

LOCKBIT

The most prolific ransomware brand of the past decade, running since 2019 with a Fortune 500-studded victim list. Survived an international law enforcement takedown in 2024 and returned within months as LockBit 5.0, now climbing back toward the top of the leaderboard.

ABCD (original 2019 name)

LockBit Black (3.0)

LockBit 5.0 "ChuongDong"

Windows/Linux/ESXi

RISK RATING

Critical

ACTIVE SINCE

2019

BUSINESS MODEL

RaaS, \$500 affiliate entry fee

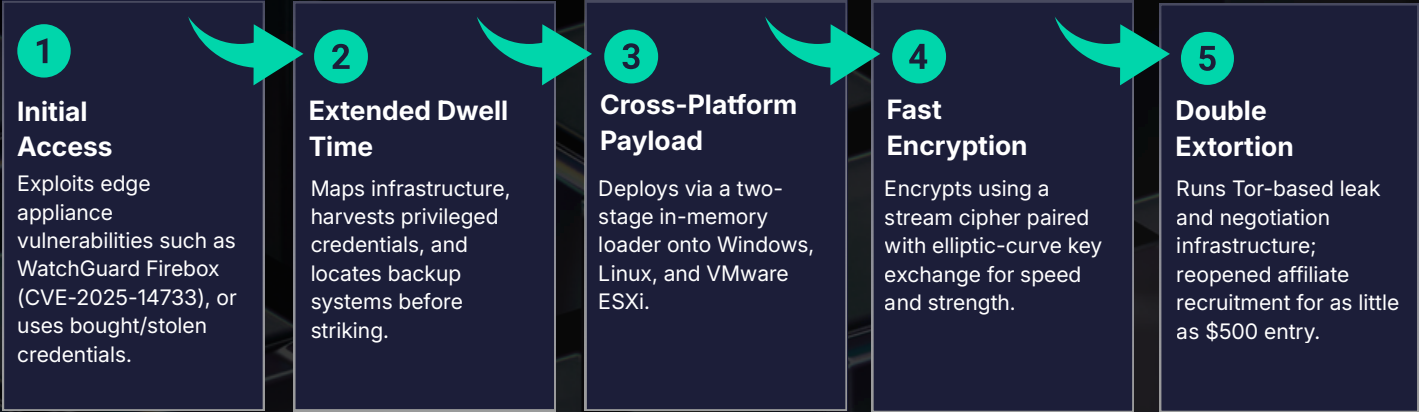
PRIMARY VECTOR

WatchGuard Firebox, edge CVEs

2026 STANDING

335+ victims since Dec 2025 relaunch

ATTACK CHAIN



MITRE ATT&CK MAPPING

ID	TECHNIQUE
T1190	Exploit public-facing application (WatchGuard Firebox, edge appliances)
T1078	Valid accounts (stolen or purchased credentials)
T1003	OS credential dumping (privileged credential harvesting)
T1489	Service stop (targets backup infrastructure directly)
T1486	Data encrypted for impact (stream cipher + ECC key exchange)
T1567	Exfiltration over web service (StealBit data-theft tooling)

SECTOR BY SECTOR Summary



Manufacturing

The most-hit sector under LockBit 5.0, continuing a pattern that has held since the group's earliest versions.



Professional Services

A close second, reflecting the group's long-standing preference for firms holding client access and sensitive records.



Technology

Rounds out its top three, alongside a historic victim list that includes Boeing and Accenture.

ORIGIN & EVOLUTION

The most prolific ransomware brand of the past decade, running since 2019 with a Fortune 500-studded victim list. Survived an international law enforcement takedown in 2024 and returned within months as LockBit 5.0, now climbing back toward the top of the leaderboard.

THREAT LANDSCAPE CONTEXT

The only actor in this series with a named, sanctioned administrator, Dmitry Khoroshev (LockBitSupp), publicly identified and OFAC-sanctioned in May 2024. Several affiliates defected to ALPHV and RansomHub after the Cronos takedown, yet the brand rebuilt fast enough to reclaim a top-five spot within two years.

SIGNATURE TRADecraft

Exploits edge appliance vulnerabilities such as WatchGuard Firebox, or uses bought/stolen credentials, then maps infrastructure and locates backup systems before striking. Deploys via a two-stage in-memory loader onto Windows, Linux, and VMware ESXi, encrypting with a stream cipher paired with elliptic-curve key exchange for speed and strength.

ANALYST OUTLOOK

LockBitSupp's OFAC sanction creates real legal exposure for any victim considering payment, a deterrent none of the other nine actors carry. Given the brand's history of rebuilding after disruption, expect LockBit 5.0 to keep climbing the leaderboard rather than fade a second time.

NOTABLE INCIDENTS

Boeing

2023

One of the group's most prominent historic victims, cited across nearly every LockBit retrospective as evidence of its Fortune-500 reach at peak activity.

Operation Cronos

February 2024

International law enforcement seized LockBit's servers and publicly leaked working decryption keys; LockBitSupp later published an unusually candid admission that a personal failure to patch a known PHP vulnerability had enabled the takedown.

SCB Group, Singapore

February 2024

Claimed a double-extortion attack on the Singaporean construction firm under the LockBit 5.0 brand, evidence that the comeback is landing real victims, not just relaunching infrastructure.