Interpol: Lockbit ransomware attacks affecting American SMBs

By Sergiu Gatlan

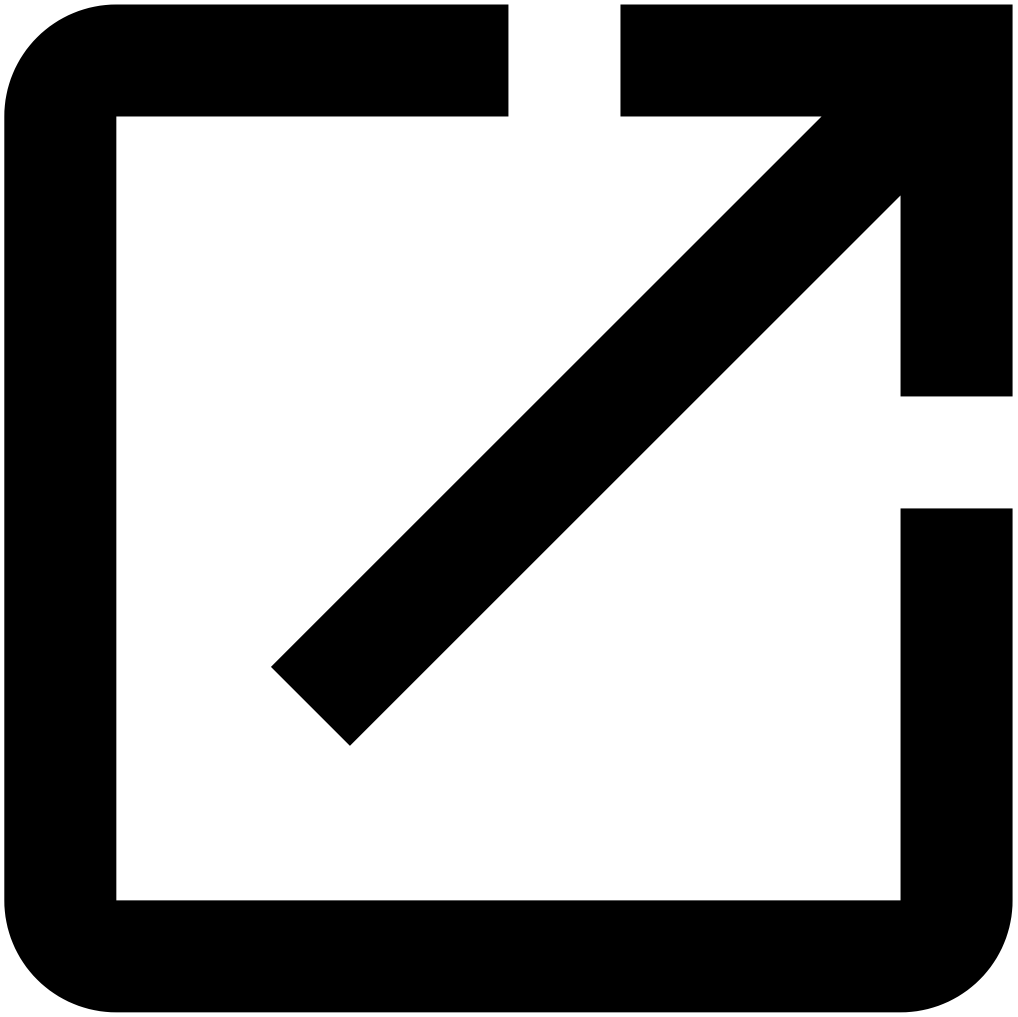
Published: 2020-08-04 · Archived: 2026-04-05 13:28:49 UTC

American medium-sized companies are actively targeted by LockBit ransomware operators according to an Interpol report on the impact the COVID-19 pandemic had on cybercrime around the world.

The report was produced by Interpol's Cybercrime Directorate and it includes data from 48 Interpol member countries and 4 private partners, as well as info and analysis from Interpol's Cybercrime Threat Response (CTR) unit and its Cyber Fusion Centre (CFC).

"The resulting analysis was supplemented by information provided by private sector partners and the INTERPOL Regional Working Groups on Cybercrime," the Interpol says.


DIE LINKE.
0:00



American SMBs in LockBit's line of fire

As part of a short summary of regional cybercrime trends, the International Criminal Police Organization (Interpol) says [PDF] that "a ransomware campaign carried out mainly through LOCKBIT malware is currently affecting medium-sized companies in some countries within this region."

LockBit, a human-operated Ransomware-as-a-Service (RaaS) operation that surface in September 2019 as a private operation targeting enterprises and later observed by Microsoft while targeting healthcare and critical services.

This ransomware strain's operators use the publicly available CrackMapExec penetration testing tool to move laterally once they get a foothold on a victim's network.

Two months ago, LockBit partnered with Maze ransomware's operators to create an extortion cartel that allows them to share the same data leak platform during their operations and to exchange tactics and intelligence.

Maze later told BleepingComputer that other ransomware groups might join this collaborative effort to generate ransom payments.

Most active ransomware strains during the pandemic

Interpol also took a closer look at data provided by private partners to get an overview of the most aggressive ransomware gangs during the pandemic.

Based on their analysis, CERBER, NetWalker, and Ryuk were the top ransomware families recently detected by Interpol private partners and they are seen as "constantly evolving to maximize the potential damage of a single attack as well as the financial profit for its perpetrators."

"In the first two weeks of April 2020, there was a spike in ransomware attacks by multiple threat groups which had been relatively dormant for the past few months," the Interpol added.

"This implies that there may still be organizations that have been infected but where the ransomware has not yet been activated."

On a related note, Interpol mentioned the Emotet botnet (known as a ransomware infection vector) in the data harvesting malware part of the report, with 13% of organizations being affected by this malware globally.

Ransomware operators are also targeting European healthcare institutions and critical infrastructure involved in COVID-19 response according to Interpol's report.

The international police organization previously warned in April about a surge of ransomware attacks targeting hospitals and attempting to lock them out of critical systems even though most of them were already overwhelmed by the influx of patients caused by the ongoing pandemic.

Ransomware defense measures

Interpol recommends organizations exposed to ransomware attacks to keep their software and hardware up to date, and to back up their data using offline storage devices to block ransomware operators from accessing and encrypting them.

The police organization also advises orgs to take the following defense measures to protect their systems:

• Only open emails or download software/applications from trusted sources;
• Do not click on links or open attachments in emails which you were not expecting to receive, or come from an unknown sender;
• Secure email systems to protect from spam which could be infected;
• Backup all important files frequently, and store them independently from your system (e.g. in the cloud, on an external drive);

• Ensure you have the latest anti-virus software installed on all systems and mobile devices, and that it is constantly running;
• Use strong, unique passwords for all systems, and update them regularly.

Source: https://www.bleepingcomputer.com/news/security/interpol-lockbit-ransomware-attacks-affecting-american-smbs/