AL2025_45 LockBit 5.0 Emerges- Cross Platform Ransomware Targets Windows, Linux and ESXi (September 30th , 2025)

Description

A new iteration of the LockBit ransomware marketed as **LockBit 5.0** has been observed in the wild. This variant includes cross-platform binaries (Windows, Linux, and VMware ESXi), heavier obfuscation and anti-analysis techniques, and faster/more efficient encryption routines. Researchers warn that LockBit 5.0 is positioned to increase impact on heterogeneous enterprise environments, particularly by targeting ESXi hosts and mixed OS estates.

Attack Details

- **Cross-platform capability:** LockBit 5.0 includes tooling and binaries for Windows, Linux, and ESXi, enabling single campaigns to encrypt servers and hypervisor VMs.
- **Evasion & obfuscation:** The sample exhibits advanced code obfuscation and anti-analysis checks intended to hinder detection and reverse engineering.
- **Faster encryption & modular design:** The ransomware's encryption routines are optimized for speed and can be deployed as modular components, increasing operational flexibility for affiliates.
- **Affiliate / RaaS model revival:** LockBit 5.0 appears tied to a renewed affiliate push (rebranded recruitment / portal activity), indicating attempts to rebuild a partner network despite prior disruptions.
- **Likely attack chain:** Initial access observed in prior LockBit campaigns (phishing, exposed RDP/VPN, compromised credentials, and exploitable internet-facing services) remains a common vector; once foothold achieved, lateral movement to backup and virtualisation hosts is prioritized.

Remediation

- Isolate and protect hypervisors: Ensure ESXi hosts are on a management network, restrict access, and harden management interfaces. Regularly patch hypervisor firmware and management tools.
- Patch and update: Apply vendor security updates promptly for OS, hypervisors, backup software, VPN/remote access appliances, and EDR/antivirus
- Harden remote access: Disable or tightly restrict RDP/SMB/VPN exposure to the internet; require strong authentication and network allow-lists or VPN gateways.

- Protect backups: Keep offline or air-gapped backups, restrict backup admin access, and test restoration procedures regularly. Ensure backups are immutable where possible.
- Increase detection & logging: Tune EDR and SIEM for suspicious file-system encryption activity, unusual process spawning, and lateral movement (SharpShares, RMM abuse indicators). Enable comprehensive logging for authentication, file changes, and hypervisor management.
- Network segmentation & least privilege: Segment critical services, limit lateral movement, and apply least privilege for service and admin accounts. Rotate and secure credentials; use MFA for all remote and privileged access.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Cardiet, L. (2025, September 12). LockBit is Back: What's New in Version 5.0. Vectra. Retrieved from https://www.vectra.ai/blog/lockbit-is-back-whats-new-in-version-5-0

- Solomon, H. (2025, September 26). Meet LockBit 5.0: Faster ESXi drive encryption, better at evading detection. CSO Online. Retrieved from https://www.csoonline.com/article/4064250/meet-lockbit-5-0-faster-esxi-drive-encryption-better-at-evading-detection.html