TIC

COLOMBIA 2026:
EL HORIZONTE DEL CIBER-ASEDIO

ARQUITECTURA DE UNA AMENAZA CRÍTICA

Contenido

Resumen ejecutivo

Entre 2021 y julio de 2026, Colombia ha registrado actividad confirmada de al menos 18 grupos de ransomware. El presente análisis prioriza diez de estos actores basándose en su vigencia operativa, sofisticación técnica, red de alianzas y relevancia sectorial. Recientemente, se han identificado cuatro nuevas víctimas colombianas, lo que confirma que el país es un objetivo consolidado dentro de las estrategias de victimización regional y no un actor periférico.

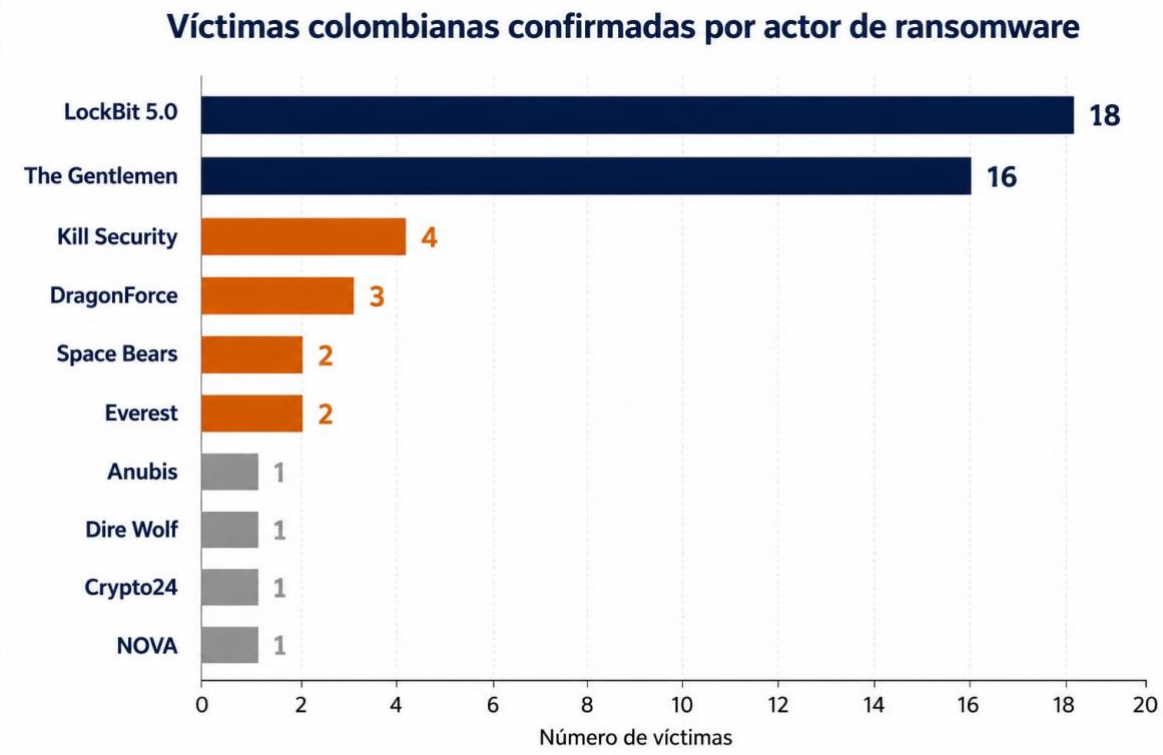
El impacto sectorial se concentra predominantemente en el sector público, la justicia, la salud, la energía, los servicios públicos y el comercio/manufactura. Mientras que los operadores consolidados de *Ransomware-as-a-Service* (RaaS) priorizan el ataque a infraestructuras críticas y cadenas de suministro tecnológico, los actores oportunistas focalizan sus esfuerzos en organizaciones medianas. Estas últimas suelen presentar condiciones favorables para la intrusión, tales como servicios RDP o VPN expuestos, aplicaciones perimetrales sin actualizar y capacidades limitadas de detección y respuesta.

El nivel de riesgo general para el país se mantiene en **ALTO**, impulsado por dos dinámicas principales en el ecosistema cibercriminal. La primera es la convergencia de una coalición entre LockBit, DragonForce y Qilin, lo cual amplifica la disponibilidad de infraestructura, herramientas de evasión y el intercambio de afiliados experimentados. La segunda es la rápida escalada de The Gentlemen: durante el primer semestre de 2026 se posicionó como uno de los operadores RaaS más activos, superando a Qilin en volumen trimestral de víctimas (según datos de ReliaQuest, 2026). Ambos fenómenos se apalancan en una explotación sostenida de vulnerabilidades críticas en la infraestructura perimetral.

En consecuencia, la estrategia de ciberseguridad y ciberdefensa de las organizaciones colombianas no debe orientarse exclusivamente hacia una única familia de ransomware. Los vectores de acceso inicial y compromiso como el uso de credenciales válidas, RDP/VPN expuestos, vulnerabilidades en servicios publicados en internet, abuso de herramientas RMM legítimas y la explotación de controladores vulnerables son transversales a múltiples actores de amenazas. Por lo tanto, una defensa eficaz depende fundamentalmente de la reducción sistemática de esta superficie común de exposición y del sostenimiento de capacidades reales y probadas de recuperación operativa.

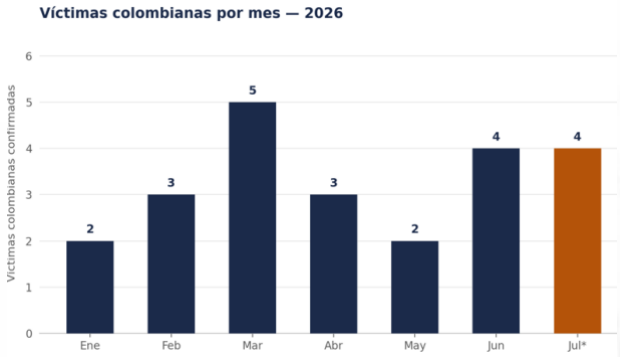
Panorama de la actividad en Colombia

La distribución de víctimas muestra una concentración marcada. LockBit 5.0 y The Gentlemen reúnen la mitad de los casos acumulados, mientras que el resto se distribuye entre operadores de RaaS con una a cinco víctimas. La concentración no reduce el riesgo de los actores menores: muchos funcionan como afiliados, brókeres de acceso o especialistas que pueden entregar una intrusión a otra marca.



Gráfica 1. Víctimas colombianas confirmadas por actor de ransomware.

La serie anual pasa de una víctima en 2021 a 23 en los primeros siete meses de 2026, el dato de 2026 no representa un cierre anual; aun así, ya supera el total de 2025 y confirma una aceleración sostenida. En el comportamiento mensual de 2026, marzo registra cinco casos y junio y julio cuatro cada uno.



A nivel sectorial se sitúa a salud, justicia, energía y comercio entre los más expuestos, esta distribución combina valor económico, dependencia operativa y sensibilidad de los datos. En salud y justicia, la interrupción puede

afectar servicios esenciales; en energía, una intrusión puede extenderse desde TI hacia procesos de operación; en comercio, la presión se apoya en continuidad, reputación y datos personales.

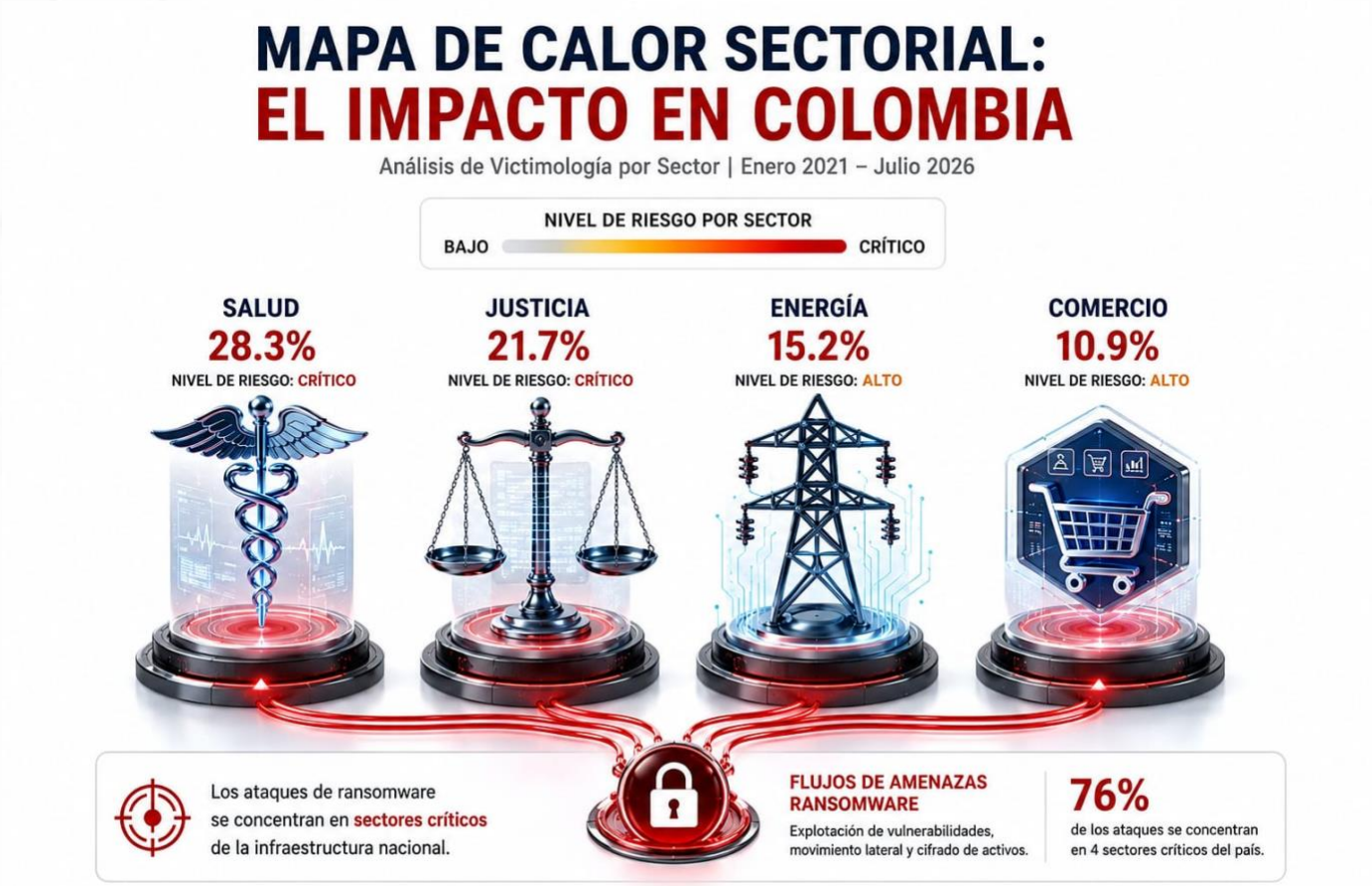


Figura 1. Concentración sectorial de víctimas y exposición crítica.

Las implicaciones sectoriales, en salud y justicia, la disponibilidad del servicio y la confidencialidad de expedientes aumentan la presión sobre la víctima. En energía y servicios públicos, la prioridad es impedir que el compromiso de TI alcance sistemas de operación. En comercio y manufactura, la recuperación debe considerar ventas, logística, identidad de clientes y continuidad de proveedores.

Actores prioritarios y familias operativas

Los diez perfiles se agrupan por la función que cumplen dentro del ecosistema criminal. The Gentlemen, DragonForce y LockBit 5.0 representan el núcleo RaaS de mayor prioridad y concentran capacidad de afiliación, cifrado multiplataforma y evasión de defensas. Anubis, Space Bears, Dire Wolf y Kill Security intensifican el componente destructivo o reputacional. Everest, Crypto24 y NOVA aportan capacidades especializadas de acceso, persistencia, evasión o evolución técnica.

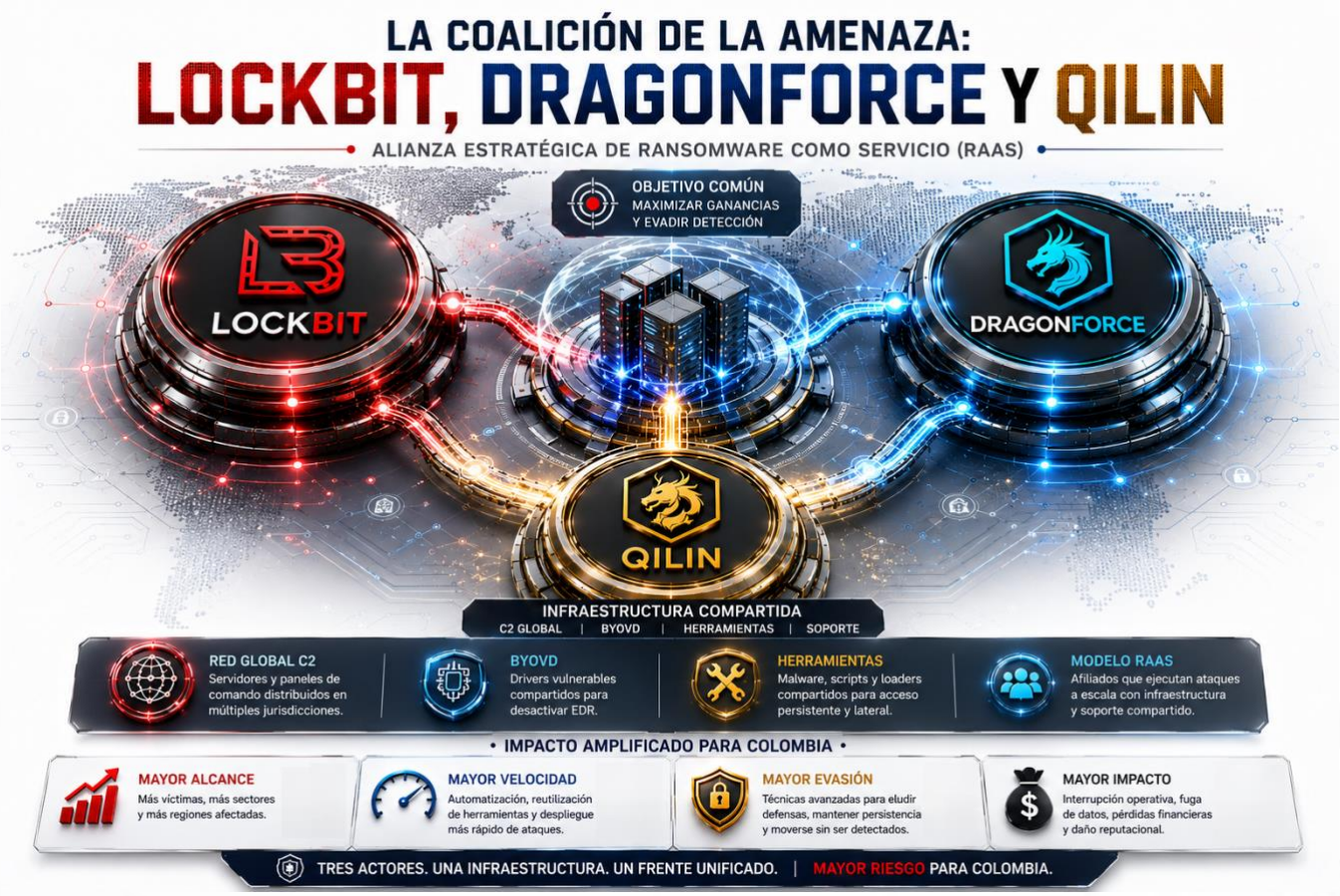


Figura 2. Coalición LockBit, DragonForce y Qilin: convergencia de infraestructura y capacidades.

Actor	Prioridad	Estado	Sector Objetivo
The Gentlemen	CRÍTICA	ONLINE / actividad crítica	Energía / sector público
DragonForce	CRÍTICA	ONLINE / actividad crítica	TI / ciberseguridad (MSSP)
LockBit 5.0	CRÍTICA	ONLINE / riesgo de despliegue	Construcción / histórico multisector
Anubis	ALTA	ONLINE / actividad confirmada	Retail / supermercados
Space Bears	ALTA	ONLINE / actividad confirmada	Comercio / PYME
Dire Wolf	ALTA	ONLINE / actividad confirmada	Salud
Everest	ALTA	ONLINE / bróker de acceso inicial con giro creciente hacia la extorsión pura	Servicios públicos
Kill Security	ALTA	ONLINE / actividad activa	Salud / justicia
Crypto24	ALTA	ONLINE / capacidades de evasión de EDR más sofisticadas	Financiero
NOVA	MEDIA	En reestructuración de infraestructura tras exposición pública	Sector público / justicia

1. The Gentlemen

Crecimiento acelerado, evasión en kernel y cifrado multiplataforma

Prioridad: CRÍTICA | **Estado:** ONLINE / actividad crítica | **Primera actividad:** Julio de 2025 (DLS operativo desde mediados de julio; lanzamiento público del RaaS en septiembre de 2025) | **Atribución:** Grupo de habla rusa. Surgió tras una disputa de pago con los operadores RaaS de Qilin.

The Gentlemen pasó de ser un RaaS emergente a ocupar una posición dominante en menos de un año, registra aproximadamente 332 víctimas publicadas durante sus primeros cinco meses de actividad completa y, para el segundo trimestre de 2026, 300 víctimas frente a 289 de Qilin El grupo reparte a sus afiliados el 90% de lo

recaudado, diez puntos por encima del estándar del sector (Krebs on Security, 2026), explica parte de su capacidad para atraer operadores de RaaS experimentados.

La operación combina reconocimiento con SharpADWS, NetScan y Advanced IP Scanner, captura de tráfico mediante netsh y análisis externo con Wireshark. La capacidad de impacto no se limita a Windows: dispone de cifradores para Linux/BSD y de un módulo específico para VMware ESXi. En la intrusión, el acceso perimetral puede apoyarse en fallas de FortiOS/FortiProxy y credenciales VPN; la evasión incluye controladores vulnerables y utilidades legítimas para alcanzar privilegios SYSTEM.

Cadena operacional documentada. Explotación perimetral → Evasión BYOVD → SystemBC y túneles SOCKS5 → Propagación por GPO/SMB → Cifrado en Windows, Linux/BSD y ESXi

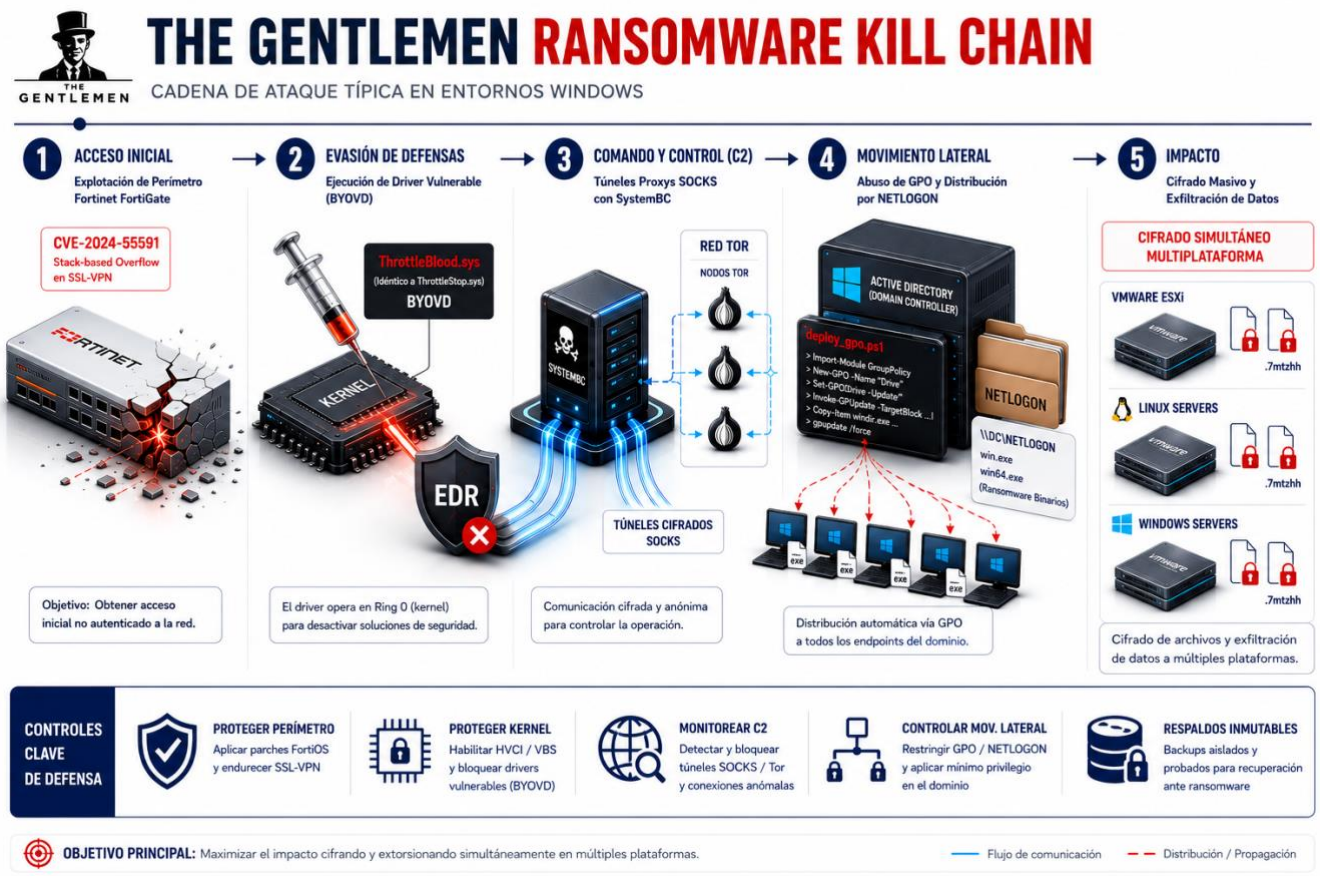


Figura 3. Cadena operacional sintetizada de The Gentlemen.

2. DragonForce

Infraestructura RaaS de marca blanca y operación por afiliados

Prioridad: CRÍTICA | **Estado:** ONLINE / actividad crítica | **Primera actividad:** Agosto de 2023 (actividad de ransomware documentada desde diciembre de 2023) | **Atribución:** Infraestructura geolocalizada en la Federación Rusa según ReliaQuest; el grupo niega vínculos con el colectivo hacktivista DragonForce Malaysia.

DragonForce evolucionó desde un RaaS emergente hacia una plataforma de “marca blanca” que permite a otros operadores de RaaS desplegar campañas con infraestructura, paneles y soporte compartidos, en septiembre de 2025 propuso públicamente en foros clandestinos formar una coalición con LockBit y Qilin "para dictar las condiciones del mercado", coalición que LockBit confirmó y que sigue activa a julio de 2026, el grupo registra 101 víctimas y también se documenta colaboración operativa con el bróker de acceso Scattered Spider.

El actor mantiene dos líneas de cifrado: una derivada de LockBit 3.0 Black y otra reescrita sobre Conti v3 con ChaCha8, el acceso suele apoyarse en RDP expuesto, fuerza bruta y explotación de vulnerabilidades conocidas. Tras obtener acceso, los afiliados realizan reconocimiento, vuelcan LSASS con Mimikatz, despliegan SystemBC como backdoor y reducen la visibilidad mediante borrado de registros o desactivación de Microsoft Defender.

Cadena operacional documentada. Escaneo, RDP y explotación → Robo de credenciales en LSASS → SystemBC y C2 sigiloso → Persistencia y control remoto → Cifrado y doble extorsión

Figura 4. Cadena operacional sintetizada de DragonForce.

3. LockBit 5.0

Retorno operativo, automatización y explotación de WSUS

Prioridad: CRÍTICA | **Estado:** ONLINE / riesgo de despliegue | **Primera actividad:** Operativo desde 2019; relanzamiento como LockBit 5.0 el 3 de septiembre de 2025 tras la Operación Cronos de 2024 | **Atribución:** Grupo de habla rusa/europea del este; afiliación abierta en el foro RAMP.

LockBit relanzó su programa de afiliados como LockBit 5.0 el 3 de septiembre de 2025, después del impacto de la Operación Cronos, el programa recuperó soporte para Windows, Linux y VMware ESXi y registró 163 víctimas publicadas en el primer trimestre de 2026. Desde octubre de 2025 integra la coalición con DragonForce y Qilin, un cambio que puede ampliar el acceso a infraestructura, afiliados y herramientas de evasión.

El vector de mayor relevancia descrito para 2025-2026 es el CVE-2025-59287 en WSUS, una falla de ejecución remota de código con privilegios de sistema. Una vez comprometido el servidor, el atacante despliega el payload,

abusa de GPO para propagarlo y emplea controladores vulnerables (entre ellos gdrv.sys) para anular controles de seguridad. El impacto incluye cifrado, eliminación de instantáneas y obstaculización de la recuperación.

Cadena operacional documentada. Explotación de WSUS → Ejecución remota del payload → Propagación mediante GPO → BYOVD y anulación de defensas → Cifrado, exfiltración e inhibición de recuperación

Figura 5. Cadena operacional sintetizada de LockBit 5.0.

4. Anubis

Abuso de herramientas RMM y capacidad destructiva opcional

Prioridad: ALTA | **Estado:** ONLINE / actividad confirmada | **Primera actividad:** Diciembre de 2024 (anuncio formal de programas de afiliados el 23 de febrero de 2025 en el foro RAMP) | **Atribución:** Foros de habla rusa; se sospecha origen en Europa del Este.

El nombre Anubis también corresponde a un troyano bancario Android, pero el actor tratado aquí es una operación RaaS para Windows independiente. La característica que lo diferencia es el modo de destrucción opcional: además del cifrado y la extorsión, puede sobrescribir archivos de forma irreversible, incluso después de un eventual pago, el programa ofrece modalidades de RaaS, extorsión de datos y monetización de accesos.

En 2026 se documentaron credenciales VPN válidas y explotación de CitrixBleed 2 (CVE-2025-5777) en NetScaler ADC/Gateway. Dentro de la red, los operadores de RaaS abusan de ScreenConnect, Zoho Assist, MeshAgent, UltraVNC y otras herramientas RMM. Ese uso se mezcla con la actividad normal de soporte, reduce la probabilidad de detección y facilita movimiento lateral, exfiltración y control remoto persistente.

Cadena operacional documentada. Credenciales VPN o CitrixBleed 2 → Herramientas RMM legítimas → Movimiento lateral sigiloso → Exfiltración previa → Cifrado o activación de wipe mode

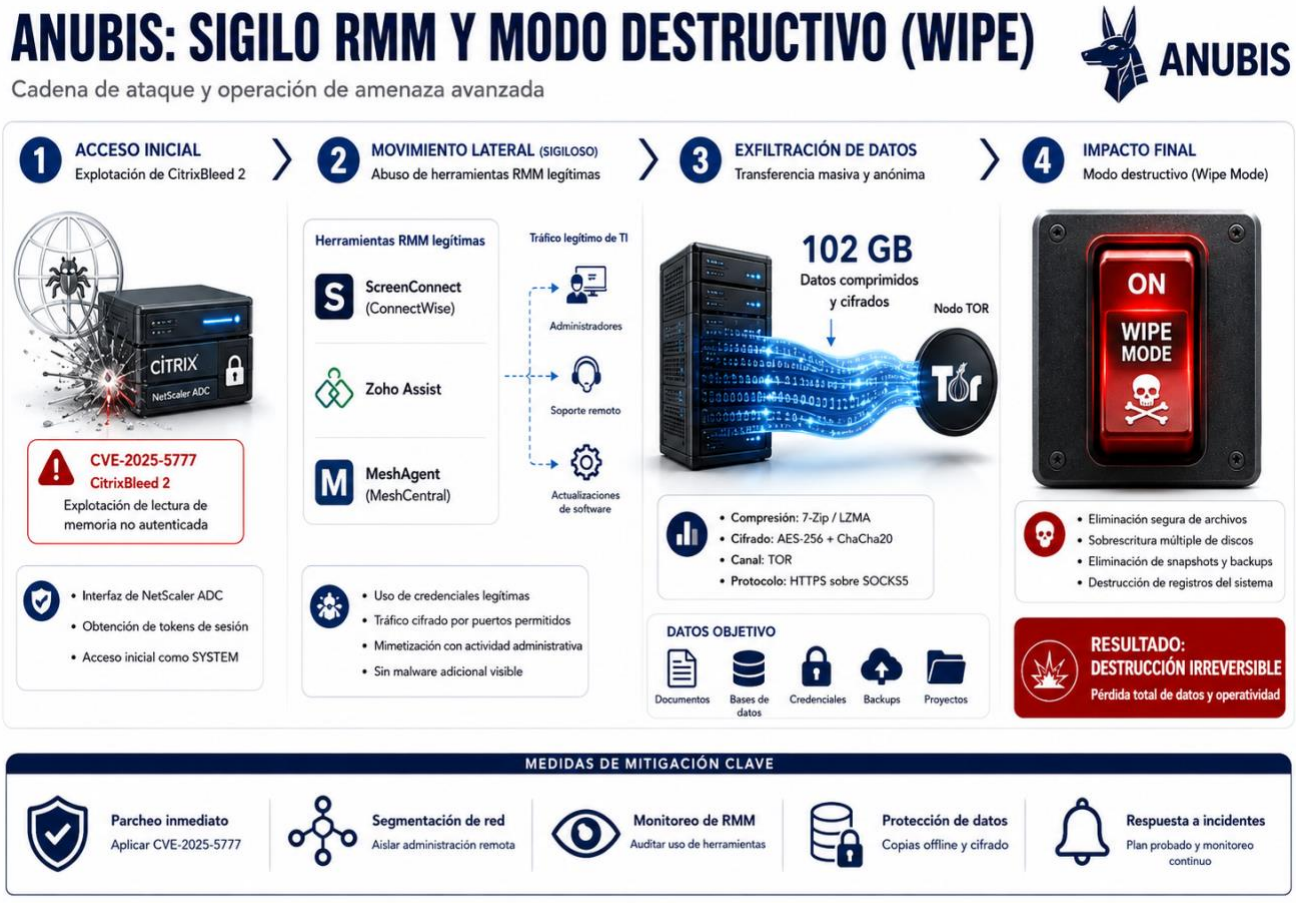


Figura 6. Cadena operacional sintetizada de Anubis.

5. Space Bears

Extorsión oportunista contra pequeñas y medianas organizaciones

Prioridad: ALTA | **Estado:** ONLINE / actividad confirmada | **Primera actividad:** Abril de 2024 | **Atribución:** Vinculado operativamente al programa de afiliados Phobos; sin atribución geográfica pública confirmada.

Space Bears fue identificado como un afiliado que opera sobre infraestructura Phobos. Su sitio de filtración utiliza una apariencia corporativa y un "muro de la vergüenza" para exponer a las víctimas y aumentar la presión de pago, su actividad se documenta desde abril de 2024 y registra alrededor de 34 víctimas públicas.

La operación se dirige principalmente a pequeñas y medianas organizaciones con defensas limitadas. El acceso combina RDP mal protegido, servidores web expuestos y campañas de phishing con adjuntos. La ejecución mediante PowerShell codificado en Base64 busca evadir firmas locales; los archivos se agrupan antes de la transferencia por HTTPS y la presión culmina con publicación y cuenta regresiva en el portal de filtración.

Cadena operacional documentada. Phishing o servicios expuestos → PowerShell codificado → Empaquetado y transferencia HTTPS → Publicación y presión reputacional

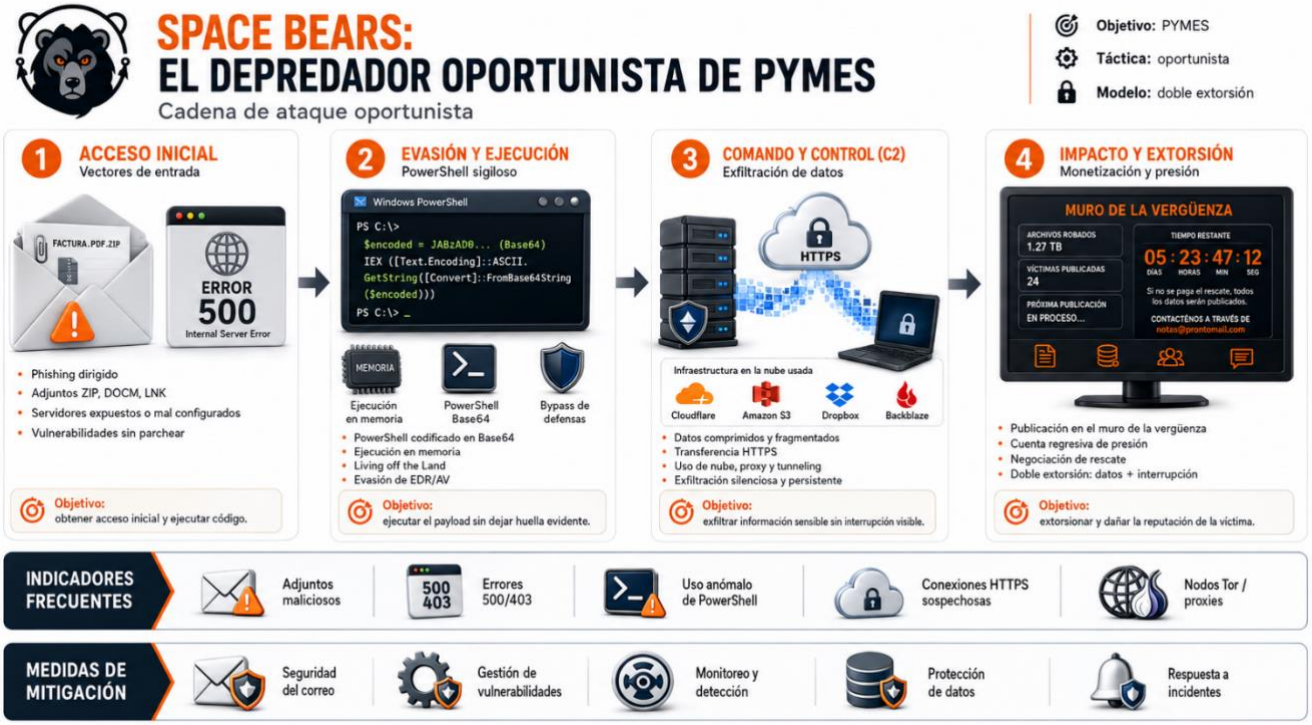


Figura 7. Cadena operacional sintetizada de Space Bears.

6. Dire Wolf

Cifrado selectivo y afectación de servicios críticos

Prioridad: ALTA | **Estado:** ONLINE / actividad confirmada | **Primera actividad:** Mayo de 2025 (primeras seis víctimas publicadas el 26 de mayo de 2025) | **Atribución:** Sin atribución geográfica pública confirmada; operación independiente, sin vínculo demostrado con otros colectivos de intrusión conocidos.

Dire Wolf combina el cifrado (Curve25519 y ChaCha20 y agrega la extensión .direwolf), negocia exclusivamente mediante Tox. El grupo declara una motivación económica y opera bajo un modelo de doble extorsión, a julio de 2026 acumula alrededor de 41 víctimas en al menos 16 países, con concentración en sectores de manufactura y tecnología.

Su cifrado busca velocidad: procesa completamente los archivos menores de 1 MB y solo el primer MB de los archivos grandes, esa lógica puede inutilizar bases de datos sin cifrarlas por completo. La fase de impacto incluye terminación de sqlservr.exe y outlook.exe, detención de servicios de respaldo como BackupExecJobEngine y VeeamTransportSvc, eliminación de registros y degradación deliberada de la capacidad de recuperación.

Cadena operacional documentada. Phishing o cuentas de servicio → Acceso y movimiento lateral → Cifrado selectivo por tamaño → Detención de SQL y respaldos → Negociación mediante Tox

Figura 8. Cadena operacional sintetizada de Dire Wolf.

7. Everest

Bróker de acceso, extorsión y reclutamiento de insiders

Prioridad: ALTA | **Estado:** ONLINE / bróker de acceso inicial con giro creciente hacia la extorsión pura | **Primera actividad:** Diciembre de 2020 (con capacidades completas de cifrado y doble extorsión desde 2021) | **Atribución:** Grupo de habla rusa, con nexo probable en Europa del Este. Everest combina tres negocios: despliegue de ransomware, venta de accesos previamente comprometidos y reclutamiento pagado de empleados internos, la venta de accesos está documentada desde 2021 y desde 2023 el grupo ofrece a insiders un porcentaje de la extorsión. La eliminación frecuente de anuncios de víctimas dificulta medir el volumen real de la actividad. La operación ha evolucionado hacia la extorsión pura, el actor exfiltra volúmenes que habitualmente superan un terabyte por víctima y, en varios casos, evita el cifrado ruidoso. Cuando cifra, utiliza AES-128-CBC envuelto en RSA, elimina copias de sombra y desinstala Raccine. ProcDump, Cobalt Strike, AnyDesk, TeamViewer y RDP sostienen el acceso, el volcado de credenciales y la persistencia. **Cadena operacional documentada.** Compra, phishing o acceso remoto → Volcado de LSASS con ProcDump → Cobalt Strike y movimiento lateral → Exfiltración masiva o cifrado → Negociación y monetización

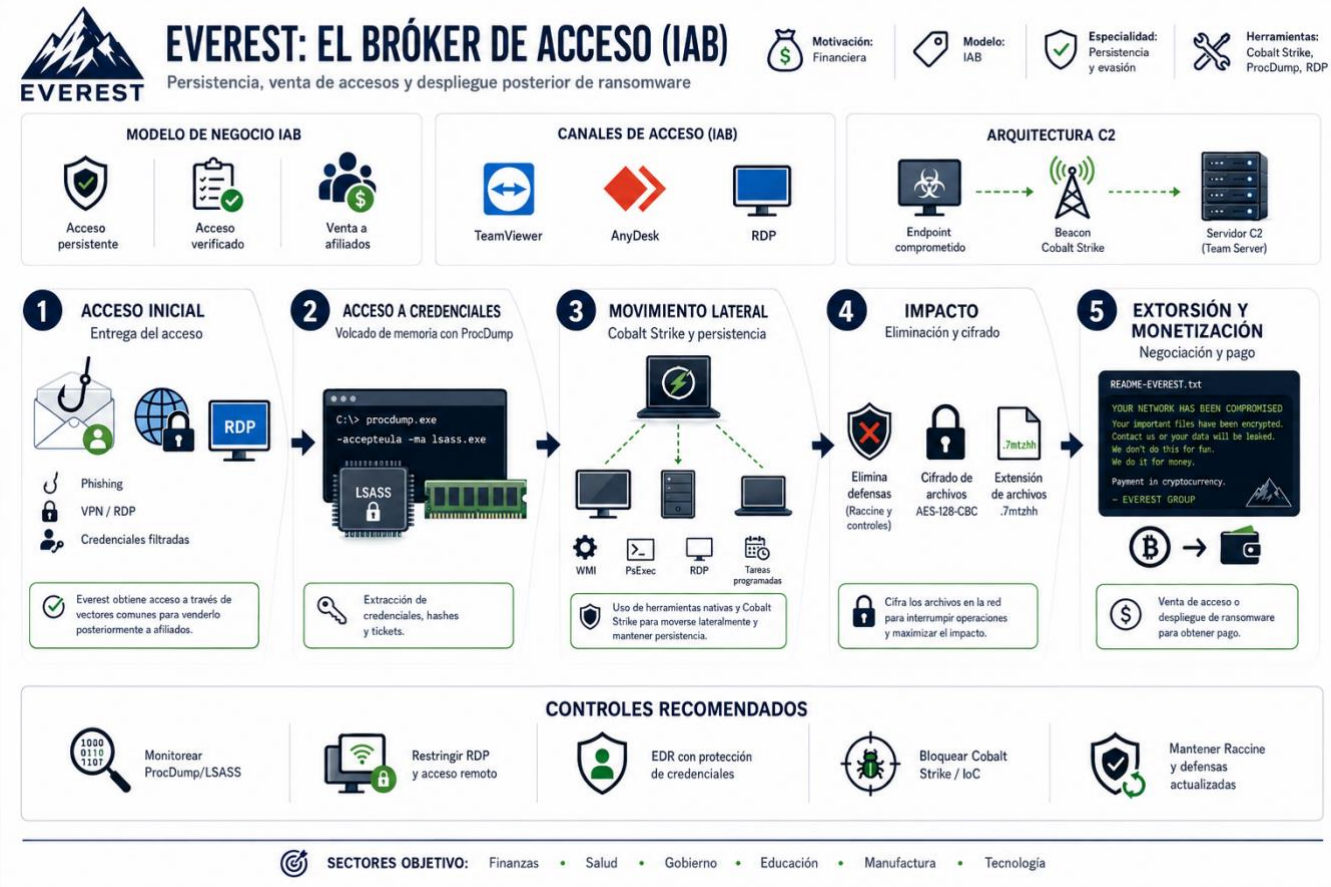


Figura 9. Cadena operacional sintetizada de Everest.

8. Kill Security

De hacktivismo a RaaS multiplataforma

Prioridad: ALTA | **Estado:** ONLINE / actividad activa | **Primera actividad:** Octubre de 2023 (como colectivo hacktivista desde 2022; RaaS formal desde junio de 2024; agresividad creciente desde finales de 2024) | **Atribución:** Colectivo internacional/multilingüe, con origen hacktivista afín a Anonymous. Kill Security evolucionó desde un colectivo hacktivista hacia una operación RaaS con panel por Tor. El programa cobra una cuota de entrada de 250 USD y permite al afiliado retener hasta el 88 % de los ingresos, aunque las reglas declaran restricciones sobre infraestructura crítica, el sector salud aparece como la categoría más atacada, con 36 víctimas registradas.

Las variantes KillSecurity 2.0 y 3.0 incluyen capacidad para VMware ESXi, el actor explota servicios y aplicaciones públicas, incluida CVE-2025-31161 en CrushFTP, y también se beneficia de configuraciones abiertas en AWS S3 o Azure. El acceso conduce a exfiltración, despliegue del loader, Cobalt Strike, eliminación de Raccine y cifrado AES-128-CBC con extensiones configurables, incluida .killsec. **Cadena operacional documentada.** CrushFTP, nube expuesta o RDP → Loader y Cobalt Strike → Credenciales y movimiento lateral → Persistencia y C2 → Cifrado multiplataforma y extorsión

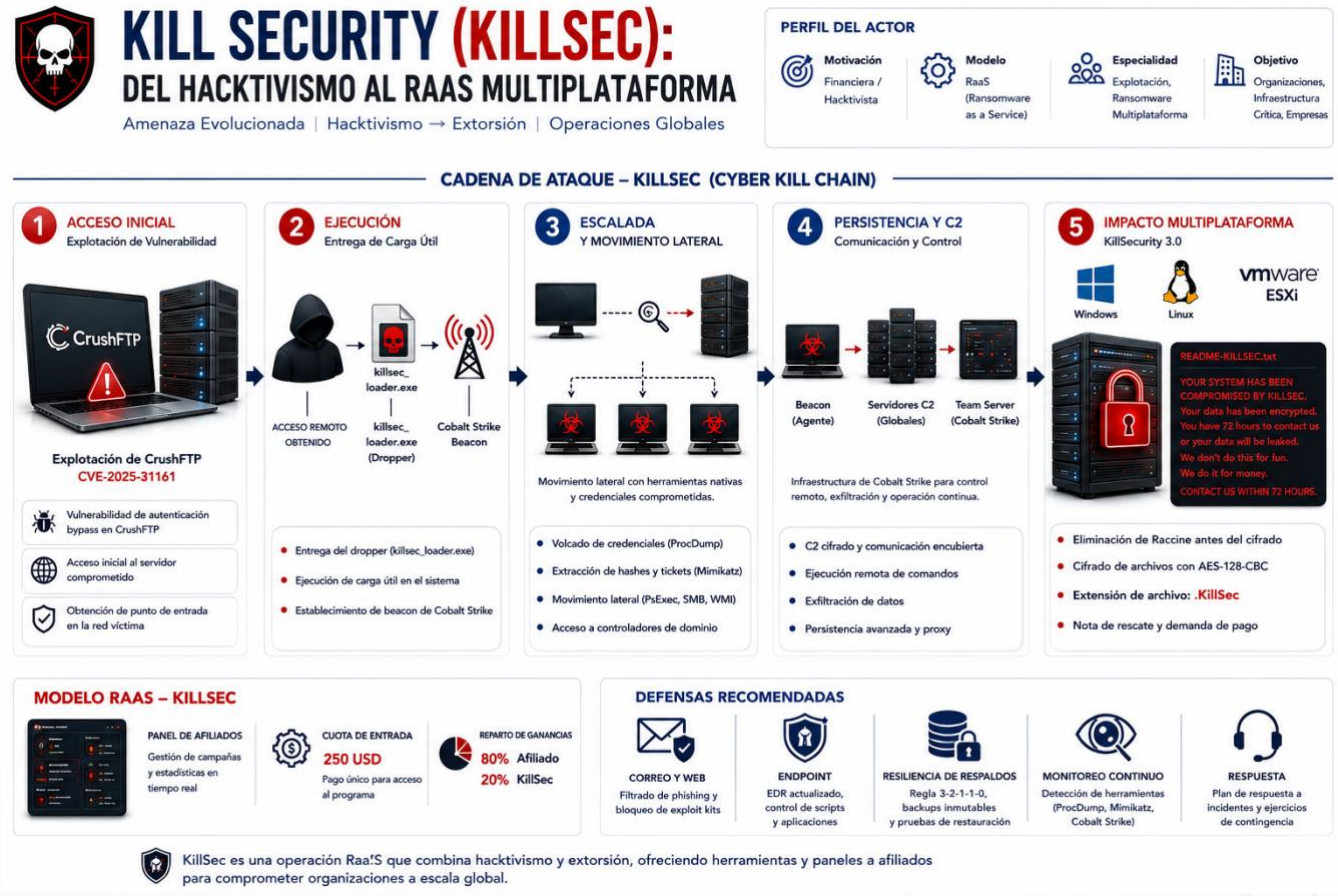


Figura 10. Cadena operacional sintetizada de Kill Security.

9. Crypto24

Evasión de EDR personalizada y exfiltración por servicios legítimos

Prioridad: ALTA | **Estado:** ONLINE / capacidades de evasión de EDR más sofisticadas | **Primera actividad:** Consolidación operativa documentada desde finales de 2024 / principios de 2025 | **Atribución:** Infraestructura multilingüe; sin atribución geográfica confirmada de forma independiente, aunque algunas fuentes sugieren posible nexo en Europa del Este.Crypto24 combina herramientas legítimas con componentes propios en una cadena de evasión especialmente elaborada. WinMainSvc.dll funciona como keylogger bajo svchost.exe; una modificación de termsrv.dll permite sesiones RDP concurrentes; y una versión personalizada de RealBlindingEDR identifica cerca de 30 fabricantes de seguridad y desactiva callbacks de detección en kernel.Con privilegios administrativos, el actor abusa de gpscript.exe para ejecutar el desinstalador oficial de Trend Vision One. PsExec, AnyDesk y TightVNC sostienen el movimiento lateral y el acceso persistente. La exfiltración se realiza hacia Google Drive mediante WinINet. El cifrado se ejecuta como el servicio MSRuntime.dll, agrega la extensión .crypto24 y deja la nota Decryption.txt. Las campañas suelen desarrollarse en horarios de baja actividad y completarse en cuestión de horas.

Cadena operacional documentada. Phishing, servicios expuestos o VPN/RDP → RealBlindingEDR y retiro del EDR → Reactivación de cuentas y persistencia → PsExec y acceso remoto → Keylogger, Google Drive y cifrado

Figura 11. Cadena operacional sintetizada de Crypto24.

10. NOVA

Linaje Babuk y técnicas de ejecución nativa

Prioridad: MEDIA | **Estado:** En reestructuración de infraestructura tras exposición pública | **Primera actividad:** Marzo de 2025 como RALord; rebranding a NOVA a mediados de 2025 | **Atribución:** Rusia/Ucrania

NOVA, conocido anteriormente como RALord, utiliza un cifrador derivado del código filtrado de Babuk. Tras un intento de extorsión fallido contra un laboratorio médico en los Países Bajos, investigadores expusieron direcciones IP de backend e identidades de reclutadores, el grupo respondió con rotación de infraestructura y un repliegue táctico; la fuente lo clasifica en reestructuración, no como inactivo.

La evidencia técnica se concentra en llamadas a la API nativa de Windows, evasión de hooks, secuestro del flujo de ejecución mediante Process Hollowing o Ghosting y persistencia a través de servicios, tareas programadas, registro y WMI. También registra explotación de aplicaciones públicas y reconocimiento de recursos compartidos.

Cadena operacional documentada. Ejecución mediante API nativas → Evasión de hooks y monitoreo → Inyección en procesos legítimos → Persistencia por servicios, tareas, registro y WMI → Uso de drivers vulnerables contra EDR

Figura 12. Cadena operacional sintetizada de NOVA.

Patrones transversales de la amenaza

Exposición perimetral como punto de entrada. RDP, VPN, WSUS, FortiGate, NetScaler, CrushFTP y aplicaciones web aparecen de forma reiterada. El problema no es una sola CVE, sino la permanencia de servicios críticos expuestos, segmentación y ciclos de parcheo verificables.

Credenciales válidas y administración remota. Mimikatz, ProcDump, sesiones RDP, AnyDesk, ScreenConnect, Zoho Assist y MeshAgent permiten que la actividad criminal se confunda con operaciones legítimas de TI. La telemetría debe evaluar usuario, horario, origen, destino y secuencia de acciones.

Neutralización del EDR. BYOVD, RealBlindingEDR, desinstaladores oficiales y utilidades de Windows muestran dos vías complementarias: operar en kernel o utilizar mecanismos legítimos en espacio de usuario. HVCI, WDAC y alertas sobre nuevos servicios de driver son controles prioritarios.

Exfiltración antes del cifrado. Google Drive, HTTPS, C2 y herramientas RMM se utilizan para retirar información antes del impacto. La doble extorsión convierte la confidencialidad en un problema independiente de la recuperación técnica.

Cifrado multiplataforma y ataque a respaldos. Windows, Linux y VMware ESXi aparecen en los actores de mayor prioridad. La eliminación de snapshots, servicios Veeam y copias de sombra busca impedir la restauración y aumentar la presión de pago.

Plan defensivo priorizado

Las medidas se organizan por factor de riesgo porque los actores comparten vectores, herramientas y dependencias. Cada bloque diferencia acciones inmediatas, mejoras estructurales y medidas de contención para un incidente activo.

Credenciales VPN y RDP expuestas

The Gentlemen, DragonForce, Anubis, Sarcoma, Everest y Crypto24 explotan con frecuencia este vector.

Acción inmediata: Eliminar la exposición directa de TCP/3389 y canalizar el acceso administrativo mediante un bastión auditado o VPN con MFA resistente a phishing (FIDO2/WebAuthn).
Mejora estructural: Auditar mensualmente portales VPN, aplicar rate limiting y geobloqueo cuando la operación no requiera acceso desde el exterior.
Contención: Rotar credenciales de VPN y RDP ante inicios de sesión desde ubicaciones o franjas horarias anómalas.

Vulnerabilidades críticas en infraestructura perimetral

El documento destaca CVE-2025-59287 en WSUS, CVE-2025-53770/CVE-2025-53771 en SharePoint, CVE-2024-55591 en FortiOS/FortiProxy y CVE-2025-5777 en Citrix NetScaler.

Acción inmediata: Verificar el parcheo de WSUS y SharePoint. Si WSUS no puede actualizarse, deshabilitar temporalmente el rol o limitar 8530/8531 a subredes de gestión confiables.
Mejora estructural: Asegurar WSUS con HTTPS/TLS; mantener FortiGate y NetScaler actualizados; y rotar las claves de máquina de SharePoint después de una sospecha de explotación.

Contención: Aislar el servicio perimetral comprometido, revisar cuentas creadas o modificadas y buscar ejecución remota con privilegios de sistema.

Evasión de EDR y BYOVD

LockBit y actores asociados emplean drivers vulnerables; Crypto24 combina RealBlindingEDR con gpscript.exe y desinstaladores legítimos.

Acción inmediata: Activar HVCI/Memory Integrity en estaciones y servidores Windows y aplicar la lista de bloqueo de drivers vulnerables mediante WDAC.
Mejora estructural: Restringir el privilegio de cargar drivers y controlar AppLocker/WDAC para gpscript.exe y desinstaladores de EDR fuera de mantenimiento autorizado.
Detección y contención: Alertar por evento 7045 cuando se cree un servicio de kernel fuera de C:\Windows\System32\drivers y correlacionar la invocación de desinstaladores con la detención de servicios de seguridad.

Almacenamiento en la nube

Kill Security explota configuraciones públicas o mal implementadas en AWS S3 y Azure; otros actores reutilizan servicios legítimos para exfiltración.

Acción inmediata: Eliminar permisos públicos no justificados en buckets y contenedores.
Mejora estructural: Automatizar auditorías de permisos, alertar ante ampliaciones de acceso y aplicar mínimo privilegio a credenciales de servicio.
Prioridad sectorial: Revisar con especial atención software de gestión hospitalaria, historias clínicas y cadenas de suministro que administren datos sensibles.

Exfiltración y doble extorsión

La extracción de información previa al cifrado es transversal a prácticamente todos los actores.

Acción inmediata: Configurar DLP en red y endpoint para transferencias masivas hacia repositorios no autorizados.
Mejora estructural: Establecer líneas base para Google Drive y herramientas RMM, con alertas por uso fuera de horario o desde hosts no habituales.
Contención: Revocar tokens, bloquear destinos, preservar evidencias y determinar el alcance de datos extraídos antes de iniciar la restauración.

Continuidad y recuperación

La recuperación debe diseñarse antes del incidente. El estándar 3-2-1-1-0 exige tres copias, dos soportes distintos, una copia fuera de sitio, una copia inmutable o desconectada y cero errores en las pruebas de restauración.

- Validar la integridad del respaldo en un entorno aislado antes de restaurar a producción.
- Cuando exista sospecha de persistencia, priorizar una restauración de datos sobre una imagen completa del sistema operativo.
- Desconectar físicamente los repositorios de respaldo ante una alerta activa de ransomware en el dominio.
- Documentar RTO, RPO, orden de recuperación y responsables de negocio para los servicios críticos.

Secuencia de recuperación segura. Primero se aísla la infraestructura de respaldo y se preserva la evidencia. Después se determina si el atacante mantuvo persistencia en el sistema, en identidades o en servicios centrales. La restauración se prueba en una red separada, se valida la integridad de los datos y solo entonces se habilita el servicio para usuarios. El retorno a producción debe realizarse por prioridades de negocio, no por orden de disponibilidad técnica.


ARQUITECTURA DE RESILIENCIA
EL ESTÁNDAR 3-2-1-1-0
ESTRATEGIA MULTICAPA CONTRA RANSOMWARE
Cinco principios para garantizar una recuperación verificable
3 COPIAS
Mantenga tres copias de los datos.
2 SOPORTES
Use dos tipos de medios diferentes.
1 FUERA DE SITIO
Conserve una copia fuera de su ubicación principal.
1 COPIA INMUTABLE
Proteja una copia aislada o inalterable.
0 ERRORES DE RESTAURACIÓN
Pruebe y verifique la restauración.
3 COPIAS
2 SOPORTES
DISCO
CINTA
1 FUERA DE SITIO
DATOS CRÍTICOS
1 COPIA INMUTABLE
AIR-GAPPED
0 ERRORES DE RESTAURACIÓN
ÉXITO
BENEFICIOS CLAVE
MÁXIMA RESILIENCIA
Protección ante ransomware y fallos.
RECUPERACIÓN VERIFICADA
Disponibilidad y continuidad operacional.
REDUCCIÓN DE RIESGOS
Menor impacto económico y operativo.
CUMPLIMIENTO NORMATIVO
Alineación con buenas prácticas.
CONFIANZA OPERACIONAL
Datos disponibles cuando se necesitan.

Conclusión

A julio de 2026, el riesgo de ransomware para Colombia combina concentración y diversidad. LockBit y The Gentlemen reúnen una parte sustancial de las víctimas, pero el resto del ecosistema aporta especialidades que amplían la amenaza: DragonForce habilita marcas de terceros; Everest comercializa accesos; Anubis incorpora destrucción irreversible; Crypto24 neutraliza EDR; y Dire Wolf acelera el impacto mediante cifrado selectivo y ataque a respaldos.

La tendencia muestra una mayor presión sobre infraestructura crítica, continuidad del crecimiento del grupo The Gentlemen y persistencia de actores oportunistas sobre la misma superficie perimetral, esta proyección no implica que todos los grupos ejecuten campañas simultáneas en el país; lo que sí indica es que las organizaciones colombianas comparten condiciones de exposición que distintos afiliados pueden reutilizar.

La respuesta más eficaz no consiste en perseguir cada grupo de ransomware por separado, consiste en cerrar los vectores recurrentes, proteger identidades y administración remota, impedir la neutralización del EDR, detectar exfiltración y demostrar que la organización puede restaurar servicios críticos sin depender del atacante.

Fuentes de consulta

- Check Point Research. (2026, 14 de mayo). Thus Spoke... The Gentlemen. Check Point Research. https://research.checkpoint.com/2026/thus-spoke-the-gentlemen/
- Halcyon.ai. (2026, 4 de mayo). Threat assessment: The Gentlemen ransomware group. Halcyon. https://www.halcyon.ai/ransomware-research-reports/threat-assessment-the-gentlemen-ransomware-group
- Unit 42, Palo Alto Networks. (2026, julio). No manners here: The ruthless rise of The Gentlemen ransomware. https://unit42.paloaltonetworks.com/the-gentlemen-ransomware/
- The Hacker News. (2025, 9 de octubre). LockBit, Qilin, and DragonForce join forces to dominate the ransomware ecosystem. https://thehackernews.com/2025/10/lockbit-qilin-and-dragonforce-join.html
- Unit 42, Palo Alto Networks. (2026, 19 de febrero, actualizado). Microsoft WSUS remote code execution (CVE-2025-59287) actively exploited in the wild. https://unit42.paloaltonetworks.com/microsoft-cve-2025-59287/
- ReliaQuest. (2026, 24 de julio). The Gentlemen ransomware group emerges as most active threat actor in Q2. The Insurer / ReliaQuest Threat Research. https://www.theinsurer.com/cyber-risk/news/the-gentlemen-ransomware-group-emerges-as-most-active-threat-actor-in-q2-2026-07-24/
- Trend Micro. (2025, agosto–octubre). Unmasking The Gentlemen ransomware. https://www.trendmicro.com/en_us/research/25/i/unmasking-the-gentlemen-ransomware.html

- Group-IB. (2026, 19 de marzo). Hastalamuerte leak exposes The Gentlemen RaaS TTPs. https://www.group-ib.com/blog/hastalamuerte-gentlemen-raas-ttps/
- Check Point Research. (2026, mayo). DFIR report: The Gentlemen. https://research.checkpoint.com/2026/dfir-report-the-gentlemen/
- MITRE Corporation. (s. f.). MITRE ATT&CK Enterprise Matrix. https://attack.mitre.org

Anexo técnico. Indicadores de compromiso

A continuación, se comparten los indicadores asociados a los grupos documentados en este boletín. Los dominios Tor y la infraestructura de C2 pueden rotar.

The Gentlemen

Categoría	Indicador	Descripción / función
Dirección IP	45.86.230[.]112	Servidor central de base de datos de túneles de red SOCKS5.
Dirección IP	193.233.202[.]17:44729	Puerto de control activo de SystemBC.
Dirección IP	77.110.122[.]137:37182	Canal de comunicaciones cifradas de agentes comprometidos.
Dirección IP	91.107.247[.]163	Servidor de Comando y Control (C2).
Dominio	assets.adobedtm.com	Dominio legítimo contactado por los binarios para validar conectividad o descargar recursos de soporte.
Dominio	a1672.dscr.akamai.net	Dominio legítimo utilizado durante la actividad de red observada.
Dominio	globalsign.com	Dominio utilizado para validación de certificados y conectividad.
Dominio	ocsp2.globalsign.com	Servicio OCSP para validación de certificados digitales.
Dominio	mozilla.map.fastly.net	Dominio legítimo contactado durante el análisis de comportamiento.
Hash SHA-256	16f83f056177c4ec24c7e99d01ca9d9d6713bd0497eeedb777a3ffefa99c97f0	Nombres comunes: ThrottleStop.sys / ThrottleBlood.sys.Función: Controlador firmado abusado para finalizar procesos EDR/AV críticos en modo kernel (BYOVD).
Hash SHA-256	206f27ae820783b7755bca89f83a0fe096dbb510018dd65b63fc80bd20c03261	Nombres comunes: NSecKrnl.sys / NSecKrnl64.sys.Función: Framework "NSec-Killer" utilizado para deshabilitar defensas activas del host.
Hash SHA-256	2d91a78e739891c9854c254f5b2a6b84c0e167dfa253466cbccd2cdd1c20145d	Nombres comunes: g11.sys / l6o3a.exe.Función: Módulo de evasión adaptado contra agentes locales de seguridad.
Hash SHA-256	3414671bc9470a0cb007fec51c735fff91d4b29e588ef55518f9895e304419d3	Nombres comunes: SentinelInstaller.exe / ly5ps0.exe.Función: Instalador falso que se hace pasar por software de monitoreo legítimo.
Hash SHA-256	534bd6b99ed0e40ccbefad1656f03cc56dd9cc3f6d990cd7cb87af4cceebe144	Nombres comunes: SophosInstall.exe / azm4ddxh.exe.Función: Binario malicioso que suplanta software de Sophos para ocultar el despliegue de agentes.
Hash SHA-256	50f2cdf16f05da9253fa2d6eb60d5a42da14c02c551c0874c9e953d4119da69c	Nombres comunes: SophosInstall.exe / d421cuu5e.exe.Función: Ejecutable de soporte de intrusión asociado a mecanismos de persistencia.

DragonForce

Categoría	Indicador	Descripción / función
Dirección IP	185.59.221[.]75	Servidor de Comando y Control (C2) utilizado como nodo de exfiltración de información y entrega de herramientas de post-explotación (p. ej., Cobalt Strike).

Categoría	Indicador	Descripción / función
Dirección IP	185.73.125[.]8	Servidor de Comando y Control (C2) utilizado para exfiltración de datos y distribución de herramientas de post-explotación.
Dirección IP	69.4.234[.]20	Nodo de infraestructura C2 asociado con la entrega de payloads y balizas de post-explotación.
Dirección IP	94.232.46[.]202	Servidor utilizado para comunicaciones de Comando y Control y exfiltración de información.
Dirección IP	2.147.68[.]96	Nodo de infraestructura C2 empleado para la comunicación con sistemas comprometidos.
Hash SHA-256	1250ba6f25fd60077f698a2617c15f89d58c1867339bfd9ee8ab19ce9943304b	Nombres comunes: malware_sample_dragonforce, localfile~.Detalle: Muestra nativa del ransomware DragonForce compilada para Windows, con alta tasa de detección (64/70).
Hash SHA-256	9f1f11a708d393e0a4109ae189bc64f1f3e312653dcf317a2bd406f18ffcc507	Nombres comunes: VID001.exe, %APPDATA%\TempoRX\VID001.exe.Detalle: Payload troyanizado utilizado para establecer la persistencia inicial en el sistema.
Hash SHA-256	572d88c419c6ae75aeb784ceab327d040cb589903d6285bbffa77338111af14b	Nombres comunes: netscan.exe, netscanold.exe.Detalle: SoftPerfect Network Scanner utilizado para reconocimiento de red y descubrimiento de sistemas remotos.
Hash SHA-256	df903c620508011ca8eb2aaaf9712a526b31a12c800b856cd524ebb3fde854b2	Nombres comunes: svchost.exe, socks.exe.Detalle: Módulo proxy de tunelización empleado para mantener canales redundantes de Comando y Control.
Hash SHA-256	a31f222fc283227f5e7988d1ad9c0aecd66d58bb7b4d8518ae23e110308dbf91	Nombres comunes: img001.exe, C:\img001.exe.Detalle: Dropper/Loader utilizado para la recopilación de credenciales en memoria durante la intrusión.
Hash SHA-256	55befb5de5d9bc45978efd1a960ae21ed81e4be9c6521aaeebf8d5884444e3c9	Nombres comunes: example.txt, $R7V4EN7.exe.Detalle: Inyector malicioso con técnicas de ocultación de ventanas para evadir entornos sandbox.
Hash SHA-256	4b97d71e039d4ba71c7e9c9dfd1d447f0b984984e424eb8b720e182f46ba6c10	Detalle: Código base derivado de LockBit/Conti utilizado como herramienta directa de cifrado.
URL	https://46.29.238[.]160/	Servidor de alojamiento y descarga directa de payloads y scripts modificados utilizados por afiliados de DragonForce.

LockBit 5.0

Categoría	Indicador	Descripción / función
Hash SHA-256	0c7466ed8b51f0a769a7f85ad4b88c3770d71c4863322fa38429ccbf3d56ab06	Módulo del ransomware para sistemas Unix/ESXi.
Hash SHA-256	21aab3925870f8e11cf4c94b9b84d252118278a50206e622b8148001e205213f	Módulo del ransomware para sistemas Unix/ESXi.
Controlador vulnerable (BYOVD)	gdrv.sys	Controlador vulnerable asociado a técnicas Bring Your Own Vulnerable Driver (BYOVD). Vulnerabilidad conocida CVE-2018-19320.

Categoría	Indicador	Descripción / función
Controlador vulnerable (BYOVD)	mhyprot2.sys	Controlador vulnerable reportado en campañas que emplean técnicas BYOVD para evasión de mecanismos de seguridad.
Controlador vulnerable (BYOVD)	aswArPot.sys	Controlador vulnerable utilizado en campañas con técnicas BYOVD para obtener privilegios elevados y deshabilitar controles de seguridad.

Anubis

Categoría	Indicador	Descripción / función
Dominio	bosstan027.beget[.]tech	Portal de afiliación o distribución de scripts utilizado por la infraestructura RaaS.
Dominio	tryagain.beget[.]tech	Dominio asociado a la infraestructura de soporte y distribución de herramientas.
Dominio	ktosdelaetskrintotpidor[.]com	Dominio empleado como parte de la infraestructura web de soporte o control.
Dominio	sositehuypidarasi[.]com	Dominio relacionado con la infraestructura de operación y comunicaciones.
Dominio	www.playprotectupdate[.]top	Dominio utilizado para alojamiento o distribución de componentes maliciosos.
Dominio	www.androidmarket[.]top	Dominio utilizado para distribuir archivos o facilitar la infraestructura de ataque.
Dominio	atlanaserx.temp.swtest[.]ru	Dominio asociado con infraestructura temporal de soporte y enrutamiento web.
Dominio	browerasew.temp.swtest[.]ru	Dominio utilizado en la infraestructura de control y soporte.
Dominio	chegesov41.temp.swtest[.]ru	Dominio asociado a la infraestructura de operación de la campaña.
Dominio	putinetosm.temp.swtest[.]ru	Dominio utilizado para soporte y comunicaciones de la infraestructura.
Dominio	rewwaresrm.temp.swtest[.]ru	Dominio empleado para alojamiento o control de herramientas RMM.
Dominio	www.rootbot[.]ug	Dominio vinculado a la infraestructura de soporte utilizada por los operadores de RaaS.
Hash SHA-256	065316e6091a34c1f14cdb29a8cb0ee4ae737addd57ff06d28c16ca7f00444e3	Ruta / Nombre común: C:\Windows\3i8ye.exe.Comportamiento: Binario ejecutable Sphinx/Anubis diseñado para interactuar con sistemas Windows.
Hash SHA-256	095ad66f00afd582c2d5259671f748344b8150049dcabd9fe23f0785ac7d627d	Ruta / Nombre común: C:\Windows\ztko93555.exe.Comportamiento: Ejecutable compilado en Go con rutinas de evasión y eliminación de Volume Shadow Copies.
Hash SHA-256	1479c5d0297a895ef50c8ecb8576e01daf030834ef26e1775b17050d013354f8	Ruta / Nombre común: C:\Windows\nf0la6mgv.exe.Comportamiento: Loader utilizado para elevar privilegios e inyectar rutinas de cifrado ECIES.
Hash SHA-256	01c0e31fe5ce6b487628d9d266827e5b83635dc97b51f85f623e621ed5fd1a36	Ruta / Nombre común: classes.dex.Comportamiento: Archivo de soporte y empaquetamiento empleado en fases de reconocimiento multiplataforma.
Hash SHA-256	22ec96b1c7be75aa68a5cef65be34dc5bcda8280bb8762c3e04a0d5531f95916	Comportamiento: Cargador (loader) intermedio utilizado para evadir la detección por soluciones antivirus tradicionales.

Space Bears

No se documentan públicamente indicadores de alta confianza específicos de este actor; el indicador operativo más estable es el propio dominio del portal de filtraciones en TOR, sujeto a rotación.

Dire Wolf

Categoría	Indicador	Descripción / función
Hash SHA-256	8fdee53152ec985ffeeeda3d7a85852eb5c9902d2d480449421b4939b1904aad	Tipo: PE64 Executable.Nombre común: data345.exe / direwolf_ransom.bin.Descripción: Binario principal asociado al ransomware SNOWFANG (Dire Wolf).
Hash SHA-256	27d90611f005db3a25a4211cf8f69fb46097c6c374905d7207b30e87d296e1b3	Tipo: PE64 Executable.Nombre común: data345.exe (unpacked).Descripción: Versión desempaquetada del ejecutable principal.
Hash SHA-256	f0a85f105fa178ffa862bd3fdbc6b7ec642dd46189a10e14786c802fac8978e9	Tipo: PE64 Executable.Nombre común: sfy601.exe.Descripción: Muestra identificada de la familia SNOWFANG (Dire Wolf).
Hash SHA-256	950031040990dcac28adeb03f0c0ebbef3e31c8666a5d6573741489280c18216	Tipo: PE64 Executable.Nombre común: 567c7s9o.exe.Descripción: Ejecutable personalizado utilizado en campañas del ransomware.
Hash SHA-256	b6fa7a34b57803d2b80f3f484656d34997231597b6c1aa7fc8a386d6474c8afe	Tipo: PE64 Executable.Nombre común: dttcodexgigas....Descripción: Variante personalizada del ransomware adaptada a la víctima.
Mutex	Global\direwolfAppMutex	Mutex utilizado para verificar que solo una instancia del ransomware se ejecute en el sistema comprometido.
Archivo de marcador	C:\runfinish.exe	Archivo vacío creado al finalizar el proceso de cifrado para evitar una segunda ejecución del ransomware.
Extensión de archivo cifrado	.direwolf	Extensión agregada por el ransomware a los archivos cifrados.
Nota de rescate	HowToRecoveryFiles.txt	Archivo de instrucciones dejado por los operadores de RaaS para el pago y recuperación de los datos.
Tox ID	B344BECDC01A1282F69CB82979F40439E15E1FD1EF1FE9748EE467F5869E2148E6F1E55959E2	Identificador Tox utilizado por los atacantes como canal de contacto y soporte para la negociación del rescate.

Everest

Canal de negociación: mensajería cifrada descentralizada Qtox, reportado de forma consistente en múltiples incidentes internacionales del actor. No se documentan públicamente indicadores de alta confianza vigentes; al operar también como bróker de acceso, el indicador más relevante es la aparición de anuncios de venta de acceso a organizaciones en foros clandestinos monitoreados, más que un binario específico.

Kill Security

Categoría	Indicador	Descripción / función
Dominio Tor (.onion)	ks5424y3wpr5zlug5c7i6svvxweinhbdcqcfnptkfcutrncfazzgz5id.onion	Dirección activa del Data Leak Site (DLS) utilizado por Kill Security para publicar información de las víctimas.
Dominio Tor (.onion)	kill432ltnkqvaqntbalnsgojqqs2wz4lhnamrqjg66tq6fuvcztilyd.onion	Panel de control de afiliados y plataforma alternativa de Ransomware-as-a-Service (RaaS).
Dirección IP	82.147.84.98	Servidor de alojamiento relacionado con actividades de exfiltración de información.
Dirección IP	77.91.77.187	Servidor de Comando y Control (C2) utilizado como infraestructura de soporte y tránsito de tráfico de extorsión.
Dirección IP	93.123.39.65	Pasarela de comunicación identificada en incidentes recientes vinculados a Kill Security.
Nota de rescate	README.txt	Archivo de instrucciones de rescate dejado por el ransomware en los sistemas comprometidos.
Nota de rescate	!KillSec_Instructions.txt	Variante de la nota de rescate utilizada por operadores de RaaS o afiliados de Kill Security.
Extensión de archivo cifrado	.killsec (y variantes dinámicas)	Extensión agregada a los archivos cifrados. Los afiliados pueden configurar extensiones personalizadas para cada campaña o víctima.

Crypto24

Categoría	Indicador	Descripción / función
Hash SHA-256	ebf0511c2738bb423dfed1dabd3d726d3f88c2600e010b597a1fb51f61bfac4d	Nombre común: Decryptor.exe / Decryptor_new.exe.Descripción: Herramienta oficial de descifrado de Crypto24, protegida mediante VMProtect.
Hash SHA-256	fbcf8d16846ed21a578bfde02a768bfefd14d964629db8d4ccd5eb393a7fa994	Nombre común: Decryptor.exe.Descripción: Compilación alternativa del binario descifrador de Crypto24.
Hash SHA-256	3b0b4a11ad576588bae809ebb546b4d985ef9f37ed335ca5e2ba6b886d997bac	Nombre común: MSRuntime.dll.Descripción: Biblioteca dinámica principal del ransomware Crypto24.
Hash SHA-256	686bb5ee371733ab7908c2f3ea1ee76791080f3a4e61afe8b97c2a57fbc2efac	Nombre común: WinMainSvc.dll.Descripción: Binario del keylogger utilizado para espionaje y recolección de credenciales.
Hash SHA-256	24f7b66c88ba085d77c5bd386c0a0ac3b78793c0e47819a0576b60a67adc7b73	Nombre común: AVB.exe.Descripción: Variante personalizada de la herramienta de evasión RealBlindingEDR.
Servicio malicioso	WinMainSvc	Servicio utilizado para mantener persistencia del keylogger mediante sc.exe.
Servicio malicioso	MSRuntime	Servicio utilizado para mantener persistencia del ransomware, presentado como Microsoft Runtime Manager.
Ruta de archivo	%ProgramData%\Update\update.vbs	Script VBS utilizado para establecer persistencia en el sistema.
Ruta de archivo	%ProgramData%\Update\vm.bat	Script por lotes empleado para la ejecución silenciosa del cargador (loader).

Categoría	Indicador	Descripción / función
Ruta de archivo	%USERPROFILE%\AppData\Local\Temp\Low\AVB.exe	Ubicación habitual del ejecutable RealBlindingEDR utilizado para evasión de defensas.
Ruta de archivo	1.bat	Script por lotes inicial utilizado para reconocimiento local mediante WMIC y preparación de la intrusión.

NOVA

Categoría	Indicador	Descripción / función
Vector de ataque	Dogo_vor.exe	Ejecutable malicioso distribuido mediante campañas de phishing, camuflado como un supuesto contrato y enviado por correo electrónico a departamentos administrativos.
Comando de evasión	Add-MpPreference -ExclusionPath "C:\Users\%USERNAME%\AppData\Roaming\%FILENAME%.exe"	Comando de PowerShell utilizado para agregar una exclusión en Microsoft Defender y evitar la detección del malware antes de ejecutar el payload final.
Hash SHA-256	456b9adaabae9f3dce2207aa71410987f0a571cd8c11f2e7b41468501a863606	Nombre común: Muestra principal de Nova Ransomware (RALord).
Hash MD5	be15f62d14d1cbe2aecce8396f4c6289	Descripción: Firma MD5 del locker original de Nova.
Dominio Tor (.onion)	novavdivko2zvtrvtllnq45lxhba2rfzp76qigb4nrliklem5au7czqd.onion	Sitio principal de filtración de datos (Data Leak Site) utilizado por el grupo para publicar información de víctimas en Europa y Asia.
Dominio Tor (.onion)	novadmrkp4vbk2padk5t6pbxolndceuc7hrcq4mjaoyed6nxsqiuzyyd.onion	Portal secundario de extorsión utilizado por los operadores del ransomware.
Dominio Tor (.onion)	leak7y2247fj7dbb35rpfyxuyaqtwbshiwxp6h35ttzlhrxmhvi4fead.onion	Portal alternativo de filtración de datos utilizado para publicar información robada.