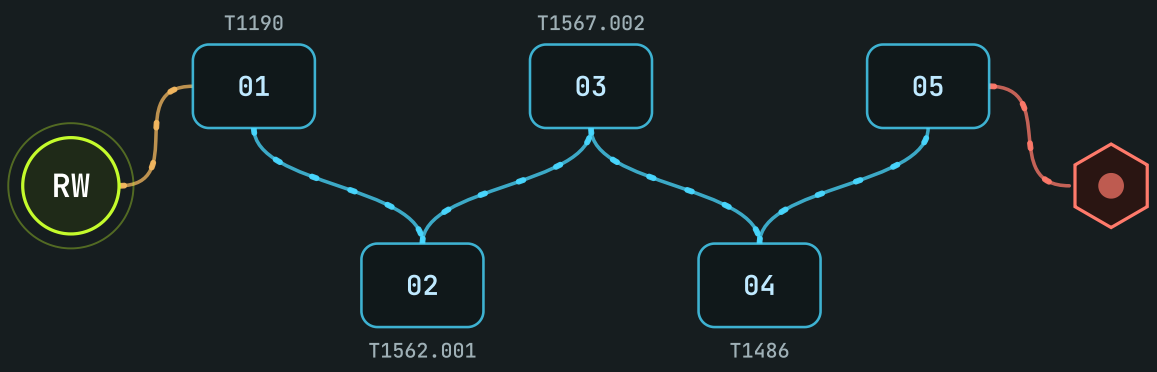


INTELLIGENCE BRIEF

LockBit is back as LockBit 5.0 and ranked fourth on leak sites in early 2026

Taken down in February 2024, LockBit relaunched as LockBit 5.0 in September 2025 with Windows, Linux and ESXi encryptors and posted 163 victims in Q1 2026. Patch edge devices and protect hypervisors now.

EDITION
Fall/Winter 2026/2027 Edition
RW-03 · Ransomware group

PUBLISHED BY
Z7 Solutions LLC
Orlando, Florida

READ ONLINE
z7solutions.com
844-974-8669

01 At a glance

STATUS

ACTIVE

Relaunched as LockBit 5.0 in September 2025 and ranked fourth worldwide by leak-site victims in the first quarter of 2026, although still far below the 20 to 30 percent of postings it held before the February 2024 takedown. [1]

HEADLINE NUMBERS

163

victims posted by LockBit in Q1 2026, up from 79 in Q4 2025 (Check Point) [1]

7,000+

attacks built with LockBit services, June 2022 to February 2024 (NCA) [11]

$500M+

ransom payments LockBit is alleged to have received, per US Treasury [10]

$10M

maximum US reward for information leading to Khoroshev's arrest and/or conviction [10]

KEY FACTS

INITIAL ACCESS

Vulnerability exploitation, brute-force attempts, phishing and leaked or stolen credentials (Halcyon, July 2026) [6]

PLATFORMS HIT

Windows, Linux and VMware ESXi variants [2]

AFFILIATE ENTRY

About $500 in Bitcoin as a deposit for panel and encryptor access [3]

LEADER

Dmitry Yuryevich Khoroshev (LockBitSupp), US indicted, sanctioned by the US, UK and Australia, US reward of up to $10 million [10]

EXTORTION

Leak threat backed by a personalized negotiation link with a 30-day deadline before stolen data is published [3]

02 What happened

LockBit was the most dominant ransomware-as-a-service operation until Operation Cronos, led by the UK National Crime Agency and the FBI, seized its infrastructure on February 19, 2024 and later unmasked its leader. The brand lost ground after the takedown, was itself hacked in May 2025, and then relaunched as LockBit 5.0 in September 2025. By the first quarter of 2026 it was again one of the most active leak-site posters.

- Before the takedown LockBit accounted for 20 to 30 percent of all data-leak-site victim postings according to Check Point, and Treasury says it targeted more than 2,500 victims worldwide and is alleged to have received more than $500 million in ransom payments.
- Operation Cronos took down 28 affiliate servers, froze more than 200 cryptocurrency accounts, obtained the platform's source code and led to arrests in Poland and Ukraine; later phases added four more arrests, sanctions on Evil Corp member Aleksandr Ryzhenkov as a LockBit affiliate, and in February 2025 Treasury sanctions on the Zservers bulletproof host.
- On May 7, 2024 authorities named Dmitry Khoroshev as LockBitSupp: the US, UK and Australia sanctioned him, the US unsealed a 26-count indictment with a 185-year maximum sentence, and a reward of up to $10 million was announced.
- On May 7, 2025 BleepingComputer reported that LockBit's affiliate panels had been defaced and a MySQL database leaked, exposing 59,975 Bitcoin addresses, 4,442 negotiation messages and 75 panel accounts with plaintext passwords.
- LockBit 5.0 appeared in early September 2025 with Windows, Linux and ESXi variants, and Trend Micro found it shares hashing and API-resolution code with LockBit 4.0; Check Point counted 163 victims posted by LockBit in Q1 2026, up 106 percent from 79 in Q4 2025, placing it fourth worldwide.
- DragonForce announced a supposed coalition with Qilin and LockBit in September 2025, and ReliaQuest expected it to share techniques and infrastructure, but Check Point calls the declarations largely symbolic and Halcyon says no combined leak site or joint attacks have been confirmed.

03 How it works

01 Get in through edge devices and logins

MITRE ATT&CK T1190

CISA lists exploitation of public-facing applications, external remote services, valid accounts and phishing as LockBit affiliate entry points. The late-2023 Citrix Bleed campaign is the best-documented example: LockBit 3.0 affiliates used it against Boeing's parts and distribution business, and a researcher reported an unpatched NetScaler at ICBC. An unpatched NetScaler let attackers bypass passwords and MFA by hijacking sessions.

02 Turn off defenses and wipe tracks

MITRE ATT&CK T1562.001

The LockBit 5.0 Windows loader decrypts its payload in memory, patches the EtwEventWrite API to blind telemetry, terminates security services matched against a hardcoded list of 63 hashed names, and clears all Windows event logs after encryption.

03 Steal data to back the ransom demand

MITRE ATT&CK T1567.002

Affiliates exfiltrate victim data with LockBit's StealBit tool and with Rclone and file-sharing services such as MEGA, so that a leak threat backs the ransom demand (CISA, 2023). Operation Cronos showed the group kept victim data even after payment.

04 Encrypt Windows, Linux and ESXi

MITRE ATT&CK T1486

LockBit 5.0 has Windows, Linux and VMware ESXi variants; files get randomized 16-character extensions and the malware exits on Russian-language systems. In its first look at about a dozen victims in September 2025, Check Point observed roughly 80 percent of attacks on Windows and 20 percent on ESXi and Linux.

05 Extort on a 30-day clock

Ransom notes now name LockBit 5.0 and carry a personalized Tor negotiation link with a 30-day deadline before stolen data is published on the leak site.

04 Who is at risk

Any organization with an unpatched internet-facing appliance, exposed remote access or a VMware ESXi estate is in scope, and Halcyon says LockBit 5.0 affiliate rules explicitly permit attacks on critical infrastructure and medical facilities.

- Business services lead LockBit 5.0 victim claims, followed by manufacturing, technology and healthcare, according to Halcyon.
- The United States leads cumulative claims, but Check Point puts it at 21.2 percent of LockBit's Q1 2026 victims against more than 50 percent historically, with Italy and Brazil at 8.6 percent each and Turkey at 5.1 percent.
- Organizations running VMware ESXi face an encryptor that Trend Micro says is designed to encrypt entire virtual machine infrastructures in a single attack.
- Local governments and courts remain exposed: LockBit's attack on Fulton County, Georgia in early 2024 disrupted county phones, internet access and its court system, and officials said no ransom was paid.
- Large firms and defense suppliers are proven targets: LockBit 3.0 affiliates used Citrix Bleed against Boeing's parts and distribution business, and Treasury links the November 2023 attack on ICBC's US broker-dealer to LockBit.

Sectors in scope: business services, manufacturing, technology, healthcare, financial services, aerospace and defense, state and local government.

05 What changed since the last edition

EACH CHANGE WITH ITS SOURCE

01 LockBit relaunched as LockBit 5.0. The administrator announced it on the RAMP forum in early September 2025, on the operation's sixth anniversary, and asked new affiliates for a Bitcoin deposit of roughly $500. Check Point describes it as an upgraded evolution of LockBit 4.0 with Windows, Linux and ESXi variants.

SOURCE 4

02 Leak-site activity rebounded. Check Point counted 163 victims posted by LockBit in Q1 2026 (85 in January, 33 in February, 45 in March), up 106 percent from 79 in Q4 2025, which lifted it from outside the top 10 to fourth place globally, just behind The Gentlemen with 166.

SOURCE 1

03 Mid-2026 momentum is unsettled. Halcyon's profile, updated July 27, 2026, says activity declined through spring before a June 2026 resurgence on the 5.0 leak site, up more than 500 percent month over month and ongoing as of July; the same page also says activity peaked in Q1 and tapered afterward.

SOURCE 6

04 DragonForce announced a supposed coalition with Qilin and LockBit on the RAMP forum in September 2025. Check Point calls these declarations largely symbolic, with no verified evidence of shared infrastructure or joint operations.

SOURCE 4

05 LockBit was hacked. On May 7, 2025 its affiliate panels were defaced with the message 'Don't do crime CRIME IS BAD xoxo from Prague' and a MySQL dump leaked 59,975 Bitcoin addresses, affiliate builds, 4,442 negotiation messages dated December 19 to April 29, and 75 user accounts with plaintext passwords; LockBitSupp confirmed the breach but said no private keys were leaked or data lost.

SOURCE 8

06 Prosecutions advanced. Rostislav Panev, a 51-year-old dual Russian and Israeli national accused of helping develop LockBit, was arrested in Israel in August 2024 and extradited to the United States, as the Justice Department announced in March 2025; SecurityWeek reported at that time that Khoroshev and others remained at large, with rewards of up to $10 million.

SOURCE 9

07 Sanctions advanced. Treasury sanctioned the Russia-based bulletproof host Zservers and two administrators on February 11, 2025 for leasing IP addresses to LockBit affiliates, and said in the same release that LockBit was responsible for the November 2023 attack on ICBC's US broker-dealer.

SOURCE 16

08 The 'operating at 73 percent reduced capacity with 69 affiliates' framing is out of date. Those were NCA figures from May 2024: average monthly LockBit attacks in the UK down 73 percent and active affiliates down to 69 since the February 2024 action. Check Point ranked LockBit fourth worldwide in Q1 2026, although far below the 20 to 30 percent of postings it held before Cronos.

SOURCE 11

06 What to do now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Patch or isolate internet-facing appliances (NetScaler, VPN gateways, firewalls, remote management tools) within 24 to 48 hours of a CISA Known Exploited Vulnerabilities listing.**

LockBit 3.0 affiliates used Citrix Bleed to bypass passwords and MFA on unpatched NetScaler appliances, including at Boeing Distribution, and CISA lists exploitation of public-facing applications as a LockBit entry point.

02 **Enforce phishing-resistant MFA on VPN, remote desktop, email and every administrative account, and restrict RDP to a jump host.**

Valid accounts, phishing and external remote services are documented LockBit entry points; phishing-resistant MFA blunts credential theft, while session-hijacking flaws such as Citrix Bleed also require fast patching.

03 **Keep offline, immutable backups that include hypervisor-level copies of virtual machines, and test a full restore each quarter.**

LockBit 5.0 ships an ESXi encryptor, so a backup that lives on the same virtual estate is not a backup.

04 **Lock down VMware ESXi and other hypervisor management interfaces: no internet exposure, separate admin credentials, and alerts on unexpected VM shutdowns or file renames.**

Check Point's early sample put about one in five LockBit 5.0 attacks on ESXi or Linux, and Trend Micro says the ESXi encryptor is built to encrypt entire virtual machine infrastructures in one attack.

05 **Run EDR with tamper protection on every server and endpoint, and alert on mass service termination, ETW patching and event log clearing.**

Trend Micro documents ETW patching and security-service termination in the loader and event log clearing after encryption, so these behaviors can give early warning.

06 **Decide your ransom policy before an incident, with counsel and an OFAC sanctions check, and assume stolen data will be published whether or not you pay.**

LockBit's leader is a sanctioned person, and Operation Cronos showed the group kept victim data it had promised to delete.

07 Segment networks and monitor for lateral movement over RDP and SMB, mass file access and large outbound transfers to cloud storage.

LockBit affiliates exfiltrate data with tools such as StealBit, Rclone and MEGA, activity a 24/7 SOC can detect; Z7 Solutions™ provides that monitoring for mid-size organizations, school districts and public agencies.

07 Indicators

Indicators the sources publish, as they print them. Hunt with them, and check the source before you block.

BEHAVIOR	Encrypted files renamed with randomized 16-character extensions; no traditional infection marker at end of file [2]
BEHAVIOR	EtwEventWrite API patched with a return instruction, then security services terminated against a hardcoded list of 63 hashed service names [2]
BEHAVIOR	All Windows event logs cleared via EvtClearLog after encryption completes [2]
BEHAVIOR	Process exits when Russian language settings or Russian geolocation are detected [2]
BEHAVIOR	Ransom note names LockBit 5.0 and includes a personalized Tor negotiation link with a 30-day publication deadline [3]

08 Sources

[1] **The State of Ransomware, Q1 2026** Check Point Research · May 11, 2026. https://research.checkpoint.com/2026/the-state-of-ransomware-q1-2026/

[2] **New LockBit 5.0 Targets Windows, Linux, ESXi** Trend Micro (Trend Research) · September 25, 2025. https://www.trendaisecurity.com/en-us/resources-insights/trendai-security-blog/lockbit-5-targets-windows-linux-esxi

[3] **LockBit Returns, and It Already Has Victims** Check Point Research · October 23, 2025. https://blog.checkpoint.com/research/lockbit-returns-and-it-already-has-victims/

[4] **The State of Ransomware, Q3 2025** Check Point Research · November 13, 2025. https://research.checkpoint.com/2025/the-state-of-ransomware-q3-2025/

[5] **LockBit, Qilin, and DragonForce Join Forces to Dominate the Ransomware Ecosystem (reporting the ReliaQuest Q3 2025 ransomware report)** The Hacker News · October 8, 2025. https://thehackernews.com/2025/10/lockbit-qilin-and-dragonforce-join.html

[6] **Threat group profile: LockBit (5.0)** Halcyon · updated July 27, 2026. https://www.halcyon.ai/threat-group/lockbit

[8] **LockBit ransomware gang hacked, victim negotiations exposed** BleepingComputer · May 7, 2025. https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-hacked-victim-negotiations-exposed/

[9] **LockBit Ransomware Developer Extradited to US (reporting the DOJ District of New Jersey release)** SecurityWeek · March 14, 2025. https://www.securityweek.com/lockbit-ransomware-developer-extradited-to-us/

[10] **Treasury sanctions LockBit leader Dmitry Yuryevich Khoroshev (press release jy2326)** U.S. Department of the Treasury · May 7, 2024. https://home.treasury.gov/news/press-releases/jy2326

[11] **LockBit leader unmasked and sanctioned** UK National Crime Agency · May 7, 2024. https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned

[12] **Russian charged with LockBit ransomware crimes, $10 million reward for his arrest (reporting the DOJ indictment)** NBC News · May 7, 2024. https://www.nbcnews.com/tech/security/russian-charged-lockbit-ransomware-crimes-10-million-reward-arrest-rcna151116

[13] **International investigation disrupts the world's most harmful cyber crime group** UK National Crime Agency · February 20, 2024. https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group

[14] **Four Individuals Connected to LockBit Ransomware Attacks Arrested; Evil Corp Members Sanctioned (reporting Europol and NCA phase three of Operation Cronos)** HIPAA Journal · October 3, 2024. https://www.hipaajournal.com/lockbit-ransomware-arrests-evil-corp-sanctions/

[15] **Treasury sanctions Evil Corp members including Aleksandr Ryzhenkov (press release jy2623)** U.S. Department of the Treasury · October 1, 2024. https://home.treasury.gov/news/press-releases/jy2623

[16] **Treasury sanctions Zservers, a Russia-based bulletproof hosting provider supporting LockBit (press release sb0018)** U.S. Department of the Treasury · February 11, 2025. https://home.treasury.gov/news/press-releases/sb0018

[17] **Russian Court Indicts Alleged Ransomware Hacker Wanted by the FBI** BankInfoSecurity · December 2, 2024. https://www.bankinfosecurity.com/russian-court-indicts-ransomware-hacker-wanted-by-fbi-a-26948

[18] **#StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability (AA23-325A)** CISA, FBI, MS-ISAC and ASD ACSC · November 21, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a

[19] **Understanding Ransomware Threat Actors: LockBit (AA23-165A)** CISA, FBI, MS-ISAC and international partners · June 14, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

[20] **LockBit ransomware leaks gigabytes of Boeing data** BleepingComputer · November 12, 2023. https://www.bleepingcomputer.com/news/security/lockbit-ransomware-leaks-gigabytes-of-boeing-data/

[21] **Royal Mail cyberattack linked to LockBit ransomware operation** BleepingComputer · January 12, 2023. https://www.bleepingcomputer.com/news/security/royal-mail-cyberattack-linked-to-lockbit-ransomware-operation/

[22] **Fulton County, Security Experts Call LockBit's Bluff** Krebs on Security · February 29, 2024. https://krebsonsecurity.com/2024/02/fulton-county-security-experts-call-lockbits-bluff/

[23] **Adverse cyber extortions are more common than commonly advised (Q2 2026 quarterly report)** Coveware by Veeam · July 29, 2026. https://coveware.com/2026/07/adverse-cyber-extortions-are-more-common-than-commonly-advised/

[25] **FinCEN says ransomware gangs extorted over $2.1B from 2022 to 2024 (reporting the FinCEN Financial Trend Analysis)** BleepingComputer · December 8, 2025. https://www.bleepingcomputer.com/news/security/fincen-says-ransomware-gangs-extorted-over-21b-from-2022-to-2024/

[26] **Dark Web Profile: LockBit 3.0 Ransomware** SOCRadar · updated September 30, 2026. https://socradar.io/blog/dark-web-profile-lockbit-3-0-ransomware/

[27] **LockBit 5.0: The RaaS That Refuses to Go Away** Arete · January 20, 2026. https://areteir.com/resources/lockbit-5-0-ransomware-threat-resurgence

[28] **The State of Ransomware, Q2 2026** Check Point Research · August 13, 2026. https://research.checkpoint.com/2026/the-state-of-ransomware-q2-2026/

[29] **Chinese multinational bank hit by ransomware** Help Net Security · November 10, 2023. https://www.helpnetsecurity.com/2023/11/10/china-bank-ransomware/

NEXT STEP

Put the same team on your environment

Talk to the team that runs the Z7 Solutions SOC about what this brief means for your environment. We will tell you what applies and what does not.

ALSO IN THIS EDITION

- Qilin still tops most ransomware counts
  More from the edition · z7solutions.com/z7-cyber/qilin/
- Qilin still hits hospitals and infrastructure
  More from the edition · z7solutions.com/z7-cyber/qilin-part-2/
- Akira still exploits SonicWall VPNs in 2026
  More from the edition · z7solutions.com/z7-cyber/akira-ransomware/

CALL	844-974-8669
EMAIL	sales@z7solutions.com
BOOK A CALL	z7solutions.com/book/

Z7 Solutions™, Z7-Claw™ and Z7-Guard™ are trademarks of Z7 Solutions LLC.