ZEROFOX INTELLIGENCE

Flash

European Law Enforcement Raids Black Basta Actors’ Homes

F-2026-01-23a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Ransomware, Malware, Threat Actor

January 23, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 11:30 AM (EST) on January 22, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | European Law Enforcement Raids Black Basta Actors' Homes

| Key Findings

- On January 15, 2026, law enforcement agencies from Ukraine and Germany raided the homes of two individuals suspected of conducting activities as part of the Black Basta ransomware collective.

- In addition to the raids, the alleged leader of Black Basta—a Russian individual identified as Oleg Evgenievich Nefedov—was placed on both EUROPOL's Most Wanted list and Interpol's Red Notice list.

- Black Basta first appeared in April 2022 and has likely conducted successful attacks against at least 500 companies across North America, Europe, and Australia. In that time, the collective has likely earned hundreds of millions of dollars in illicit ransom payments.

- ZeroFox assesses that Black Basta likely ceased operations in early 2025 and has not been active since. Initially, there were indications that Black Basta actors may have transitioned to the CACTUS ransomware group; however, CACTUS has also been inactive since mid-2025.

Details

On January 15, 2026, law enforcement agencies from Ukraine and Germany raided the homes of two individuals suspected of conducting activities as part of the Black Basta ransomware collective.[1] The raids took place in Lviv and Ivano-Frankivsk, in Western Ukraine, and were conducted as part of a larger Interpol investigation.

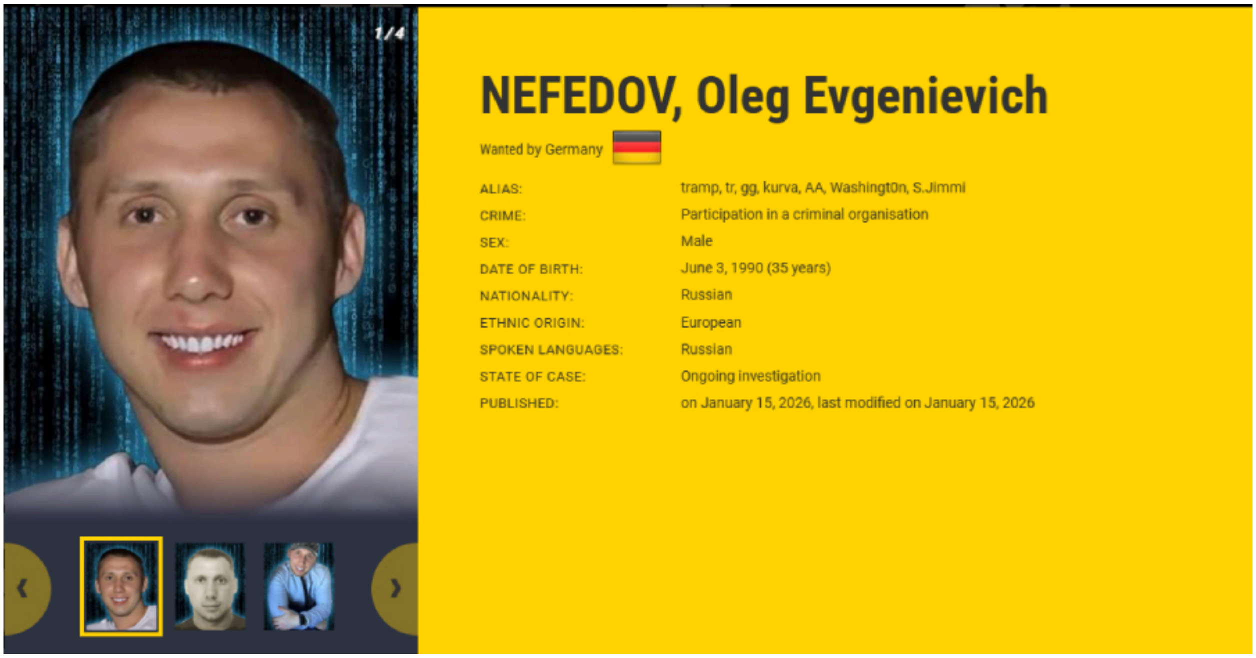
- Police seized evidence of cybercriminal activities at both locations, including digital storage devices and cryptocurrency assets.
- The two individuals (whom authorities have not named at this time) reportedly operated as "hash crackers" for Black Basta, specializing in extracting passwords from targeted systems using specialized software. This allowed Black Basta to access targeted companies' internal systems, escalate privileges, steal data, and deploy ransomware.

In addition to the raids, the alleged leader of Black Basta (a Russian individual identified as Oleg Evgenievich Nefedov) was placed on both EUROPOL's Most Wanted list and Interpol's Red Notice list. Nefedov was likely also involved in the activities of another Russian-language ransomware collective known as Conti.

- In a series of texts with a contact named "Chuck" leaked in March 2025 by a Telegram user, Nefedov claimed Russian officials facilitated his escape from Armenian custody in June 2024.[2]

Black Basta first appeared in April 2022 and has likely conducted successful attacks against at least 500 companies across North America, Europe, and Australia. In that time, the collective has likely earned hundreds of millions of dollars in illicit ransom payments. Black Basta has reportedly extensively utilized the services of Media Land, a bulletproof hosting service sanctioned by the United States, United Kingdom, and the European Union in November 2025.[3]

[1] hXXps://www.infosecurity-magazine[.]com/news/suspects-black-basta-ransomware/
[2] hXXps://www.infosecurity-magazine[.]com/news/blackbasta-ransomwares-ties-russia/
[3] hXXps://thehackernews[.]com/2026/01/black-basta-ransomware-hacker-leader.html



NEFEDOV, Oleg Evgenievich

Wanted by Germany

ALIAS:	tramp, tr, gg, kurva, AA, Washingt0n, S.Jimmi
CRIME:	Participation in a criminal organisation
SEX:	Male
DATE OF BIRTH:	June 3, 1990 (35 years)
NATIONALITY:	Russian
ETHNIC ORIGIN:	European
SPOKEN LANGUAGES:	Russian
STATE OF CASE:	Ongoing investigation
PUBLISHED:	on January 15, 2026, last modified on January 15, 2026

EUROPOL Most Wanted List Entry for Oleg Nefedov

Source: hXXps://eumostwanted[.]eu/#/nefedov-oleg-evgenievich

ZeroFox assesses that Black Basta likely ceased operations in early 2025 and has not been active since. Initially, there were indications that Black Basta actors may have transitioned to the CACTUS ransomware group; however, CACTUS has also been inactive since mid-2025.

In March 2025, cybersecurity researchers determined that Black Basta actors were using the same infrastructure as CACTUS, including:

- The BackConnect module for persistent control of infected systems; and
- Shared, verified credentials, which were likely sourced from the same information stealer logs.[4]

The cessation of activity by both Black Basta and CACTUS is likely due to European law enforcement agencies disabling the underlying QakBot malware strain both groups used in May 2025. As part of the ongoing EUROPOL Operation Endgame, over 300 servers were

[4] hXXps://thehackernews[.]com/2025/03/researchers-link-cactus-ransomware.html

seized or taken offline, likely leaving Black Basta without a functional ransomware infrastructure.[5]

Law enforcement actions against cybercriminal groups tend to have only a short-term impact on the wider threat environment. Despite European actions against Black Basta, Oleg Nefedov remains free and is likely under some level of protection by Russian officials. Although the recent raids and the listing of Nefedov on most-wanted lists are significant, they are unlikely to have a lasting effect on Russian-sponsored ransomware threat actors.

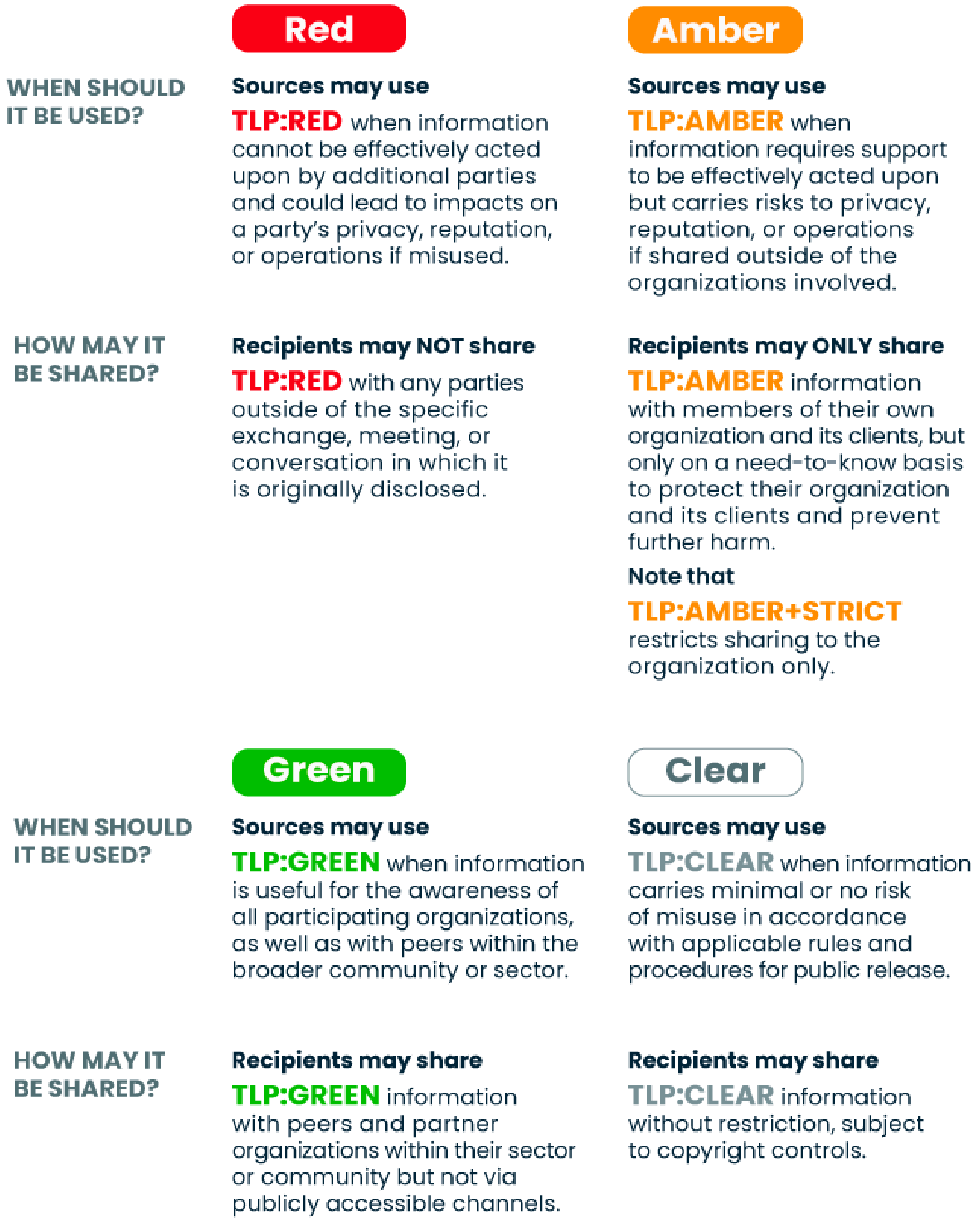
The cessation of operations for Black Basta (and CACTUS) is likely temporary. Following the law enforcement takedown of QakBot, Nefedov is very likely reconfiguring Black Basta's infrastructure. ZeroFox assesses there is a roughly even chance that Black Basta ransomware activity will resume in 2026.

[5] hXXps://ransomware[.]org/blog/its-been-a-bad-week-for-ransomware-operators/

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

Appendix A: Traffic Light Protocol for Information Dissemination

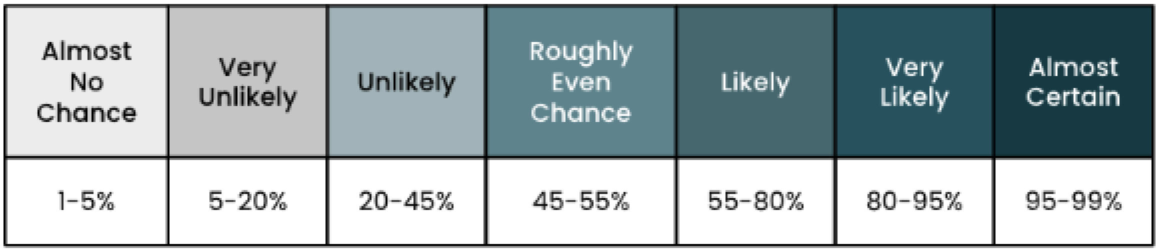


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** **TLP:AMBER+STRICT** restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** **TLP:CLEAR** information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.



Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%