THREAT BULLETINS

New LockBit Ransomware Emerges as Most Dangerous Yet

TLP:WHITE

Oct 01, 2025

Health-ISAC, in cooperation with intelligence partners, received information concerning the recently released LockBit 5.0 ransomware variant.

The variant represents an evolutionary risk to organizations due to a new focus on directly targeting virtual environments, improved and enhanced technical capabilities, evasion techniques, and affiliate engagement.

Health-ISAC provides this information to increase situational awareness and recommends that members assess their level of risk to this recent development.

Analysis

LockBit 5.0 is the latest iteration of the ransomware-as-a-service (RaaS) group, posing an elevated risk for organizations due to enhanced capabilities targeting Windows, Linux, and VMware ESXi environments. Additionally, the variant has improved technical capabilities that make it faster, more flexible for affiliates, and harder for security solutions to detect and analyze, demanding immediate security posture assessment and enhancement.

Following law enforcement disruption by Operation Cronos in early 2024, the LockBit group resurfaced in September 2025. This marks its sixth anniversary with a continuing cross-platform attack strategy that includes the ability to target and encrypt entire virtual infrastructures as well as provide a more advanced payload featuring DLL reflection, anti-analysis techniques, randomized file extensions, security service termination and operational flexibility.

Analysis reveals significant code reuse between LockBit 4.0 and 5.0, with both versions sharing identical hashing algorithms for string operations and similar code structures for dynamic API resolution. This confirms that this represents the evolutionary development of the existing codebase rather than an imitation by different threat actors.

The new variant confirms LockBit's resilience despite law enforcement actions. It demonstrates the group's continued commitment to staying ahead of competitors through aggressive technical evolution. The new variant poses an even more significant potential threat to enterprise operations and requires security posture enhancement through improved mitigation efforts using layered defenses, proactive threat hunting, and updated detection signatures aligned with known Indicators of Compromise.

New and Notable Capabilities

- Cross-Platform Attack Infrastructure: Windows, Linux and a dedicated ESXi binary with platform-specific CLI options confirms the group's continued cross-platform strategy that enables simultaneous attacks across entire enterprise networks from workstations to critical servers hosting databases to now virtualization platforms.
- ESXi-focused options: ESXi parameters and faster/more effective VM/VMFS encryption demonstrates a focus on maximizing impact through virtualization infrastructure, where a single compromised ESXi host can result in dozens or hundreds of encrypted virtual machines, significantly amplifying the attack's business disruption potential.
- Advanced Obfuscation and Evasion: The Windows version employs heavy obfuscation through packing, functioning as a binary loader that decrypts a PE binary in memory and loads it via DLL reflection

methods, significantly complicating static analysis, as well as patching of the EtwEventWrite API by overwriting it with a 0xC3 return instruction to disable Windows Event Tracing capabilities.

- Improved User Interface and Flexibility: Features a more user-friendly “help”/CLT interface with clean formatting compared to previous versions, providing detailed commands and parameters that illustrate significant flexibility and customization available to attackers (including command-line configurable options and modes (basic director specifications, invisible/verbose, filtering/exclusions, timeout, wipe free space, encryption and notes settings) that illustrates maturity and focused affiliate usability.
- Enhanced Encryption Techniques: The encryption process appends randomized 16-character extensions to files, complicating recovery efforts, while unlike some ransomware variants that use common infection markers omits traditional markers at file endings
- Anti-Forensics Capabilities: The malware terminates security-related services by comparing hashed service names against a hardcoded list of 63 values, then clears all event logs using the EvtClearLog API after encryption completion.
- Geopolitical Safeguards: Consistent with previous versions includes geopolitical safeguards, terminating execution when detecting Russian language settings or Russian geolocation, a common practice among Eastern European ransomware groups.

Targeting and Victimology Insight

- Industries with high-value data and significant virtualized infrastructure remain top targets, with the inclusion of a dedicated ESXi locker indicating a strong focus on large enterprises in sectors like technology, healthcare, finance, manufacturing, and government as well as cloud providers.
- Enterprise environments with consolidated virtualization (hosting providers, finance, retail, large SaaS/ISV customers, healthcare and education) are high value because one ESXi host can contain many critical workloads.
- Avoidance of Russian-language systems suggests geopolitical targeting preferences, with the US, India, and Brazil looked at as primary geographic targets.
- Organizations with exposed or poorly controlled RDP/remote access, weak credentials, or gaps in patching and segmentation remains at

elevated risk; previous LockBit activity demonstrates opportunistic targeting across many sectors.
- The manufacturing industry is often targeted because organizations in this sector don't always have the strongest cybersecurity, and any disruption can have major implications for other businesses and supply chains.
- Cross-platform capabilities of LockBit 5.0 expand the potential victim pool to include any organization running Windows, Linux, or ESXi systems regardless of industry vertical.

Known Indicators of Compromise

File Hash (SHA256) Indicators:

- Windows variants - detected as Ransom.Win64.LOCKBIT.YXFIOZ
  - 7ea5afbc166c4e23498aa9747be81ceaf8dad90b8daa07a6e4644dc7c2277b82
  - 180e93a091f8ab584a827da92c560c78f468c45f2539f73ab2deb308fb837b38
- Linux variants - detected as Ransom.Linux.LOCKBIT.THIBCBD and Ransom.Linux.LOCKBIT.THIBEBD
  - 4dc06ecee904b9165fa699b026045c1b6408cc7061df3d2a7bc2b7b4f0879f4d
  - 90b06f07eb75045ea3d4ba6577afc9b58078eafeb2cdd417e2a88d7ccf0c0273
  - 98d8c7870c8e99ca6c8c25bb9ef79f71c25912fbb65698a9a6f22709b8ad34b6

Behavioral and Network Indicators:

- Ransom note files named "ReadMeForDecrypt.txt"
- Randomized 16-character hexadecimal extension (e.g., .[a-f0-9]{16}$/) appended to renamed encrypted files (instead of a fixed extension)
- Event log clearing activity post encryption via EvtClearLog API after encryption and ETW patching (i.e., traces of ETW patching and sudden log deletion are strong behavioral flags)
- Termination of security services by matching specific hashed service names (look for processes/services stopped shortly before encryption)
- ETW patching activity targeting EtwEventWrite API

- CLI/parameter usage patterns (presence of help output, -d, -b, -i, -m all|local|net, -n note modes, -t timeout) in execution logs or command history on infected hosts
- Victims are directed to dedicated leak sites maintained by LockBit infrastructure featuring victim interaction portals with “Chat with Support” sections for ransom negotiations

Recommended Mitigations

- Comprehensive Cross-Platform Defenses: Ensure complete defense-in-depth controls are in place focusing on protecting virtualization infrastructure and reinforcement of both endpoint and network protections with emphasis on early detection of defense evasion techniques aimed at compromising security solutions.
- Control Emphasis: Deploy endpoint detection and response (EDR) tools capable of identifying DLL reflection and obfuscation techniques, monitor for anomalous behavior in ESXi environments, implement behavioral detection capabilities that identify ransomware activity patterns rather than relying solely on signature-based detection.
- Protect ESXi /Virtualization Layers: Patch and harden ESXi hosts, restrict administrative access to hosts, restrict management interfaces to trusted networks, enable multifactor authentication for host access, isolate management networks from general VM networks, enhanced monitoring for ESXi command execution.
- Security Service Protection: Implement tamper-resistant security solutions that cannot be easily terminated through service manipulation, monitor for unauthorized service termination attempts.
- Credential Hygiene & Segmented Access: Tighten privileged account management, rotate credentials, remove unnecessary RDP exposure, enforce MFA on administrative interfaces, implement least privilege.
- Backups & Recovery: Ensure backups are offline/immutable and regular testing of full restores (including VM recovery), with awareness that Snapshotting alone is not a recovery panacea as ransomware often deletes snapshots requiring.
- Network segmentation & micro segmentation: Isolate critical systems (domain controllers, backup servers, ESXi hosts) and restrict lateral movement pathways.
- Event Logging Protection: Implement protected event logging solutions that cannot be cleared by compromised local administrators, ensuring forensic evidence preservation even if attackers attempt log deletion.

- Proactive Threat Hunting: Look for ETW API tampering, abrupt service terminations, sudden event log clearing, and signs of in-memory loaders and deploy EDR/EPP rules that detect ETW patching and suspicious DLL reflection/in-memory PE loading.
- Updated Threat Intelligence: Ingest vendor IOC feeds, run swift sweeping of endpoint, network, and cloud logs for behavioral IOCs, conduct regular tabletop exercises simulating ransomware scenarios.

Reference(s)	trendmicro, ibm, justice, cybelangel, reuters, treasury, flashpoint, listennotes, wikipedia, akamai, apple, justice 1, csoonline, trendmicro 1, infosecurity-magazine, petri, trendmicro 2, cisa

Alert ID 960f908e

View Alert

Share Feedback

was this helpful? |

Tags LockBit 5.0 Ransomware, LockBit

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**