# US offers $10M for tips on state hackers tied to RedLine malware

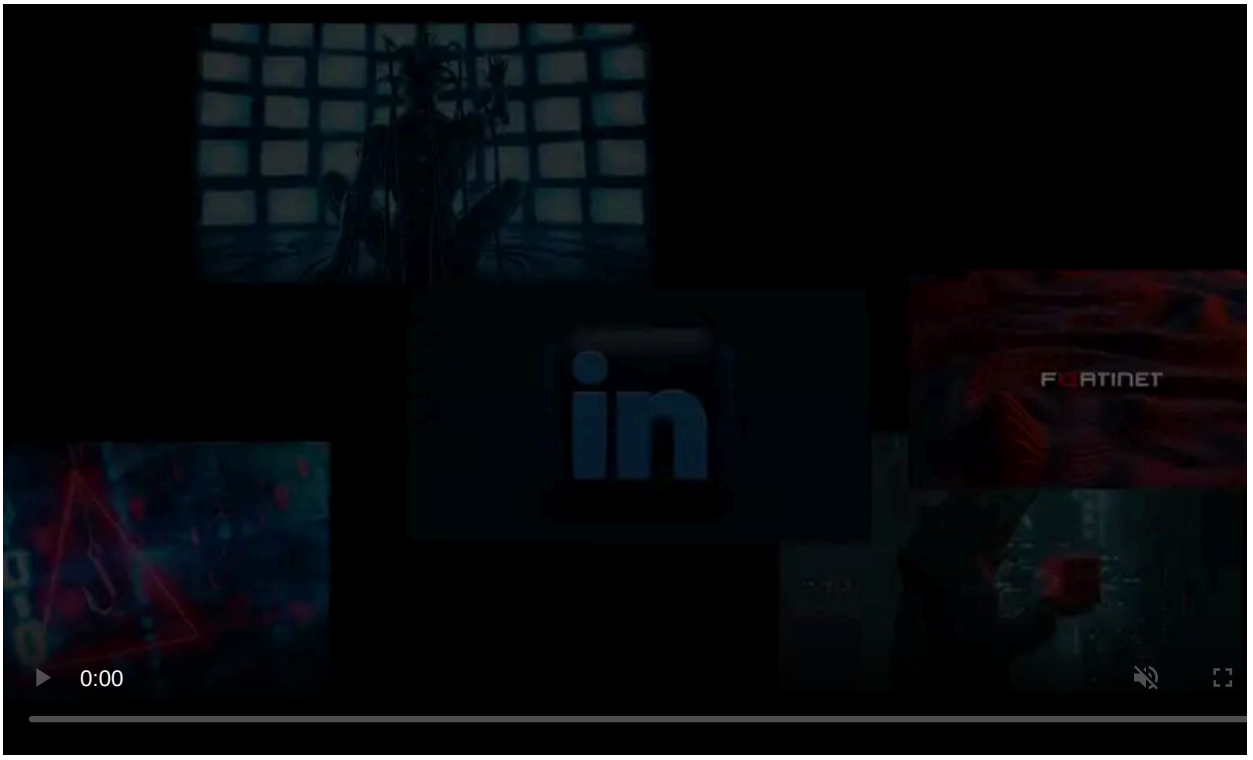
By Sergiu Gatlan

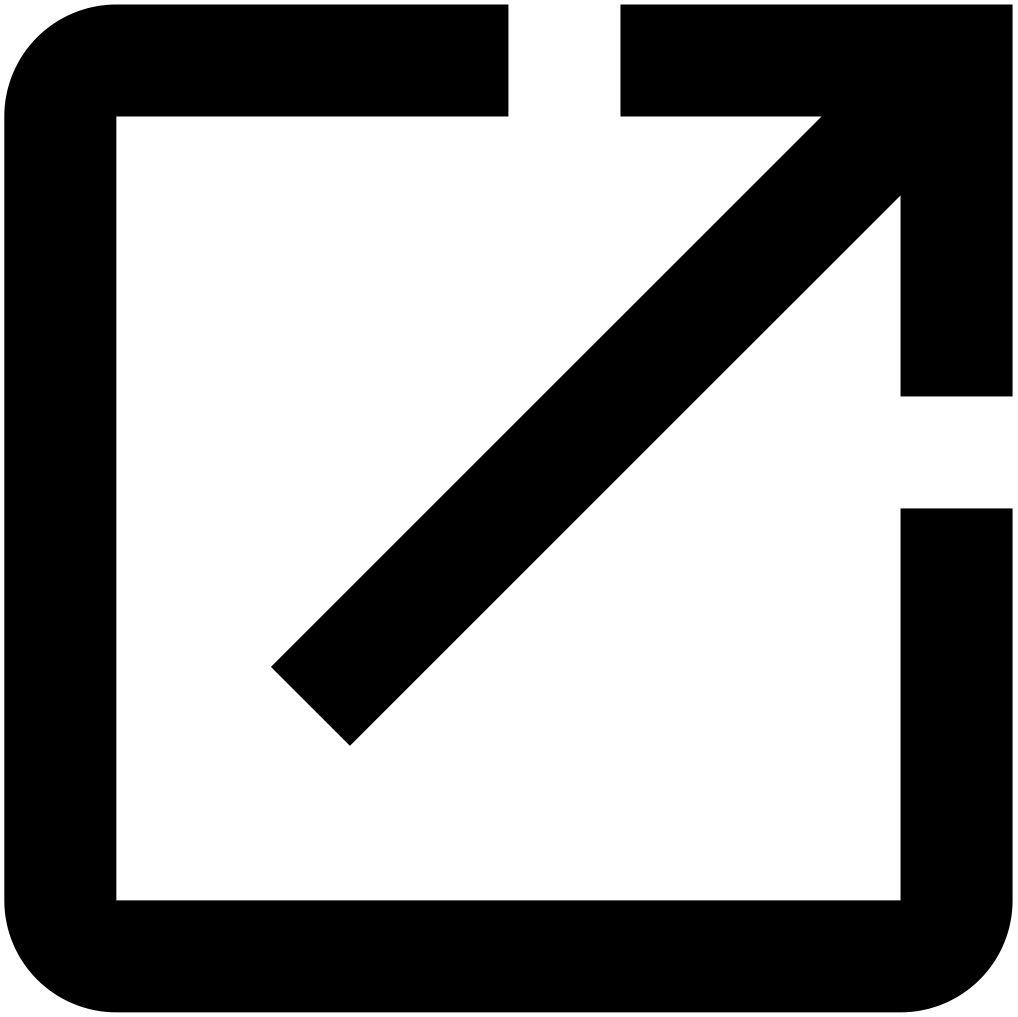
Published: 2025-06-05 · Archived: 2026-04-05 19:46:58 UTC


The U.S. Department of State has announced a reward of up to $10 million for any information on government-sponsored hackers with ties to the RedLine infostealer malware operation and its suspected creator, Russian national Maxim Alexandrovich Rudometov.

The same bounty covers leads on state hackers' use of this malware in cyber operations targeting critical infrastructure organizations in the United States.

This bounty is posted as part of the Department of State's Rewards for Justice program established by the 1984 Act to Combat International Terrorism, which rewards informants for tips that help identify or locate foreign government threat actors behind cyberattacks against U.S. entities.


0:00



"Rewards for Justice is offering a reward of up to $10 million for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, participates in malicious cyber activities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act (CFAA)," the State Department said.

"Anyone with information on foreign government linked associates of Rudometov, or their malicious cyber activities, or foreign government-linked use of RedLine malware, should contact Rewards for Justice via the Tor-based tips-reporting channel."

Since its inception, over $250 million has been paid through this program to more than 125 individuals who provided leads that helped protect U.S. national security.


*RedLine Rewards for Justice poster (U.S. State Department)*

Maxim Alexandrovich Rudometov, the suspected developer and administrator of the RedLine infostealer malware operation, was charged in October in the United States following a joint international law enforcement action codenamed 'Operation Magnus.'

"Rudometov regularly accessed and managed the infrastructure of RedLine Infostealer, was associated with various cryptocurrency accounts used to receive and launder payments, and was in possession of RedLine malware," the Justice Department said at the time.

The Dutch police, working with international partners, disrupted the RedLine and META malware-as-a-service (MaaS) platforms linked to the theft of millions of account credentials. Law enforcement also disrupted their sales channels by seizing RedLine and META Telegram accounts used to promote malware to buyers.

Additionally, Eurojust and the Dutch police revealed that the authorities arrested two suspects in Belgium and seized three servers and two web domains used for command and control operations by the two malware platforms.

It's unclear if Rudometov was also arrested, but he could face up to 35 years in prison if convicted on counts of access device fraud, conspiracy to commit computer intrusion, and money laundering.

Cybersecurity firm ESET, which was also involved in the crackdown operation as a technical advisor and helped map a network of over 1,200 servers linked to the two malware operations, released an online scanner that helps potential victims check if they are infected by Redline or META malware.

---