I. DATOS GENERALES:

Clase de alerta: Incidente

Tipo de Incidente: Ransomware

Nivel de riesgo: Alta

Sectores potencialmente afectados: Tecnología, Manufactura, Comercio, Salud, Servicios públicos, Gobierno, Financiero y Agricultura.

II. ALERTA

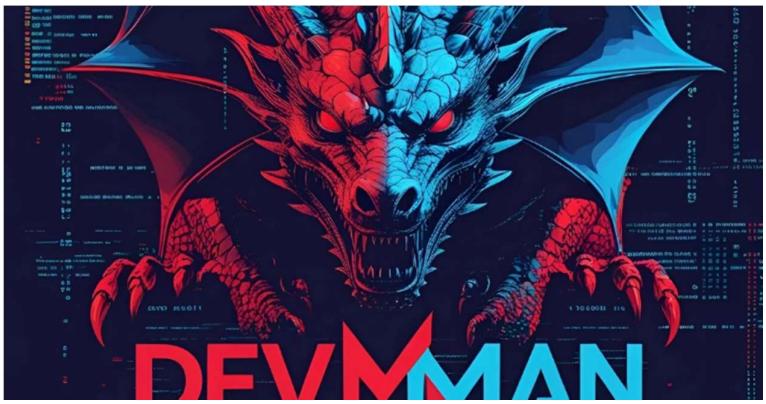

Figura 1. DevMan 2.0 - figura referencial

DevMan 2.0 es la versión evolucionada del ransomware DevMan, observado por primera vez en julio de 2025, con mejores capacidades que su predecesor, es una variante evolucionada de Ransomware-as-a-Service (RaaS) con capacidades de cifrado y robo de datos (*double-extortion*), utilizada por actores criminales para extorsionar entidades con demandas de rescate. Su infraestructura operativa facilita campañas globales y recurrentes, ampliando el impacto operativo y financiero de las organizaciones comprometidas.

III. INTRODUCCIÓN

Este ransomware inicialmente estaba asociado como variante de DragonForce y otros grupos RaaS, pero desde DevMan 2.0 opera con su propia plataforma de afiliación, con panel de construcción de cifradores y utilidades automáticas de exfiltración.

Comparte mecanismos técnicos con DragonForce y Conti, como el uso de Windows Restart Manager para el cifrado, pero presenta características distintas (por ejemplo: notas de rescate y operación offline).

DevMan 2.0 mantiene campañas globales con víctimas en Estados Unidos, América Latina, Europa, Asia y África, entre otros, afectando sectores críticos, y publicando los datos robados en sitios como *Tor*

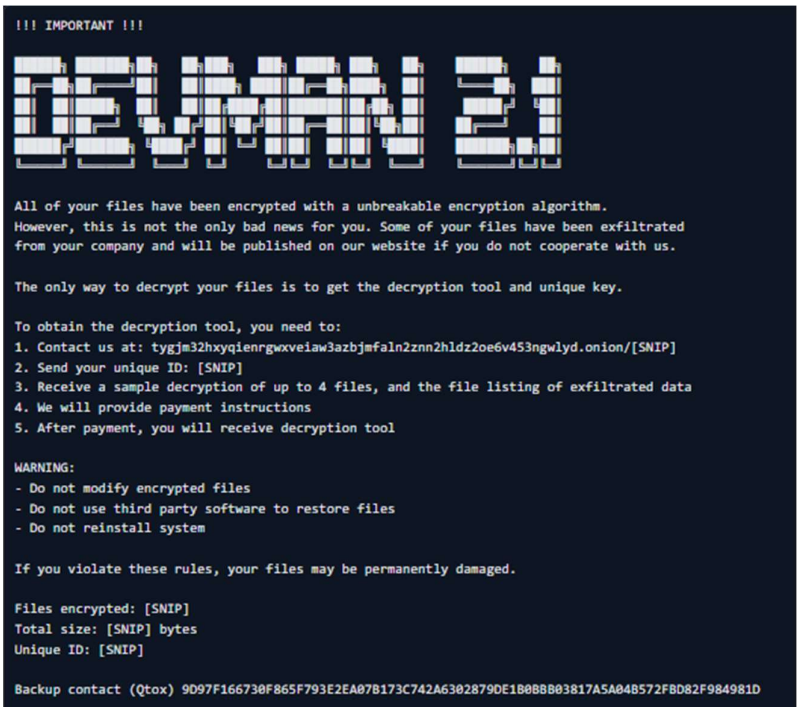

Figura 2. Nota de rescate Devaman, Fuente: https://www.ransomlook.io/notes/devman2

IV. VECTOR DE ATAQUE

Los reportes señalan varias rutas típicas de acceso:

- **Credenciales comprometidas** (RDP/VPN con contraseñas débiles).
- **Phishing y spear-phishing** con archivos maliciosos.
- **Servicios expuestos sin parches** o configuraciones deficientes.

Las técnicas utilizadas (MITRE ATT&CK), están relacionadas con la etapa de acceso inicial y movimiento lateral, entre otras:

Ciclo de Vida (Kill Chain)	Técnica MITRE	Nombre de la Técnica	Descripción	Táctica Asociada
Pre-ataque (Preparación)	**T1588.001**	**Stolen Credentials**	El adversario obtiene credenciales (nombres de usuario y contraseñas, hashes, tickets Kerberos, etc.) robadas de fuentes externas para su uso en la intrusión.	Comprar listas de credenciales filtradas en foros clandestinos o usar "info-stealers" (ladrones de información) para robarlas.
Acceso Inicial, Ejecución, Persistencia, Escalada de Privilegios, Movimiento Lateral	**T1078.002**	**Valid Accounts: Domain Accounts**	El adversario utiliza credenciales legítimas de cuentas de dominio para autenticarse y mantener el acceso a sistemas, evadiendo controles de seguridad.	Usar credenciales robadas o comprometidas de un usuario del dominio para acceder a servidores o estaciones de trabajo.

Ciclo de Vida (Kill Chain)	Técnica MITRE	Nombre de la Técnica	Descripción	Táctica Asociada
Movimiento Lateral	**T1021.002**	**SMB/Windows Admin Shares**	Utiliza los recursos compartidos administrativos predeterminados (como ADMIN$ o C$) para moverse lateralmente y ejecutar comandos en sistemas remotos.	Usar net use o psexec para conectarse a ADMIN$ en una máquina de destino usando credenciales válidas.
Comando y Control (C2)	**T1571**	**Non-Standard Port**	El adversario utiliza un puerto no estándar (diferente al predeterminado) para la comunicación de comando y control (C2) o para otros servicios, evadiendo detecciones basadas en puertos comunes.	Enviar tráfico C2 a través del puerto 8080 (HTTP alternativo) o 2222 (SSH alternativo) en lugar de los puertos 80 o 22.
Impacto	**T1486**	**Data Encrypted for Impact**	El adversario encripta datos en sistemas de la víctima para interrumpir las operaciones y exigir un rescate por la clave de desencriptación.	Ejecutar ransomware que cifra archivos con extensión .locked o .crypt y deja una nota de rescate (README.txt).

Tabla 1.- MITRE ATT&CK – DevMAn 2.0

V. IMPACTO

Impacto técnico

- Cifrado de archivos locales y de red con extensión reconocida como .DEVMAN o variantes personalizadas.
- Eliminación de copias de respaldo y bloqueo de servicios críticos.

Impacto operativo

- Interrupción de operaciones de negocio, parálisis de servicios y necesidad de recuperación forense.
- Potenciales brechas de datos críticos.

Impacto económico y reputacional

- Demandas de rescate millonarias.
- Costos de remediación, pérdida de productividad y daño reputacional.

Posible cifrado, exfiltración o doble extorsión

- DevMan 2.0 emplea doble extorsión: cifrado y publicación/venta de datos robados.

VI. INDICADORES DE COMPROMISO

- Dominios TOR, usados como infraestructura de extorsión:

Dominios / Tor / Identificadores maliciosos
qljmlmp4psnn3wqskkf3alqquatymo6hntficb4rhq5n76kuogcv7zyd.onion
devmanblggk7ddrtqj3tsocnayow3bwnozab2s4yhv6ueitjzid.onion
wugurgyscp5rxpihef5vl6b6m5ont3b6sezhl7boboso2enib2k3q6qd.onion
z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion/news
tygjm32hxyqienrgwxveiaw3azbjmfaln2znn2hldz2oe6v453ngwlyd.onion
z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion
3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd.onion

Tabla 2.- Detecciones relacionadas. Fuente: https://www.ransomware.live

- Archivos, extensiones, nombres de procesos:
  - Extensión de archivos cifrados típicamente .DEVMAN o variantes.
  - Ransom note con nombres aleatorios / cifrados debido a builder flaw.
- Comportamientos sospechosos:
  - Exploración SMB para movimiento lateral.
  - Eliminación de Shadow Copies.
  - Creación de sesiones temporales con Restart Manager.

- Hashes reportados

Hash SHA-256 identificados
df5ab9015833023a03f92a797e20196672c1d6525501a9f9a94a45b0904c7
b9821b480618327182c3a6ef9299c16dc4650ffd622824a4fab5962fdc3e2321
a96c1e909d678574f0de7d9e0bbc96ded63077a6355163f209d4d8ba886f21ff
6076dfe4669029f498ed2e7a5caf3a9960bce2059ba439c4caed476e122d6b68
06b3bef5cf867496c86977865403234dd00ec147c4e1fcc8e57a7f898275706f
b97a66c2059c84eccdfd84892e0e5a65cf78340d7b28ffd7585523e9c55d2521
3e81f7c67d2b265a82705565fdd6934580d26b35a898ed35d632699cabcce779
7c7f990a03eb2fc78df4af059ca313cd65cd57a28e579b4db6c92662c87e13a0
b230fd2030c919861cad41f070d226c897fbac6fb4ccd8276f7d786f6f164d04
1814c491987af5899343d8440fb98b045d20e6b1e6c596fe5c2e1199995a4bc2
d1cf75e35d2610718a79bbd55bb759c37777b016ffd846eaff2e744fdb7022cf
153b6a1765f48ec9be9fbe5767485a91fb151d236763a575cee4aca0e6bb5c4f
a2a123cdff645fbc6ebf17d8d84b3cb0e5e4caf85023d6aa0b1d4361e7ebc99e
451a42db9c514514ab71218033967554507b59a60ee1fc3d88cbeb39eec99f20
0dfe23ab86cb5c1bfaf019521f3163aa5315a9ca3bb67d7d34eb51472c412b22
df5ab9015833023a03f92a797e20196672c1d6525501a9f9a94a45b0904c7403

Tabla 3.- Hash – ***Fuente:*** *https://www.virustotal.com/gui/search/devman*

- Otros indicadores de compromiso

Tipo	IoC
Ip	83.217.209.210
Ip	38.132.122.213
Ip	38.132.122.214
Mensajería Tox	9D97F166730F865F793E2EA07B173C742A6302879DE1B0BBB03817A5A04B572FBD82F984981D
Mensajería Tox	C173B0BBD44655F3E0C2CD2FA721D24A72DE7BD5F51E2199594235BC097C25352E6C943C8F90
Cuenta X	@Inifintyink

Tabla 4.- Otros IoCs – ***Fuente:*** *https://www.ransomware.live/group/devman*

VII. RECOMENDACIONES:

- Aplicar todos los parches disponibles en sistemas Windows/Linux, servidores, y aplicaciones.
- Segmentar la red y restricciones de RDP/VPN
- Usar autenticación multifactor (MFA).
- Aislar los entornos críticos (servidores, backups, bases de datos) del resto de la red para evitar la propagación.
- Agregar hashes en las herramientas de detección.
- Monitorizar anomalías de comportamiento, en especial monitorización del tráfico SMB y detección de patrones de movimiento lateral.
- Crear alertas de eliminación de “Shadow Copies” o “Volume Shadow Copy Service (VSS)”
- Realizar copias de respaldo offline y verificar regularmente su integridad y restauración.
- Correlación de eventos de autenticación anómala y uso de cuentas privilegiadas
- Usar listas de reputación y analizar tráfico sospechoso.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

AnyRun. (2025, diciembre 19). DEVMAN: Ransomware Overview. Recuperado 13 de enero de 2026, de Medium website: https://medium.com/%40anyrun/devman-ransomware-overview-32600d4da684

Cardiet, L. (2025, diciembre 11). De Conti a Black Basta y a DevMan: el interminable cambio de marca del ransomware [Web log post]. Recuperado 14 de enero de 2026,

de Vectra.ai website: https://es.vectra.ai/blog/from-conti-to-black-basta-to-devman-the-endless-ransomware-rebrand

Halcyon. (s. f.). Threat Actor DevMan. Recuperado 13 de enero de 2026, de Halcyon.ai website: https://www.halcyon.ai/threat-group/devman

Israel National Cyber Directorate (2025, julio). DevMan Ransomware Threat Actor Report. Recuperado 13 de enero de 2026, de Gov.il website: https://www.gov.il/BlobFolder/reports/alert_1907/he/ALERT-CERT-IL-W-1907.pdf

Mousqueton, J. (s. f.). Group: devman. Recuperado 13 de enero de 2026, de Ransomware.live website: https://www.ransomware.live/group/devman

Ransomlook. (s. f.). Devman2 details. Recuperado 13 de enero de 2026, de Ransomlook.io website: https://www.ransomlook.io/group/devman2

RansomLook. (s. f.). Open ransomware intelligence. Recuperado 13 de enero de 2026, de Ransomlook.io website: https://www.ransomlook.io/search

Sin titulo. (s. f.). Recuperado 14 de enero de 2026, de X (formerly Twitter) website: https://x.com/RakeshKrish12/status/1924716514202288232

Watchguard. (2025, julio 7). Devman 2.0 ransomware. Recuperado 13 de enero de 2026, de Watchguard.com website: https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/devman-20