US offers $15 million bounty for info on LockBit ransomware gang

By Sergiu Gatlan

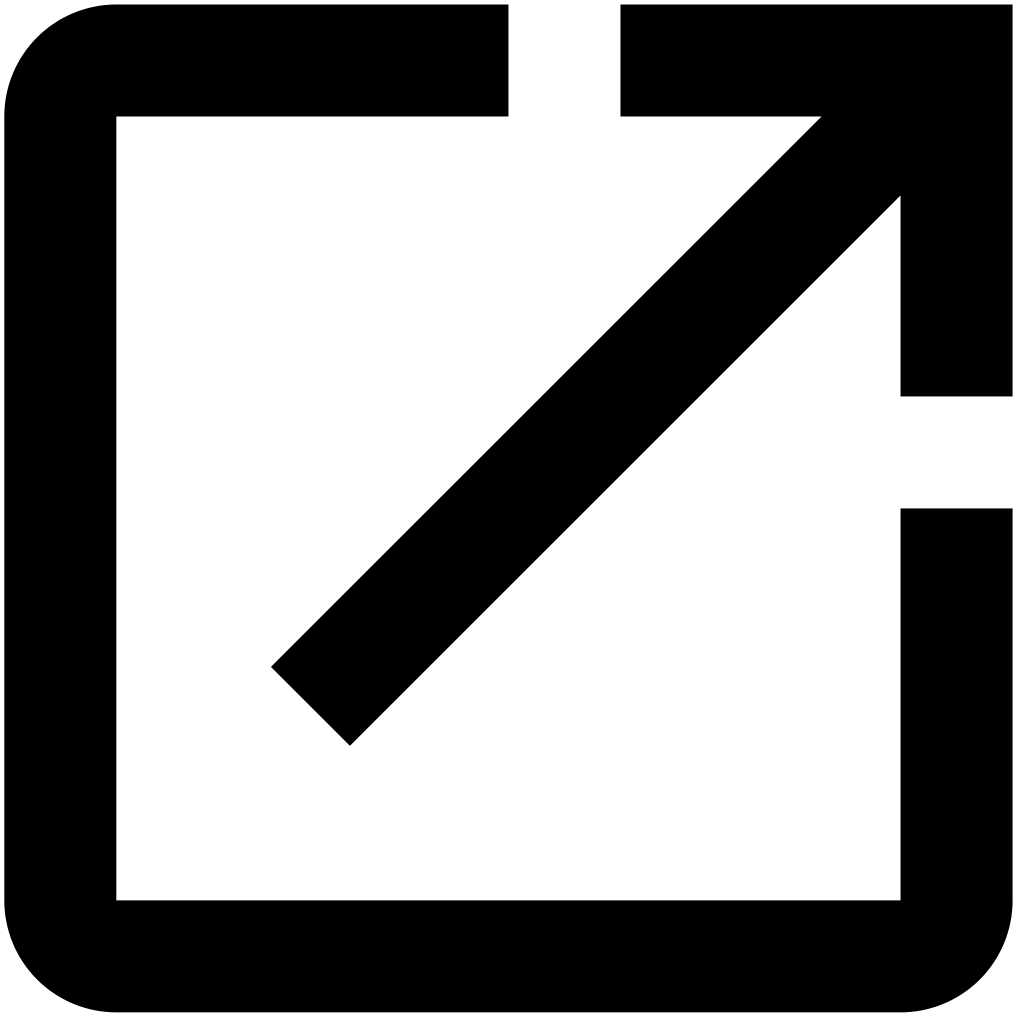
Published: 2024-02-21 · Archived: 2026-04-05 14:12:31 UTC

The U.S. State Department is now also offering rewards of up to $15 million to anyone who can provide information about LockBit ransomware gang members and their associates.

$10 million is offered for information that could lead to locating or identifying LockBit leadership, and an extra $5 million is available for tips that could lead to the apprehension of LockBit ransomware affiliates.

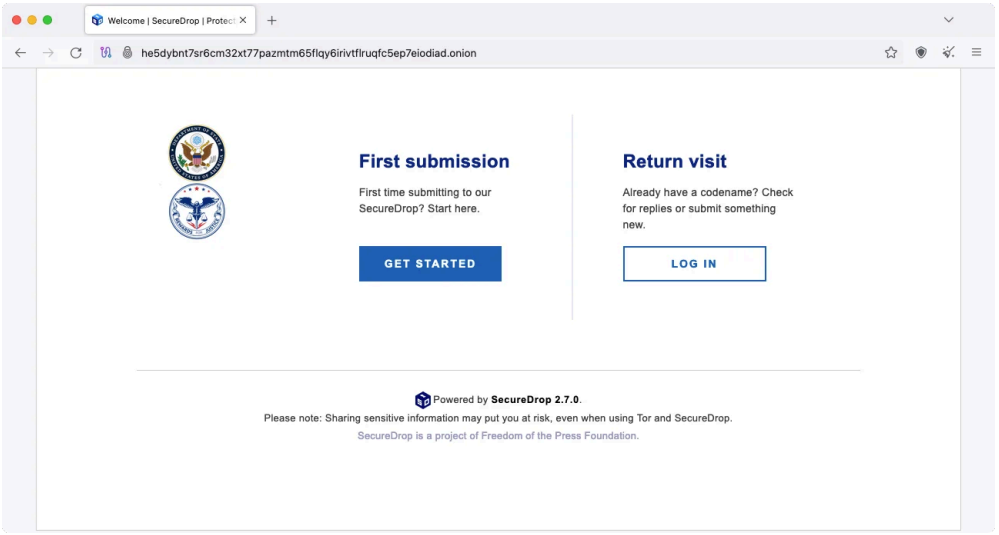
The U.S. Department of Justice linked the gang to over 2,000 victims and said it raked in more than $120 million after ransom demands totaling hundreds of millions of dollars.


DIE LINKE.
0:00



The rewards are provided via the Transnational Organized Crime Rewards Program (TOCRP), with the U.S. government having already paid more than $135 million for helpful tips since 1986.

The State Department has a dedicated Tor SecureDrop server that can be used to anonymously submit tips on LockBit and other wanted threat actors.



U.S. State Department Secure Drop page (BleepingComputer)

"The Department of State is announcing reward offers totaling up to $15 million for information leading to the arrest and/or conviction of any individual participating in a LockBit ransomware variant attack and for information leading to the identification and/or location of any key leaders of the LockBit ransomware group," U.S. State Department Spokesperson Matthew Miller said today.

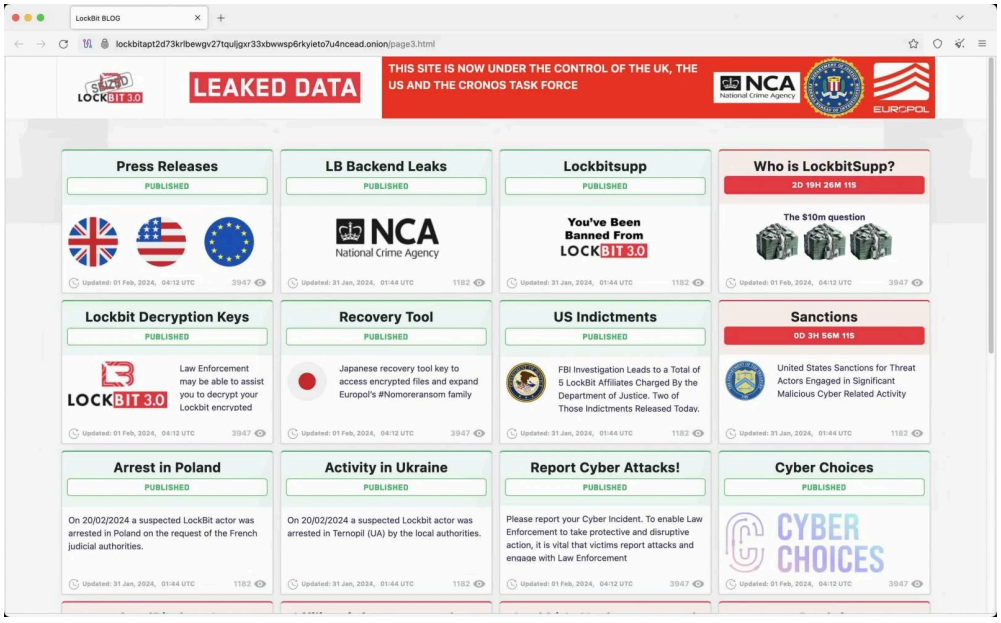
"Since January 2020, LockBit actors have executed over 2,000 attacks against victims in the United States, and around the world, causing costly disruptions to operations and the destruction or exfiltration of sensitive information.

"More than $144 million in ransom payments have been made to recover from LockBit ransomware events."

LockBit down after law enforcement crackdown

LockBit ransomware's infrastructure was seized this Tuesday after its dark web leak sites were taken down on Monday in a global law enforcement operation codenamed Operation Cronos that started months ago and was led by the U.K.'s National Crime Agency (NCA).

Police officials released a free LockBit 3.0 Black Ransomware decryptor on the 'No More Ransom' portal, developed using over 1,000 decryption keys retrieved from LockBit's seized servers.



LockBit leak site after seizure (BleepingComputer)

Two LockBit affiliates were arrested in Poland and Ukraine, while French and U.S. judicial authorities issued three international arrest warrants and five indictments against other LockBit threat actors.

The U.S. Justice Department also unsealed two of the indictments this week against two Russian suspects, Artur Sungatov and Ivan Gennadievich Kondratiev (aka Bassterlord), charging them for their alleged involvement in LockBit attacks.

In total, police seized 34 Lockbit servers worldwide and over 200 crypto-wallets used by the gang to collect ransom payments.

Law enforcement released additional information today on the group's dark web leak site, revealing that LockBit had employed 188 affiliates over time. However, no details are available regarding the number of active affiliates at the time of the crackdown

The LockBit ransomware-as-a-service (RaaS) operation emerged in September 2019 and was the longest-running before being taken down this week.

Since it surfaced, LockBit has claimed attacks on many large-scale and government organizations worldwide, including Boeing, the Continental automotive giant, the UK Royal Mail, and the Italian Internal Revenue Service.

Most recently, Bank of America warned customers of a data breach after its Infosys McCamish Systems (IMS) service provider got hacked in an attack claimed by LockBit.
