Alerta

Técnica

Vulnerabilidad detectada en Lockbit

COLCERT AL-20251002 - 076

TLP:CLEAR

LockBit 5.0 representa la evolución más reciente de una de las familias de ransomware más activas, incorporando mejoras en sus técnicas de evasión y ampliando su alcance a sistemas Windows, Linux y VMware ESXi. **Esta versión refuerza la complejidad del análisis al usar empaquetamiento avanzado, desactivar mecanismos de monitoreo como ETW, eliminar servicios de seguridad y borrar registros de eventos para dificultar la detección y la respuesta.**

En sus variantes multiplataforma, se han identificado opciones configurables que permiten a los operadores personalizar los ataques, incluyendo la selección de directorios a cifrar, exclusiones y modos de operación silenciosos. **Su capacidad de atacar entornos virtualizados mediante ESXi incrementa el riesgo, ya que permite comprometer múltiples máquinas virtuales desde un único punto.** Estos avances confirman la estrategia de continuidad y sofisticación del grupo detrás de LockBit, consolidando su posición como una de las amenazas más significativas en el panorama actual de ciberseguridad.

Variante de Windows de LockBit 5.0

LockBit 5.0 representa la evolución más reciente de una de las familias de ransomware más activas, incorporando mejoras en sus técnicas de evasión y ampliando su alcance a sistemas Windows, Linux y VMware ESXi. Esta versión refuerza la complejidad del análisis al usar empaquetamiento avanzado, desactivar mecanismos de monitoreo como ETW, eliminar servicios de seguridad y borrar registros de eventos para dificultar la detección y la respuesta.

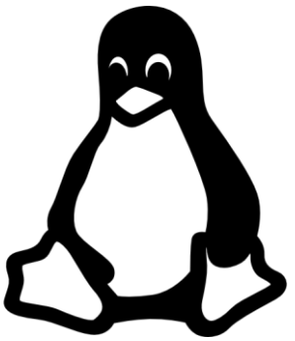
En sus variantes multiplataforma, se han identificado opciones configurables que permiten a los operadores personalizar los ataques, incluyendo la selección de directorios a cifrar, exclusiones y modos de operación silenciosos. Su capacidad de atacar entornos virtualizados mediante ESXi incrementa el riesgo, ya que permite comprometer múltiples máquinas virtuales desde un único punto. **Estos avances confirman la estrategia de continuidad y sofisticación del grupo detrás de LockBit, consolidando su posición como una de las amenazas más significativas en el panorama actual de ciberseguridad.**

NIVEL DE RIESGO

ALTO

Variante de Linux de LockBit 5.0

La variante de LockBit 5.0 para Linux mantiene muchas similitudes con su contraparte en Windows, pero se distingue por ofrecer un control detallado a través de parámetros de línea de comandos. **Entre sus funciones está la posibilidad de seleccionar directorios a cifrar, establecer exclusiones específicas y ajustar el comportamiento del proceso de cifrado.**



A diferencia de la versión de Windows, este ejecutable genera registros de actividad que muestran información sobre los archivos procesados, los directorios omitidos y las estadísticas finales del ataque, como el número de archivos cifrados y el tamaño total de los datos comprometidos. Esta capacidad de generar reportes indica que la variante está diseñada no solo para ejecutar el cifrado, sino también para proporcionar visibilidad al operador sobre los resultados obtenidos, lo que refuerza su utilidad dentro del modelo de ransomware como servicio.

Variante de Linux de VMware ESXi

La variante de LockBit 5.0 orientada a VMware ESXi está diseñada para maximizar el impacto en entornos de virtualización, ya que un único host comprometido puede afectar a múltiples máquinas virtuales. Esta versión incluye parámetros específicos que le permiten dirigirse a archivos críticos asociados a la configuración y operación de las VM, con lo cual interrumpe de forma directa los servicios alojados en la infraestructura.

El hecho de enfocarse en ESXi demuestra una clara estrategia de los operadores para atacar entornos corporativos y de centros de datos, donde la virtualización es ampliamente utilizada. Con esta capacidad, LockBit 5.0 incrementa significativamente su alcance y gravedad, al poder paralizar de manera simultánea un gran número de sistemas y servicios clave desde un solo punto de compromiso.

Vectores de ataque usados para distribuir a LockBit 5.0

- **Phishing y spearphishing:** envío de correos dirigidos para obtener credenciales o ejecutar cargas útiles iniciales. Este sigue siendo uno de los vectores primarios para afiliados que quieren acceso inicial.
- **Credenciales comprometidas:** los actores compran o reutilizan credenciales filtradas y acceso RDP/VPN para entrar en las redes objetivo y moverse lateralmente. LockBit opera como RaaS: sus afiliados usan estos accesos diversos según la oportunidad.
- **Explotación de vulnerabilidades:** se han documentado campañas de afiliados de LockBit aprovechando vulnerabilidades críticas en los puntos de entrada a la red para omitir autenticación y obtener control.
- **Exposición de interfaces de gestión de virtualización:** para la variante ESXi, los atacantes buscan hosts VMware expuestos o mal configurados para cifrar múltiples VM desde un único punto.
- **Movimiento lateral con herramientas legítimas y abuso de administración remota (living-off-the-land):** uso de herramientas administrativas, scripts y comandos legítimos (PSExec, PowerShell, SSH, herramientas de backup) para escalar privilegios y desplegar el cifrado evitando detección.

Técnicas MITRE asociadas

NOMBRE TÉCNICA	ID TÉCNICA	DESCRIPCIÓN	EVIDENCIA DEL CASO
Data Encrypted for Impact	T1486	Adversarios cifran datos para afectar la disponibilidad del sistema y exigir rescate	LockBit 5.0 cifra archivos en Windows/Linux/ESXi, usa extensiones aleatorias de 16 caracteres.
Impair Defenses: Disable Windows Event Logging	T1562.002	Deshabilitar el registro de eventos de Windows para dejar menos evidencia del compromiso.	Se ha documentado que LockBit 5.0 parchea la API EtwEventWrite para desactivar ETW, impidiendo trazas y telemetría.
Impair Defenses: Disable or Modify Tools (kill/disable security tools)	T1562.001	Finalizar procesos y/o servicios de seguridad o modificar herramientas defensivas para evitar detección.	El binario de Windows incluye lógica para terminar servicios de seguridad y para interferir con controles locales.

Mitigaciones MITRE

MITIGACIÓN	ID MITIGACIÓN	RELEVANCIA
Behavior Prevention on Endpoint	M1040	Bloquea comportamientos anómalos en endpoints como la carga en memoria, ejecución inusual de procesos, patrones de acceso masivo a archivos. Útil contra técnicas de evasión de LockBit (*DLL reflection*, ejecución en memoria) porque detecta y bloquea comportamientos sospechosos en lugar de firmas estáticas.
Data Backup	M1053	Permite recuperación ante cifrado masivo. Backups frecuentes, versionado y almacenamiento fuera de línea reducen el impacto operativo y la necesidad de pagar rescate. Fundamental por la capacidad de LockBit 5.0 de cifrar Windows, Linux y ESXi.
Restrict File and Directory Permissions	M1022	Restringir permisos evita que el actor modifique o borre archivos de logs (.evtx) o que reescriba backups y archivos críticos. Esto dificulta tanto el borrado de evidencias como la destrucción de copias de seguridad antes/durante el cifrado.
User Account Management	M1018	Aplicar principio de menor privilegio, separación de cuentas administrativas, control de cuentas de servicio y MFA reduce la posibilidad de que el ciberdelincuente obtenga privilegios para detener servicios, modificar registro o desplegar el cifrador en múltiples hosts.

Recomendaciones

1. Dividir la red en segmentos aislados con reglas de firewall internas y aplicar listas de control de acceso reduce el movimiento lateral de un atacante una vez que obtiene acceso inicial. Al restringir la comunicación entre servidores Windows, sistemas Linux y hosts ESXi, se minimiza la propagación del cifrador de LockBit 5.0 y se limita el alcance de un incidente, evitando que toda la infraestructura quede comprometida.

2. Realizar copias de seguridad frecuentes, probar su restauración periódicamente y almacenarlas en medios inmutables u offline evita que el ransomware elimine o cifre las copias. Dado que LockBit 5.0 también apunta a sistemas virtualizados en VMware ESXi, es crítico que los respaldos de máquinas virtuales se encuentren protegidos en repositorios desconectados de la red de producción, garantizando la continuidad del negocio en caso de ataque.

3. Desarrollar programas de formación periódica para todos los niveles de la organización fortalece la primera línea de defensa contra la distribución de ransomware mediante phishing, credenciales comprometidas o abuso de accesos remotos. Capacitar al personal no solo en detección de correos sospechosos, sino también en reporte ágil y cumplimiento de protocolos, reduce el riesgo de que un vector humano abra la puerta a ransomware.

4. Definir escenarios de ataque con ransomware en los planes de continuidad y recuperación ante desastres asegura que la organización esté preparada para mantener operaciones críticas, incluso si sistemas Windows, Linux o ESXi resultan comprometidos. Esto implica pruebas regulares de recuperación, comunicación de crisis y coordinación con las áreas legales y de negocio.

FUENTES

Trend Micro, 25 de septiembre de 2025, “New LockBit 5.0 Targets Windows, Linux, ESXi”, informe técnico (Trend Research), fuente corporativa.
https://www.trendmicro.com/en_us/research/25/i/lockbit-5-targets-windows-linux-esxi.html

Anexo – Indicadores de compromiso

IOC IDENTIFICADOS	
MD5	95daa771a28eaed76eb01e1e8f403f7c
SHA1	cdd5717fd3bfd375c1c34237c24073e92ad6dccc
SHA256	7ea5afbc166c4e23498aa9747be81ceaf8dad90b8daa07a6e4644dc7c2277b82
MD5	5e1f61b9c1c27cad3b7a81c804ac7b86
SHA1	c1888ba296f57e87a84411ddfce3cabc4536b142
SHA256	180e93a091f8ab584a827da92c560c78f468c45f2539f73ab2deb308fb837b38
MD5	ca93d47bcc55e2e1bd4a679afc8e2e25
SHA1	41e1e094c19fffde494c24ef4cab0d7577d5a025
SHA256	4dc06ecee904b9165fa699b026045c1b6408cc7061df3d2a7bc2b7b4f0879f4d
MD5	a1539b21e5d6849a3e0cf87a4dc70335
SHA1	561db92000409fe7093964452143ec371f930681
SHA256	90b06f07eb75045ea3d4ba6577afc9b58078eafeb2cdd417e2a88d7ccf0c0273
MD5	9bcff8da7165977f973ace12dd4c0ce0
SHA1	801a97a2fe5c3749b713d71172de6eafb961a888
SHA256	98d8c7870c8e99ca6c8c25bb9ef79f71c25912fbb65698a9a6f22709b8ad34b6