Alerta ID:	089
Fecha del reporte:	07/04/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	Operaciones Rápidas del Grupo Storm-1175 y Ransomware Medusa
Herramienta de detección	N/A
Activo involucrado:	sistemas expuestos a internet
Tipo de alerta:	Boletín informativo
Nivel de riesgo:	Alta

Resumen ejecutivo

Informar a las entidades del Ecosistema Digital sobre las recientes campañas del actor de amenazas Storm-1175. Este documento tiene como fin preparar a los equipos de defensa frente a la explotación de vulnerabilidades de día cero (zero-day) en sistemas expuestos a internet, una táctica que este grupo utiliza para comprometer redes de forma acelerada y desplegar el ransomware Medusa.

Descripción:

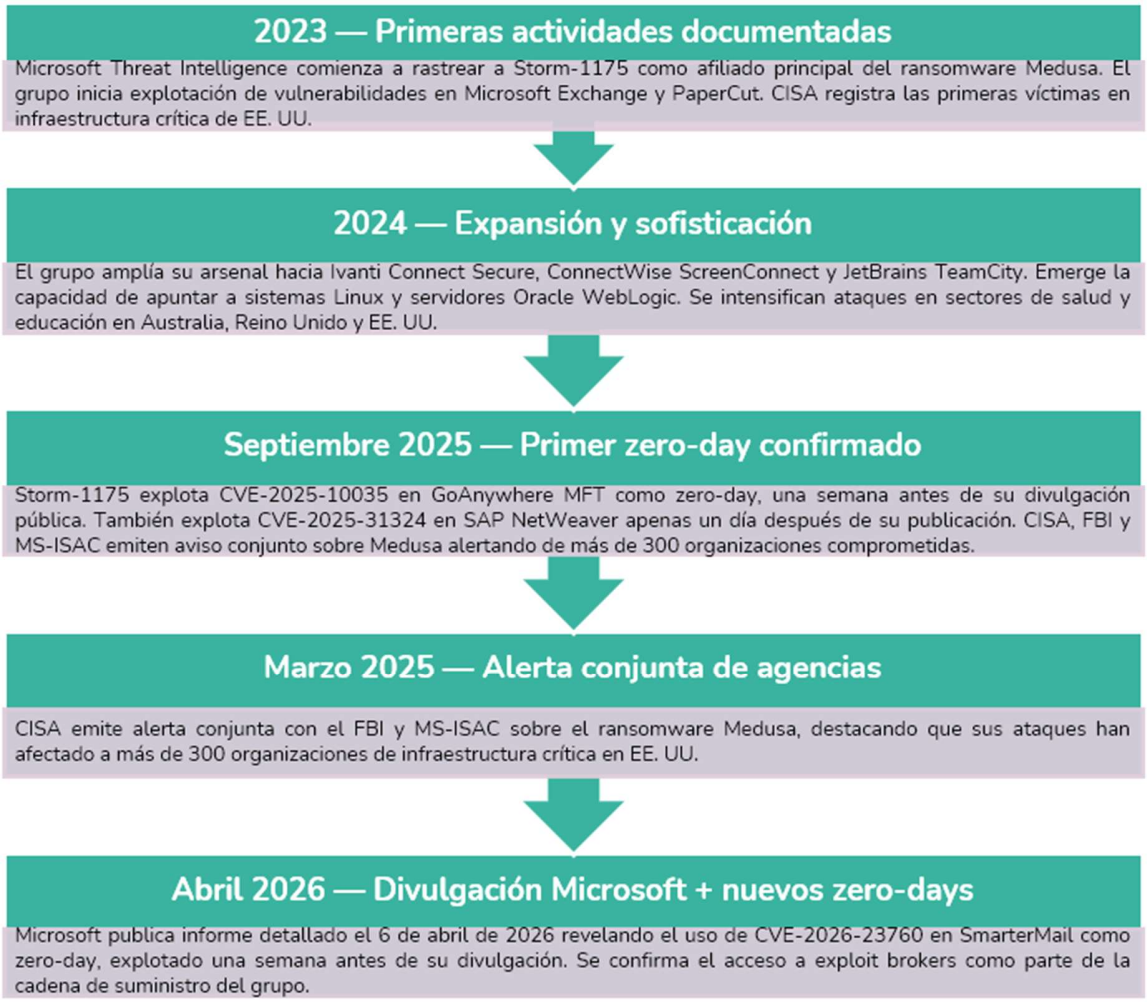
Las campañas de Storm-1175 se caracterizan por una velocidad de ataque crítica ("high-velocity"). Inician con la explotación de fallos de seguridad (tanto de día cero como vulnerabilidades recién publicadas) en aplicaciones perimetrales web. La gravedad radica en la ventana de tiempo: el actor de amenazas es capaz de pasar del acceso inicial al robo masivo de datos y la ejecución del ransomware Medusa en un periodo que oscila entre 24 horas y cinco días, dejando un margen de respuesta defensiva casi nulo.

El modelo de extorsión empleado es el de **doble extorsión**: primero roban datos sensibles y luego los cifran, amenazando con publicarlos en su sitio de filtraciones si la víctima no paga el rescate. Este enfoque maximiza la presión sobre las organizaciones víctimas.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Historia del grupo

Identificado por la Inteligencia de Amenazas de Microsoft, Storm-1175 es un grupo cibercriminal de motivación financiera que opera como un afiliado altamente sofisticado del ransomware Medusa (Ransomware-as-a-Service o RaaS). Operan agresivamente desde al menos 2023 y su firma distintiva es operar como un "oleoducto bien engrasado": capitalizan el tiempo que tardan las organizaciones en aplicar parches a sistemas expuestos para infiltrarse. Históricamente, se especializan en aprovechar vulnerabilidades de componentes empresariales comunes.



CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Cómo Operan

- **Reconocimiento y selección de objetivos**

Utilizan interfaces de escaneo público (Shodan, Censys, FOFA) para identificar activos con interfaces web expuestas. Se especializan en identificar versiones sin parches de software durante la ventana post-divulgación de CVE. En algunos casos, su capacidad de fingerprinting permite identificar stacks tecnológicos complejos y encadenar múltiples exploits.

- **Acceso inicial y establecimiento de beaconing**

Aprovechan exploits publicados (N-days) o en ocasiones zero-days adquiridos a través de brokers. Tras el compromiso inicial, despliegan herramientas RMM legítimas como SimpleHelp y MeshAgent para establecer comunicación persistente con el C2. En ataques documentados han encadenado exploits, como la técnica OWASSRF, para actividad post-compromiso.

- **Movimiento lateral y robo de credenciales**

Utilizan PDQ Deployer para distribución silenciosa de herramientas y cargas maliciosas. Emplean Impacket para movimiento lateral vía PSExec/WMI. Roban credenciales mediante volcado de LSASS con Impacket y Mimikatz. Habilitan WDigest credential caching mediante registro de Windows. Pivotan hacia controladores de dominio para extraer NTDS.dit y SAM para cracking offline.

- **Evasión de defensas y exfiltración**

Modifican configuraciones del Registro de Windows para Microsoft Defender Antivirus, añadiendo exclusiones totales (ej. exclusión de C:\). Comprimen datos de alto valor con utilidades como Bandizip. Usan Rclone para exfiltración continúa hacia almacenamiento en la nube controlado por los atacantes. La exfiltración ocurre a lo largo de todas las etapas del ataque sin requerir interacción del atacante.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- **Despliegue del ransomware Medusa**

Despliegan Medusa a través de PDQ Deployer scripts o actualizaciones de Políticas de Grupo (GPO), cifrando sistemas en toda la red. El modelo de doble extorsión combina cifrado de archivos con amenaza de publicación de datos robados en el sitio de filtraciones de Medusa. El rescate es exigido bajo amenaza doble: pérdida de acceso a datos y daño reputacional por la publicación pública de información sensible.

Modo de explotación detallado.

El proceso de explotación de Storm-1175 sigue una metodología altamente estructurada y repetible, con tiempos de operación progresivamente más cortos:

Fase 1 — Monitoreo y adquisición del exploit (días/horas antes del parche)
El grupo monitorea activamente canales de divulgación de vulnerabilidades: avisos de fabricantes, publicaciones en NVD/NIST, PoC en plataformas como GitHub y comunicados de CISA. En el caso de zero-days (CVE-2025-10035, CVE-2026-23760), la evidencia apunta a la adquisición de exploits a través de brokers especializados o al desarrollo propio facilitado por similitudes con vulnerabilidades previas. Una vez identificada la vulnerabilidad, arman el exploit en horas o días.

Fase 2 — Escaneo masivo y fingerprinting de objetivos
Realizan escaneos perimetrales usando interfaces públicas (Shodan, Censys) para identificar instancias del software afectado expuestas a internet. El fingerprinting avanzado les permite verificar versiones vulnerables específicas. Priorizan objetivos con alto valor (salud, finanzas, educación) y seleccionan múltiples víctimas simultáneamente para maximizar el rendimiento de la campaña. En el caso de SAP NetWeaver (CVE-2025-31324), iniciaron explotación activa apenas 1 día después de la publicación del aviso de SAP el 24 de abril de 2025.

Fase 3 — Explotación del activo web y acceso inicial
El vector de acceso inicial es siempre un activo web expuesto a internet: servidores de correo electrónico, gateways de acceso remoto, plataformas de transferencia de archivos gestionada

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

(MFT) o herramientas de gestión de TI. En vulnerabilidades de deserialización (GoAnywhere MFT CVE-2025-10035), el atacante envía una solicitud HTTP especialmente crafteada hacia el servlet de licencias del servidor, lo que desencadena la ejecución de código arbitrario sin necesidad de autenticación. En vulnerabilidades de omisión de autenticación (SmarterMail CVE-2026-23760), explotan fallas en la validación del flujo de autenticación para obtener acceso administrativo directo. Algunos ataques emplean la técnica OWASSRF (encadenamiento de exploits en Exchange) para actividad post-compromiso.

Fase 4 — Establecimiento de persistencia multicanal

Inmediatamente tras el acceso inicial: (a) crean nuevas cuentas de usuario con privilegios elevados; (b) despliegan web shells en el servidor comprometido para acceso persistente vía HTTP; (c) instalan software RMM legítimo (SimpleHelp, MeshAgent) que se camufla con tráfico de red normal; (d) establecen comunicación C2 usando beacons cifrados a través de los agentes RMM. La persistencia multicanal asegura que el cierre de un vector no elimine el acceso total.

Fase 5 — Escalación y dominio de la red interna

Con acceso establecido, inician movimiento lateral usando Impacket (PSExec, WMI) y RDP hacia sistemas internos. Vuelcan credenciales de LSASS con Impacket y Mimikatz. Habilitan WDigest caching para obtener contraseñas en texto plano en futuros inicios de sesión. Con credenciales de dominio, acceden a controladores de dominio para extraer NTDS.dit y SAM, permitiendo el cracking offline de todas las contraseñas del dominio. Distribuyen herramientas adicionales usando PDQ Deployer en modo silencioso.

Fase 6 — Exfiltración y evasión final

Antes de desplegar el ransomware, deshabilitan las defensas modificando el registro de Defender para excluir unidades completas (C:\). Identifican y comprimen datos de alto valor (bases de datos, archivos financieros, registros médicos, propiedad intelectual) usando Bandizip. Configuran Rclone para sincronización continua y automatizada hacia almacenamiento en la nube controlado por los atacantes. La exfiltración opera en paralelo con otras fases del ataque, asegurando que los datos sean robados antes del cifrado.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Fase 7 — Despliegue del ransomware Medusa

Despliegan el payload de Medusa a través de PDQ Deployer (scripts de instalación silenciosa) o mediante Políticas de Grupo (GPO) comprometidas, garantizando distribución masiva y simultánea en toda la red. Medusa cifra los archivos del sistema y deja notas de rescate. La víctima es contactada en el sitio de negociación de Medusa con plazos específicos y amenaza de publicación de datos en su sitio de filtraciones. El modelo RaaS permite que Storm-1175 reciba un porcentaje del pago del rescate, mientras el operador de Medusa gestiona la infraestructura de extorsión.

Indicadores de compromiso

Herramientas y binarios maliciosos observados

- PDQ Deployer (uso legítimo reaprovechado para distribución de payload).
- Impacket (lateral movement, credential dumping vía PSExec/WMI).
- Mimikatz (robo de credenciales, volcado LSASS).
- Rclone (exfiltración de datos hacia almacenamiento en la nube).
- Bandizip (compresión de datos previo a exfiltración).
- SimpleHelp / MeshAgent (RMM para C2 y persistencia).
- Netscan (reconocimiento de red interno).
- Web shells (persistencia en servidores web comprometidos).

Indicadores de comportamiento (TTP-based IOC)

- Creación súbita de nuevas cuentas de administrador local
  Modificación del registro: HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths → C:\
- WDigest habilitado: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest → UseLogonCredential = 1
- Acceso a LSASS desde procesos no reconocidos (credential dumping)
- Ejecución de Rclone con parámetros de sincronización hacia storage externo

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Actividad RDP hacia controladores de dominio desde hosts comprometidos
- Despliegue de GPO inusual o ejecución masiva vía PDQ Deployer
- Presencia de NTDS.dit o SAM fuera de rutas estándar del sistema

También durante las campañas de explotación rápida de vulnerabilidades (específicamente asociadas al fallo CVE-2025-10035 de GoAnywhere MFT), las plataformas de seguridad han rastreado el tráfico de ataque hacia las siguientes direcciones IP.

Indicador (IP)	Tipo	Contexto / Campaña
31.220.45.120	IPv4	Explotación de infraestructura y Comando/Control
213.183.63.41	IPv4	Explotación de infraestructura
206.168.190.143	IPv4	Explotación de infraestructura
31.222.247.64	IPv4	Explotación de infraestructura
144.168.41.74	IPv4	Explotación de infraestructura
172.96.10.212	IPv4	Explotación de infraestructura

Vulnerabilidades explotadas.

A continuación se detallan las principales vulnerabilidades explotadas por Storm-1175 desde 2023, con énfasis en los zero-days más recientes:

CVE	Producto afectado	Tipo	CVSS	Descripción
CVE-2026-23760	SmarterMail (SmarterTools)	Zero-Day	Crítico	Omisión de autenticación (authentication bypass) en el servidor de correo y colaboración SmarterMail. Explotada por Storm-1175 una semana antes de su divulgación pública. Similar estructuralmente a una vulnerabilidad previamente conocida del mismo producto, lo que facilitó su desarrollo o adquisición.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

CVE	Producto afectado	Tipo	CVSS	Descripción
CVE-2025-10035	GoAnywhere MFT (Fortra)	Zero-Day	Crítico	Vulnerabilidad de deserialización crítica en el servlet de licencias de GoAnywhere Managed File Transfer. Permite la ejecución remota de código sin autenticación en instancias expuestas a internet. Explotada una semana antes de su divulgación pública. GoAnywhere MFT había sido objetivo previo de ransomware (Clop), lo que facilitó el desarrollo del exploit.
CVE-2025-31324	SAP NetWeaver	N-Day (1 día)	Crítico 10.0	Vulnerabilidad crítica en SAP NetWeaver que permite carga de archivos no autorizada y ejecución remota de código. Storm-1175 armamentizó el exploit apenas un día después de la publicación del advisory oficial de SAP (24 de abril de 2025), demostrando la velocidad operacional del grupo.
CVE-2024-1709	ConnectWise ScreenConnect	N-Day	Crítico 10.0	Omisión de autenticación crítica que permite a atacantes remotos eludir completamente el control de acceso en ConnectWise ScreenConnect, obteniendo acceso administrativo a la plataforma de control remoto.
CVE-2024-1708	ConnectWise ScreenConnect	N-Day	Alto	Vulnerabilidad de path traversal que, encadenada con CVE-2024-1709, permite la escritura de archivos arbitrarios en el sistema de la víctima para lograr ejecución remota de código.
CVE-2023-46805	Ivanti Connect Secure / Policy Secure	N-Day	Alto 8.2	Omisión de autenticación en los endpoints de Ivanti Connect Secure y Policy Secure que permite a atacantes no autenticados acceder a recursos protegidos mediante falsificación de comprobaciones de control de acceso.
CVE-2024-21887	Ivanti Connect Secure / Policy Secure	N-Day	Crítico 9.1	Inyección de comandos en los componentes web de Ivanti que permite a administradores autenticados (o en combinación con CVE-2023-46805, a atacantes no autenticados) ejecutar comandos arbitrarios en el dispositivo.
CVE-2024-27198	JetBrains TeamCity	N-Day	Crítico 9.8	Omisión de autenticación en la interfaz web de JetBrains TeamCity que permite a atacantes remotos no autenticados tomar el control completo del servidor de CI/CD, incluyendo la ejecución de código en el contexto del servidor.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

CVE	Producto afectado	Tipo	CVSS	Descripción
CVE-2024-57726 / 57727 / 57728	SimpleHelp	N-Day	Alto	Cadena de vulnerabilidades en SimpleHelp que incluyen escalación de privilegios, acceso no autorizado a archivos y ejecución remota de código. SimpleHelp es una herramienta RMM legítima cuya compromisión permite a los atacantes usarla para movimiento lateral y persistencia.
CVE-2023-21529	Microsoft Exchange Server	N-Day	Alto 8.8	Vulnerabilidad de ejecución remota de código en Microsoft Exchange Server que puede ser explotada por un atacante autenticado con acceso de red. Parte de la cadena OWASSRF documentada en ataques de Storm-1175.
CVE-2023-27350 / 27351	PaperCut NG/MF	N-Day	Crítico 9.8	Omisión de autenticación y ejecución remota de código en las plataformas de gestión de impresión PaperCut, ampliamente usadas en entornos educativos y corporativos. Permiten tomar control completo del servidor desde internet sin credenciales.
CVE-2025-31161	CrushFTP	N-Day	Crítico	Vulnerabilidad crítica de omisión de autenticación en CrushFTP que permite a atacantes remotos no autenticados acceder al servidor de transferencia de archivos y ejecutar operaciones privilegiadas.
CVE-2026-1731	BeyondTrust	N-Day	Crítico	Vulnerabilidad crítica en la plataforma de gestión de acceso privilegiado (PAM) BeyondTrust. Su compromiso es especialmente grave ya que otorga acceso a credenciales privilegiadas almacenadas y gestionadas por la plataforma.
CVE-2025-52691	SmarterMail	N-Day	Alto	Vulnerabilidad adicional en SmarterMail, explotada por Storm-1175 como parte de su arsenal contra esta plataforma de comunicación empresarial, complementando el zero-day CVE-2026-23760.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Principales activos atacados.

Servidores de correo electrónico

Microsoft Exchange Server, SmarterMail — vectores de acceso inicial frecuentes por su exposición directa a internet

Gateways de acceso remoto

Ivanti Connect Secure, Policy Secure — soluciones VPN ampliamente usadas como perímetro de red

Plataformas MFT

GoAnywhere MFT, CrushFTP — herramientas de transferencia de archivos gestionada con alta exposición

Herramientas de gestión TI

ConnectWise ScreenConnect, SimpleHelp, BeyondTrust PAM — plataformas de administración remota y acceso privilegiado

Pipelines CI/CD

JetBrains TeamCity — objetivos de alta relevancia en entornos de desarrollo de software

ERP / Aplicaciones empresariales

SAP NetWeaver — plataformas de gestión empresarial críticas con alto valor para la extorsión

Gestión de impresión

PaperCut NG/MF — ampliamente usados en universidades y organizaciones educativas

Servidores Linux / Oracle

Oracle WebLogic en entornos Linux — objetivo desde finales de 2024, indicando expansión multiplataforma

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Recomendaciones

- Verificar la creación de nuevas cuentas con privilegios administrativos fuera de procesos aprobados. Monitorear cambios en HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions y en la clave WDigest (UseLogonCredential). Implementar detección de uso de Mimikatz e Impacket mediante reglas YARA/Sigma actualizadas.

- Implementar alertas para ejecución de Rclone, especialmente con parámetros de sincronización hacia servicios cloud externos (Mega, Dropbox, Google Drive, S3). Monitorear uso inusual de Bandizip o herramientas de compresión sobre volúmenes grandes de datos. Configurar DLP (Data Loss Prevention) para detectar transferencias masivas fuera del horario normal.

- Mantener inventario de herramientas RMM autorizadas. Alertar sobre instalación o ejecución de SimpleHelp, MeshAgent u otras herramientas RMM no aprobadas. Detectar actividad PSExec/WMI inusual entre hosts (especialmente hacia controladores de dominio). Registrar y analizar accesos RDP hacia servidores críticos desde fuentes no habituales.

- Usar herramientas de External Attack Surface Management (EASM) como Microsoft Defender EASM para mantener visibilidad continua de activos expuestos a internet. Suscribirse a feeds de inteligencia de vulnerabilidades (CISA KEV, Microsoft MSRC) para identificar nuevas CVEs que afecten al inventario de software. Establecer SLA de parcheo de 24-48 horas para vulnerabilidades críticas en activos web expuestos.

- Aplicar con urgencia los parches para todos los CVEs listados en este boletín, priorizando los activos expuestos a internet. Si el parche no está disponible, aplicar mitigaciones temporales: aislar el sistema detrás de VPN, desactivar funcionalidades vulnerables o desconectar temporalmente de internet. Documentar el inventario completo de versiones de software expuesto.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Colocar todos los activos web detrás de WAF (Web Application Firewall) y proxies inversos. Requerir VPN para acceso a sistemas de gestión interna. Implementar DMZ para separar activos expuestos de la red interna. Habilitar reglas de reducción de superficie de ataque en Microsoft Defender para bloquear PSExec/WMI y otras técnicas de Impacket.

- Implementar segmentación de red estricta para limitar el movimiento lateral en caso de compromiso. Restringir el acceso de cuentas de servicio a los mínimos permisos necesarios. Proteger controladores de dominio con acceso restringido y monitoreo intensivo. Auditar regularmente cuentas con privilegios elevados y deshabilitar las no usadas.

Fuentes:

- **Microsoft Security Blog:** *"Storm-1175 focuses gaze on vulnerable web-facing assets in high-tempo Medusa ransomware operations"* (6 de abril de 2026). Esta es la fuente primaria que detalla la velocidad del ataque, las tácticas de evasión (como la modificación de Windows Defender) y el uso de herramientas como Rclone y el comando net.
- **Microsoft News Center LATAM:** *"Storm-1175 centra la atención en activos vulnerables que se conectan a la web en operaciones de ransomware Medusa de alta velocidad"* (6 de abril de 2026). Versión oficial en español del reporte de Microsoft Threat Intelligence.
- **The Hacker News:** *"China-Linked Storm-1175 Exploits Zero-Days to Rapidly Deploy Medusa Ransomware"* (7 de abril de 2026). Fuente que complementa la información sobre las herramientas específicas de robo de credenciales (*Impacket*, *Mimikatz*) y la lista histórica de vulnerabilidades explotadas.
- **Hive Pro Threat Advisory / Security Affairs:** *"CVE-2025-10035 Exploit: Storm-1175 Attack on GoAnywhere MFT"*. De aquí se extraen los detalles técnicos precisos sobre la explotación de la vulnerabilidad de día cero (deserialización) en la plataforma GoAnywhere MFT y el uso de software RMM oculto bajo los procesos de transferencia de archivos.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- **IBM X-Force Exchange (OSINT Advisory):** Reporte sobre la campaña de alta velocidad de Storm-1175, confirmando los sectores objetivo-principales (salud, educación, finanzas) y el uso de vulnerabilidades tipo N-day y Zero-day.
- **CSO Online:** *"Microsoft says Medusa-linked Storm-1175 is speeding ransomware attacks"* (7 de abril de 2026). Análisis sobre el impacto de estas campañas en la gestión de la superficie de ataque y el tiempo de respuesta defensiva de las organizaciones

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 3168931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570