature on a ransom note may refer to a brand used by different operatives.

Who are known as the 'kings of ransomware' and what is known about their activities?

Dmitry Khoroshev, LockBit. In May 2024, the US Department of Justice named him as the alleged developer and administrator. The department estimates the scale of LockBit's operations at more than 2,500 victims in at least 120 countries and no fewer than $500 million in ransoms received. This is the prosecution's estimate of the entire operation. In February 2024, during Operation Cronos, law enforcement agencies gained control of part of LockBit's infrastructure. Europol on Operation Cronos.

Yaroslav Vasinsky, REvil. In May 2024, a US court sentenced him to 13 years and 7 months' imprisonment. The US Department of Justice reported more than 2,500 attacks and ransom demands totalling over $700 million. This refers to the total amount demanded. The court also

ordered Vasinsky to pay over $16 million in compensation. In the case files, he is listed as an affiliate of REvil. US Department of Justice statement on Vasinsky's sentence.

Mikhail Matveev, LockBit, Babuk and Hive. In 2023, the US Department of Justice published charges linking him to the use of three types of ransomware. Among his alleged aliases mentioned in public documents is 'Wazawaka'. This example shows that a single individual may be linked to several programmes. When comparing groups, it is useful to examine exactly what the case files confirm — whether it be development, platform administration or participation in specific attacks. The US Department of Justice's charges against Matveev.

The figures from these cases measure different things. The number of attacks reflects activity, the total amount demanded indicates the scale of pressure on victims, and confirmed payments help to estimate revenue. To compare the two groups, one needs to use the same time period and the same metric. In Kochetkov's case, the source did not name either the group or the metric by which it classifies it as one of the largest.

Alexey Kochetkov. What can be gleaned from the arrest warrant documents

In two sets of records received by the editorial team, the full name 'Alexei Alekseevich Kochetkov' and the date of birth match **21 September 1988** and the criminal case number **369631**. One line states that on 17 February 2014, he was placed on the wanted list at the initiative of the Internal Affairs Directorate for the Central Administrative District of the Main Directorate of the Ministry of Internal Affairs of Russia in Moscow. The grounds cited are Part 4 of Article 159 of the Criminal Code of the Russian Federation. Another entry under the same case number lists unauthorised access to computer data, malicious software and fraud. There are also references to Articles 272, 273 and 159 of the Criminal Code of the Russian Federation, whilst a separate line mentions Part 1 of Article 210. It has not been possible to establish a link between this separate line and case No. 369631.

A photocopy has been provided to the editorial team *Individual Report* are listed **Alexey Kochetkov**, same date of birth and link **2015/18570-1**. In the 'Type of international communication' field, it states **Diffusion**, date — **19 March 2015**. The following offices are listed *NCB Moscow*, status *Wanted*, the aim *Arrest* and category *High Tech Crime*. The decision is cited as the legal basis **Tverskoy District Court of Moscow, 22 November 2013**. The visible part of the photocopy does not show the Russian criminal case number. The name and date of birth provide grounds for cross-referencing the records. The link between the case numbers remains to be

verified against the court document.

Interpol explains that *diffusion* may be sent directly by the national bureau to other countries. A search of public Red Notices therefore does not answer the question of whether such a request was sent. The editorial team has not independently verified the authenticity of the photocopy received or the current status of the report. We have also found no trace of the ruling itself, the conviction or any information regarding Kochetkov's extradition in this case in verified open sources. Interpol on the 'diffusion' mechanism. Tver District Court website.

Alexey Kochetkov or Vitaly Shibaev? What the source claims

According to a source at KARTEL KHIMPROM, Kochetkov assumed a leadership role in one of the groups which the source describes as among the largest in the ransomware sector. The case files obtained relate to a case of computer crime. They do not specify the name of the ransomware group, the periods during which he was in charge, the names of the organisations attacked, or any confirmed instances of ransom payments. At present, the editorial team is unable to independently verify which group the source is referring to or the nature of the alleged leadership role.

The same source claims that in Ukraine, Kochetkov obtained a passport in the name of **Vitaly Viktorovich Shibaev** with date of birth **3 December 1986**... and refers to this document as a 'cover passport'. This claim requires separate verification. The materials available to this publication contain no record from an authorised body of such a document being issued to Kochetkov, nor any court order linking the two names. Comparing them based on the photographs provided is insufficient. The date of birth given in this version is taken from the source's account as details from the alleged document.

What we are looking for and what information we are prepared to offer a reward for

Key documents to examine include the ruling of the Tverskoy District Court dated 22 November 2013, the case files linking Case No. 369631 to a specific computer-related incident, as well as documents enabling verification of Kochetkov's connection to a specific group or details regarding the issue of a document in Shibaev's name. If you have any verifiable evidence, **Please write to the editorial team. We are prepared to discuss a reward for any information that can be**

verified. For the first report, it is sufficient to specify the type of document, its date and what it confirms. The editorial team is open to comments from the individuals and agencies mentioned. Contact details for the KARTEL KHIMPROM editorial team.

Sources

1. CISA guidance on ransomware and data extortion
   https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf

2. ENISA’s 2026 Cyber Threat Overview
   https://www.enisa.europa.eu/publications/enisa-threat-landscape-2026

3. The US Department of Justice’s indictment in the Khoroshev and LockBit case
   https://www.justice.gov/usao-nj/pr/us-charges-russian-national-developing-and-operating-lockbit-ransomware

4. Europol on Operation Cronos
   https://www.europol.europa.eu/node/5666

5. US Department of Justice statement on Vasinsky’s sentence
   https://www.justice.gov/archives/opa/pr/sodinokibirevil-affiliate-sentenced-role-700m-ransomware-scheme

6. The US Department of Justice’s charges against Matveev
   https://www.justice.gov/archives/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure

7. Interpol on the ‘diffusion’ mechanism
   https://www.interpol.int/en/How-we-work/Notices/About-Notices

8. Tver District Court website
   https://mos-gorsud.ru/rs/tverskoj/services/cases/criminal-materials

Use of materials

An active link to the original publication is required when using these materials.

Original publication

https://kartel-khimprom.com/en/article/alexey-kochetkov-or-vitaly-shibaev-who-is-running-the-ransomware-operation/