LOTE 5: Servicios de información y consultoría especializada de ciberseguridad

Informe de programas malignos recientes

4 de diciembre de 2025

Castilla-La Mancha

Índice de contenidos

Agencia de Transformación Digital de Castilla-La Mancha
Dirección General de Infraestructuras de las Telecomunicaciones y Ciberseguridad.
C/ Río Estenilla, s/n
45071 Toledo

Tel.: 925 269043
Correo-e: dgitc@jccm.es

www.castillalamancha.es

Castilla-La Mancha

1. Resumen ejecutivo

Este documento analiza la amenaza crítica predominante en el cuarto trimestre (q4) de 2025: la evolución del ransomware LockBit 5.0. Tras un periodo de fragmentación en el cibercrimen, este grupo ha resurgido consolidando capacidades técnicas avanzadas que ponen en riesgo la continuidad de negocio de empresas y la seguridad digital de la ciudadanía.

Síntesis de la amenaza: resurgimiento y evolución a la versión 5.0.

LockBit 5.0 representa un salto cualitativo en la extorsión digital. A diferencia de versiones anteriores, esta variante ha sido diseñada como una "amenaza universal" capaz de operar nativamente en Windows, Linux y, de forma crítica, en hipervisores VMware ESXi. Su principal innovación es la capacidad de "mimetizarse" con el sistema operativo utilizando herramientas legítimas (como defrag.exe) para ejecutar el cifrado sin ser detectado, técnica conocida como living off the land (LotL).

Nivel de criticidad y sectores de mayor riesgo.

Criticidad: crítica / alta: la capacidad de LockBit 5.0 para detener infraestructuras virtualizadas completas en minutos eleva el riesgo de parálisis operativa total.

Sectores objetivo

- **Manufactura e industria (68% de incidentes):** objetivo principal debido al alto coste de la inactividad en plantas de producción.
- **Servicios y administración pública:** objetivos de alto valor por la sensibilidad de los datos gestionados y la dependencia de servicios al ciudadano.
- **Sector financiero:** objetivo persistente por su capacidad económica.

Resumen de acciones urgentes.

Para empresas y PYMES

- **Blindar la virtualización:** aislar inmediatamente las consolas de gestión de ESXi en redes fuera de banda (oob) y aplicar parches de seguridad.
- **Afinar la detección:** configurar soluciones EDR para bloquear la ejecución anómala de procesos del sistema como defrag.exe y vssadmin.
- **Backups inmutables:** asegurar copias de seguridad con bloqueo de escritura y mantener una copia totalmente desconectada (offline).

Para la ciudadanía

- **Ignorar "actualizaciones falsas":** no descargar nunca actualizaciones de navegador desde ventanas emergentes en webs; hacerlo solo desde los menús oficiales.
- **Protección móvil:** extremar la precaución con aplicaciones que soliciten permisos de accesibilidad en Android, principal vector de fraude bancario actual.

Agencia de Transformación Digital de Castilla-La Mancha
Dirección General de Infraestructuras de las Telecomunicaciones y Ciberseguridad.
C/ Río Estenilla, s/n
45071 Toledo

Tel.: 925 269043
Correo-e: dgitc@jccm.es

www.castillalamancha.es

2. Introducción y contexto

La ciberseguridad, en el umbral del año 2026, ha trascendido su naturaleza técnica para consolidarse como el eje vertebrador de la **estabilidad institucional y la garantía de los servicios** públicos. Este informe aborda una de las amenazas más persistentes y sofisticadas detectadas en el cuarto trimestre (Q4) de 2025: la evolución del ransomware LockBit 5.0.

Alcance y propósito del informe

El presente documento tiene como objetivo dotar a los diferentes actores de la sociedad de la inteligencia necesaria para anticiparse y protegerse ante esta amenaza crítica. El análisis se estructura diferenciando dos niveles de impacto y respuesta:

- **Para empresas y pymes:** El informe detalla las capacidades técnicas de LockBit 5.0 contra infraestructuras corporativas, específicamente en entornos virtualizados y servidores, proporcionando directrices para la continuidad de negocio y el cumplimiento normativo.
- **Para la ciudadanía:** Se pone el foco en la identificación de los vectores de acceso inicial (como las "actualizaciones falsas") y la protección de la identidad digital, dado que el usuario final suele ser el eslabón donde comienza la cadena de ataque.

Este análisis se alinea estrictamente con los boletines de alerta temprana del Instituto Nacional de Ciberseguridad (INCIBE) y las directrices del Centro Criptológico Nacional (CCN-CERT), integrando las mejores prácticas definidas en las recientes actualizaciones de las guías CCN-STIC de noviembre de 2025.

Panorama del ciberdelito (Q4 2025)

El cierre del año 2025 ha estado marcado por una diferenciación en el ecosistema cibercriminal: una descentralización operativa masiva acompañada, simultáneamente, por un reagrupamiento técnico en torno a herramientas de intrusión de élite. **Europa se ha consolidado** en este periodo como el **segundo objetivo global más atacado** (soportando el 22% de las víctimas mundiales), situando a España en el centro de la diana.

Aunque las fuerzas del orden, mediante **operaciones internacionales** como Cronos, lograron desestabilizar grandes cárteles a principios de 2024, el vacío de poder ha derivado en dos fenómenos clave durante este trimestre:

- **Atomización (fragmentación):** Se ha registrado un récord histórico en el número de grupos de extorsión activos, superando las 85 entidades distintas. Esta proliferación de actores más pequeños y agresivos dificulta la atribución y la defensa basada en firmas tradicionales.

- **Recentralización técnica**: El resurgimiento de marcas consolidadas como LockBit, que con su versión 5.0 ha atraído de nuevo a afiliados gracias a una infraestructura robusta capaz de atacar entornos híbridos (Windows/Linux/ESXi).

Este informe se centra en **LockBit 5.0** precisamente porque **representa la cristalización de esta tendencia**: una amenaza que ha sobrevivido ha evolucionado técnicamente y ahora lidera la ofensiva contra infraestructuras corporativas y gubernamentales en Europa.

3. Descripción técnica: El arma de extorsión LockBit 5.0.

LockBit 5.0 no es simplemente un código malicioso, sino una **suite de herramientas de intrusión** altamente refinada para la industrialización del cibercrimen. Esta versión ha sido rediseñada para maximizar el daño en el menor tiempo posible, **priorizando la velocidad de cifrado** y la capacidad de operar en cualquier entorno corporativo moderno.

Arquitectura y capacidades multiplataforma

El grupo ha desarrollado binarios específicos compilados para **operar de forma nativa en los tres entornos** críticos de la infraestructura empresarial: **Windows, Linux y VMware ESXi**. Esta versatilidad elimina la necesidad de herramientas de terceros, permitiendo un despliegue unificado.

- **Amenaza a la virtualización (ESXi):** La capacidad más devastadora de LockBit 5.0 es su módulo dirigido a hipervisores. En lugar de cifrar archivos individuales dentro de un servidor, el malware ataca la infraestructura subyacente.
- **Mecánica de Ataque:** El malware enumera todas las máquinas virtuales activas en el host ESXi y ejecuta comandos para terminar sus procesos. Una vez apagadas, procede al cifrado directo de los volúmenes de almacenamiento y discos virtuales (.vmdk, .vmx).
- **Consecuencia:** Esto provoca una "denegación de servicio" total e inmediata. Una sola ejecución en el hipervisor puede dejar inoperativas decenas de servidores (correo, bases de datos, aplicaciones web, etc.) Simultáneamente, sin necesidad de infectar cada máquina individualmente.

Innovaciones en evasión y "Living off the Land" (LotL):

Para eludir las soluciones de seguridad modernas, LockBit 5.0 ha perfeccionado las técnicas de Living off the Land (LotL), que consisten en utilizar herramientas legítimas del sistema operativo para fines maliciosos.

El camuflaje defrag.exe

Análisis forenses han detectado que, si el malware se ejecuta sin parámetros específicos, **lanza automáticamente la utilidad legítima de Windows** Desfragmentador de Disco (defrag.exe).

Mimetismo operativo

Bajo la apariencia de este proceso de mantenimiento rutinario -un binario firmado por Microsoft y confiable por defecto-, **el malware inyecta su código** o utiliza el proceso p**ara recorrer el sistema** de archivos. Esto confunde a los analistas y sistemas de monitoreo, que interpretan la alta actividad de disco como una tarea de optimización en lugar de un proceso de cifrado masivo.

Control y ejecución

LockBit 5.0 ofrece a sus afiliados una Interfaz de Línea de Comandos (CLI) robusta, accesible mediante el parámetro *-h*, que permite un control granular sobre la detonación del ataque para adaptarlo al objetivo.

Métodos de ejecución

- **Modo sigilo (stealth):** Ejecuta el cifrado en segundo plano sin ninguna indicación visual, ideal para comprometer la red sin alertar a los administradores hasta que el daño es irreversible.
- **Modo verbose:** Muestra una barra de progreso detallada en la consola, utilizada por los atacantes para monitorear la velocidad de infección en tiempo real

Gestión inteligente

El ransomware incluye configuraciones para proteger la "viabilidad del pago". Utiliza exclusiones inteligentes para evitar cifrar archivos ejecutables críticos del sistema (Kernel, Boot), asegurando que el equipo siga encendiendo para que la víctima pueda ver la nota de rescate. Además, permite configurar si la nota de extorsión se deposita en cada subcarpeta o solo en la raíz del disco.

Vectores de acceso inicial y distribución

LockBit funciona como la fase final de un ataque, **apoyándose en una red** de Initial Access Brokers (iabs) **para la penetración inicial**. En el Q4 de 2025, la simbiosis más peligrosa se ha establecido con el grupo TA569 y su malware SocGholish.

La trampa de los "fake updates"

SocGholish utiliza sistemas de distribución de tráfico (TDS) para **comprometer sitios web legítimos**. Cuando un usuario corporativo visita estos sitios, se le muestra una **alerta falsa de "Actualización urgente de navegador"** (Chrome/Edge). Al descargar el archivo, se instala un loader que permite a los atacantes desplegar LockBit posteriormente.

Explotación de perímetro

Los **atacantes suelen acceder a las redes empresariales** utilizando métodos como el robo de credenciales para servicios de acceso remoto, como RDP (Remote Desktop Protocol) y VPN (Virtual Private Network). De este modo, se hacen pasar por usuarios legítimos y logran entrar en los sistemas de la empresa. Además, aprovechan fallos de seguridad graves que no han sido corregidos, como la vulnerabilidad CVE-2025-62215 en el Kernel de Windows. Estas debilidades les permiten obtener permisos de administrador dentro de la red y, una vez dentro, distribuir el ransomware de manera masiva a través de todos los sistemas conectados.

4. Impacto potencial y consecuencias

La **naturaleza "universal" de LockBit 5.0** y su integración con redes de distribución masiva transforman este malware en un riesgo sistémico. A continuación, se detalla cómo se materializa este daño en diferentes estratos de la sociedad.

Para empresas (PYMES y corporaciones)

El impacto en el sector corporativo ha dejado de ser meramente una interrupción de TI para convertirse en una crisis de supervivencia empresarial.

Impacto operativo

El "apagón" de la virtualización: A diferencia de ataques previos que cifraban archivos individualmente, el ataque a hipervisores ESXi **detiene instantáneamente toda la actividad**. Al eliminar las máquinas virtuales, las empresas **pierden acceso inmediato a sistemas clave** como CRM (Customer Relationship Management), ERP (Enterprise Resource Planning), correos y bases de datos. La recuperación **requiere reconstruir toda la infraestructura de servidores**, lo que puede aumentar el tiempo de inactividad de horas a semanas.

Impacto económico

La trampa de la doble extorsión: El coste del rescate es solo la punta del iceberg. LockBit 5.0 sistematiza una doble extorsión:

- Exigen un **pago por la clave de descifrado**.
- Exigen un segundo **pago para no filtrar los terabytes de información** sensible exfiltrada antes del cifrado (datos de clientes, propiedad intelectual, nóminas). Esto expone a las empresas a multas millonarias por incumplimiento del RGPD y daños reputacionales irreversibles.

Sectores en Riesgo

Manufactura y servicios críticos

Según la inteligencia de amenazas del Q4 2025, la Manufactura es el sector más castigado, **sufriendo el 68% de los incidentes** de ransomware industrial. Los atacantes saben que cada minuto de parada en una fábrica supone pérdidas millonarias directas. Le siguen el sector de Transporte y Logística (15%), Salud (alertas de Health-ISAC) y el sector Financiero, objetivos prioritarios por la criticidad de sus datos y su capacidad de pago.

Para la ciudadanía (impacto indirecto)

Aunque el **ciudadano** de a pie no suele ser el objetivo final del ransomware, se convierte en una **víctima colateral** y, a menudo, en el vector de entrada involuntario.

Riesgo por la cadena de suministro y servicios públicos

La ciudadanía sufre las consecuencias cuando la administración o los proveedores de servicios esenciales son atacados. Esto se traduce en la **paralización** de citas médicas, **retrasos** en trámites administrativos o la **exposición de sus datos** personales (DNI, datos bancarios) en la Dark Web tras una brecha en una entidad pública o empresa de suministros.

Aumento de fraudes

La amenaza de las "actualizaciones falsas": La mecánica de acceso inicial de LockBit (vía SocGholish) afecta directamente a la navegación diaria del usuario. El incremento de campañas de "Fake Updates" en sitios web legítimos (diarios locales, portales de hobbies) pone en riesgo los equipos personales. Un usuario que intenta actualizar su navegador en casa puede infectar su dispositivo, permitiendo el robo de sus propias credenciales bancarias o convirtiendo su equipo en una "puerta trasera" si lo utiliza para teletrabajar.

5. Medidas preventivas y estrategia defensiva

Ante la sofisticación de LockBit 5.0 y su capacidad para operar en entornos híbridos, la defensa perimetral tradicional es insuficiente. Se requiere una estrategia de defensa en profundidad que combine endurecimiento técnico, vigilancia activa y cultura organizacional.

Recomendaciones para empresas y PYMES

Las organizaciones deben asumir que el intento de intrusión ocurrirá y prepararse para resistirlo y recuperarse.

Medidas técnicas

- **Blindaje de virtualización (hardening de ESXi):** Dado que LockBit ataca directamente al hipervisor, es imperativo aislar las interfaces de gestión.
  - **Segmentación:** Mover las consolas de gestión (vcenter/ESXi host client) a una red fuera de banda (OOB - Out of Band) sin acceso directo a Internet y accesible solo vía VPN segura u otro modo de seguridad similar.
  - **Normativa:** Aplicar la guía CCN-STIC 1656 para la configuración segura de entornos de virtualización.
  - **Kill-Switch:** Deshabilitar el servicio SSH en los hosts ESXi cuando no se esté utilizando activamente para mantenimiento.
- **Detección activa (afinamiento de EDR)**: Las soluciones EDR (Endpoint Detection and Response) deben configurarse para detectar el comportamiento anómalo, no solo firmas de virus.
  - **Reglas LotL:** Configurar alertas críticas ante la ejecución del proceso defrag.exe si este proceso lanza conexiones de red o realiza operaciones de escritura masiva no programadas por el sistema.
  - **Monitorizar y bloquear vssadmin:**
    - **¿Qué es?** Las Shadow Copies (Instantáneas de Volumen) son copias de seguridad automáticas que Windows realiza en segundo plano, permitiendo restaurar archivos a versiones anteriores rápidamente.
    - El comando **vssadmin** es la **herramienta para gestionarlas**. El primer paso de cualquier ransomware moderno es ejecutar este comando para borrar todas las copias de sombra. Si se bloquea o alerta sobre esta acción, se puede detener el ataque antes del cifrado o, al menos, conservar una vía de recuperación gratuita e inmediata de los datos.
  - **Referencia:** Seguir el procedimiento CCN-STIC 1217 para el despliegue óptimo de agentes EDR.
- **Gestión de backups (la última línea de defensa):**
  - **Inmutabilidad (S3 Object Lock):**
  - **¿Qué es?** Es una tecnología de bloqueo de objetos en la nube que sigue el principio WORM (Write Once, Read Many).

    - Garantiza que, **una vez guardada una copia de seguridad, esta quede "congelada"** por un periodo definido. Ni siquiera un administrador con credenciales robadas puede borrarla o sobrescribirla. Es el seguro de vida definitivo contra la destrucción intencionada de Backups que practica LockBit.
- **Regla 3-2-1-1:** Estándar de oro de la industria para garantizar la recuperación de datos:
    - Mantener **3 copias** de los datos.
    - En **2 soportes** diferentes (ej. Disco local y nube).
    - Almacenar **1 copia fuera** de la sede (offsite).
    - Tener **1 copia inmutable** o totalmente offline (desconectada de la red). Esta última es crítica, ya que, si no está conectada a la red, el ransomware no puede alcanzarla físicamente.

Medidas organizativas

- **Gestión de Identidades (IAM):**
    - **MFA Obligatorio para RDP y VPN:**
        - **El RDP (Remote Desktop Protocol)** es la tecnología que permite a los empleados conectarse a sus ordenadores de oficina desde casa (teletrabajo).
        - Es la **"puerta de entrada" más atacada**. Si solo se protege con usuario y contraseña, es vulnerable a ataques de fuerza bruta. Implementar Autenticación Multifactor (MFA) es obligatorio para asegurar que, aunque roben la contraseña, el atacante no pueda entrar sin el segundo código de verificación.
    - **Mínimo Privilegio:** Revisar y revocar permisos de administrador local innecesarios para frenar la escalada de privilegios (mitigando riesgos como el CVE-2025-62215).
- **Formación anti-fraude web:**
    - **Concienciar a la plantilla sobre la campaña de SocGholish:** los navegadores modernos se actualizan en segundo plano y nunca mediante ventanas emergentes en sitios web de terceros. Prohibir la descarga de archivos *.js* o *.zip* desde alertas web.

Recomendaciones para la ciudadanía

El usuario doméstico debe centrarse en la higiene digital básica para evitar convertirse en la puerta de entrada o víctima de fraude bancario.

Protección del puesto de trabajo y móvil

- **Actualizaciones Oficiales:** Ignorar sistemáticamente cualquier aviso web que diga "Su navegador está desactualizado". Realizar actualizaciones solo desde el menú "Ayuda > Acerca de" del navegador o las tiendas oficiales de aplicaciones (Google Play/App Store).
- **Parcheo Automático:** Activar las actualizaciones automáticas del sistema operativo para cerrar brechas de seguridad críticas.

Detección de ingeniería social

- **Desconfiar de mensajes urgentes o alarmantes:** Si una web solicita descargar un archivo para "ver el contenido" o "mejorar la seguridad", es casi con certeza un intento de ataque.
- **Instalar soluciones antimalware en dispositivos móviles:** especialmente en Android que es más versátil para estas tareas, para así detectar aplicaciones que abusen de los permisos de Accesibilidad (como toxicpanda).

Agencia de Transformación Digital de Castilla-La Mancha
Dirección General de Infraestructuras de las Telecomunicaciones y Ciberseguridad.
C/ Río Estenilla, s/n
45071 Toledo

Tel.: 925 269043
Correo-e: dgitc@jccm.es

www.castillalamancha.es

6. Anexos y referencias

Indicadores de compromiso (IOC) y de ataque (IOA).

A continuación, se detallan los indicadores técnicos observados en las campañas del Q4 2025 para su implementación en sistemas de detección (SIEM/EDR) y bloqueo perimetral.

Tabla 1: Indicadores Técnicos de la Amenaza

Categoría	Tipo	Indicador / Comportamiento	Descripción
LockBit 5.0	Proceso	Defrag.exe (con argumentos inusuales)	Uso de herramienta legítima para ocultar el proceso de cifrado (Living off the Land).
LockBit 5.0	Comando	Vssadmin.exe Delete Shadows /All /Quiet	Comando ejecutado para eliminar copias de seguridad locales (Shadow Copies) antes del cifrado.
LockBit 5.0	Archivos	Extensiones .vmdk, .vmx, .vmem	Archivos de discos virtuales de VMware objetivo prioritario del cifrado.
SocGholish	Red	Dominios con alertas de "Update Chrome/Edge"	Sitios legítimos comprometidos inyectados con JavaScript malicioso (TDS).
SocGholish	Archivo	Descargas .zip conteniendo .js, .hta, .vbs	Archivos comprimidos descargados desde alertas falsas que inician la cadena de infección.
Móvil	Comportamiento	Uso excesivo de *Accessibility Services*	Aplicaciones Android (toxicpanda/Klopatra) que solicitan permisos de accesibilidad para leer pantalla y realizar clics.
Vulnerabilidad	CVE	**CVE-2025-62215**	Elevación de privilegios en Kernel de Windows (CVSS 7.0).
Vulnerabilidad	CVE	**CVE-2025-60724**	Ejecución remota de código en GDI+ (Microsoft Office) (CVSS 9.8).

Referencias bibliográficas y fuentes.

Este informe ha sido elaborado a partir de la información de amenazas recopilada durante el cuarto trimestre de 2025 y la normativa vigente.

Fuentes Institucionales y Normativa:

- CISA. (2025). Fact Sheet: Rising Ransomware Threat to OT Assets. Cybersecurity and Infrastructure Security Agency. Recuperado de cisa.gov

- INCIBE-CERT. (2024, 14 marzo). LockBit: Acciones de respuesta y recuperación. Instituto Nacional de Ciberseguridad. Recuperado de incibe.es

Informes de Inteligencia de Amenazas (Threat Intelligence):

- Arctic Wolf. (2025, 25 noviembre). Romcom utilizing SocGholish to deliver Mythic Agent to USA companies. Recuperado de arcticwolf.com
- Bitsight TRACE. (2025, 28 julio). Toxicpanda Android Banking Malware 2025 Study. Recuperado de bitsight.com
- Cleafy Labs. (2024, 04 noviembre). Toxicpanda: A new banking trojan from Asia hit Europe and LATAM. Recuperado de cleafy.com
- Dragos. (2024, julio). Frostygoop ICS Malware Intel Brief. Recuperado de https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-Malware-Intel-Brief-0724_r2.pdf?hsLang=en
- ESET welivesecurity. (2025, 13 noviembre). LockBit 5.0: Última versión del ransomware y sus capacidades multiplataforma. Recuperado de https://www.welivesecurity.com/es/ransomware/lockbit-5-ultima-version-ransomware/
- Lakshmanan, R. (2025, 26 noviembre). Romcom Uses SocGholish Fake Update to Target Victims. The Hacker News. Recuperado de https://thehackernews.com/2025/11/romcom-uses-socgholish-fake-update.html
- Pcrisk. (2025, 21 noviembre). Guía de desinfección de LockBit 5.0 Ransomware. Recuperado de https://www.pcrisk.es/guias-de-desinfeccion/13847-lockbit-5-0-ransomware
- Tenable. (2025, 11 noviembre). Microsoft's November 2025 Patch Tuesday Addresses 63 CVEs (CVE-2025-62215). Recuperado de https://www.tenable.com/blog/microsofts-november-2025-patch-tuesday-addresses-63-cves-cve-2025-62215
- Threatfabric. (2025, 03 junio). Crocodilus mobile malware: Evolving fast, going global. Recuperado de https://www.threatfabric.com/blogs/crocodilus-mobile-malware-evolving-fast-going-global
- Txone Networks. (2025, octubre). Mid-Year Report 2025: An In-Depth Analysis of Evolving Ransomware and Weaponized ICS Malware. Recuperado de https://media.txone.com/prod/uploads/2025/10/v6_2025-H1-WP-Mid-Year-Report-2025_An-In-Depth-Analysis-of-Evolving-Ransomware-and-Weaponized-ICS-Malware.pdf