Grupo de ransomware: DevMan

Resumen ejecutivo

DevMan es un grupo cibercriminal dedicado a realizar **operaciones de ransomware** que apareció en abril de 2025 y, desde entonces, se ha consolidado como uno de los grupos más emergentes del panorama cibercriminal. Su estrategia operativa se basa en el modelo Ransomware-as-a-Service (RaaS) y el uso de **tácticas de doble extorsión** a través de su portal "DevMan's Place" alojada en la red Tor. Aunque comenzó como afiliado de servicios RaaS consolidados, como Qilin o DragonForce, DevMan ha evolucionado hacia una **estructura autónoma**, desarrollando su propia variante de ransomware y ofreciendo **servicios personalizados a sus afiliados**, lo que ha aumentado potencialmente su alcance y capacidad de impacto.

Este grupo ha afectado a organizaciones de distintos tamaños y **sectores estratégicos, como tecnología, sanidad, administración pública, manufactura**, entre otros. Esta falta de discriminación sectorial demuestra que cualquier organización, ya sea pública o privada, está en riesgo frente a este grupo. Además, esta versatilidad convierte a DevMan en una amenaza transversal, con capacidad para **interrumpir servicios esenciales, exfiltrar datos sensibles, daños reputacionales y generar pérdidas económicas, con consecuencias legales y regulatorias**.

En cuanto a sus capacidades técnicas, DevMan lleva a cabo la explotación de servicios expuestos en Internet o el uso de credenciales válidas, movimientos laterales mediante herramientas legítimas (LOLBins), técnicas de evasión frente a soluciones de seguridad y un cifrado híbrido eficaz.

Ante esta amenaza, se recomienda **adoptar una postura defensiva sólida y proactiva**. Las organizaciones deben implementar medidas como la **autenticación multifactor**, la **segmentación de red**, el uso de **copias de seguridad aisladas** y la preparación de **planes específicos de respuesta** ante incidentes de ransomware.

Grupo de ransomware: DevMan

DevMan nació como afiliado en esquemas de Ransomware-as-a-Service (RaaS) y pronto evolucionó con el objetivo de **operar de forma independiente**, mostrando una **motivación económica** en sus acciones. Para incentivar la colaboración, ofrece porcentajes de beneficio muy altos a sus afiliados para maximizar la propagación de sus ataques, reteniendo una porción de los pagos de rescate. En junio de 2025, DevMan fue expuesto por el grupo GangExposed, lo que llevó a la pérdida de algunos afiliados y obligó al grupo a reestructurar su infraestructura, creando un nuevo sitio de filtraciones y reimplementado su **malware en lenguaje Rust**, para mejorar sus capacidades y dificultar la ingeniería inversa.

Actualmente DevMan opera con una infraestructura bien establecida y con un **modelo de doble extorsión**, tras cifrar sistemas críticos de la víctima se exfiltran los datos sensibles para amenazar con publicarlos en su portal de la red Tor. Además, mantiene presencia en la plataforma X (antigua Twitter) donde expone sus ataques y anuncia novedades en inglés y ocasionalmente en ruso.

Países y sectores afectados

DevMan **ha afectado a organizaciones de todo el mundo**, con especial incidencia en regiones de **Asia, África, Norteamérica y Europa**. El país con mayor número de víctimas identificadas es Estados Unidos, seguido de Francia, Taiwán, Tailandia y China. Durante 2025 se han reportado víctimas atribuidas a este grupo a nivel estatal, como, por ejemplo, el ayuntamiento de Nijar o el centro de Ciencia y Tecnología Forestal de Cataluña (CTFC).

En cuanto a los sectores más afectados, se incluyen **tecnología, salud, sector público y construcción**, **seguidos por agricultura y manufactura**. Esto confirma que DevMan no se especializa en un sector concreto, sino que aprovecha oportunidades en múltiples sectores.

Análisis técnico

DevMan emplea diversos vectores de acceso inicial, como por ejemplo el **compromiso de servicios expuestos a Internet, ataques de fuerza bruta o credenciales débiles en accesos remotos**. Otra vía de acceso inicial son los correos phishing con adjuntos dañinos.

Tras lograr el acceso inicial, DevMan suele **escalar privilegios y propagarse por la red interna** con rapidez, para ello intenta explotar vulnerabilidades para elevar privilegios o utilizar credenciales en el sistema comprometido. Una vez con credenciales de administrador de dominio o equivalentes, el atacante procede al **movimiento lateral** hacia otros equipos de la red. También se ha observado que realiza **técnicas de reconocimiento** ejecutando comandos de descubrimiento de red y servicios. Además, el grupo emplea **técnicas de evasión** para no ser descubierto, despliega **medidas antiforenses y desactiva los mecanismos de recuperación**.

Una vez descubierto y exfiltrados los datos sensibles, el ransomware DevMan implementa un **cifrado híbrido robusto** para bloquear los archivos de las víctimas. Combinando criptografía de clave pública y simétrica, y generando para cada archivo un identificador único que lo adjunta al nombre cifrado.

Características técnicas principales:

- **Plataformas afectadas:** DevMan ha sido observado principalmente en sistemas Windows, pero también ha demostrado capacidad contra infraestructuras VMware ESXi.

- **Uso de binarios legítimos (LOLBins):** DevMan emplea herramientas nativas de Windows como vssadmin, PowerShell y la API RestartManager de Windows. Asimismo, utiliza PsExec para movimiento lateral mediante comparticiones SMB.

- **Capacidades de cifrado:** DevMan dispone de tres modalidades de cifrado (completo, solo cabecera o personalizado) que permiten ajustar la velocidad del cifrado según el objetivo.

Técnicas MITRE ATT&CK

Táctica	Técnica más usada
Initial Access	**T1566** — Phishing **T1190** — Exploit Public-Facing Application **T1078** — Valid Accounts **T1210** — Exploitation of Remote Services
Execution	**T1059.001** — Command and Scripting Interpreter: PowerShell **T1203** — Exploitation for Client Execution
Persistence	**T1078** — Valid Accounts
Privilege Escalation	**T1068** — Exploitation for Privilege Escalation
Defense Evasion	**T1036** — Masquerading **T1562** — Impair Defenses
Credential Access	**T1003** — OS Credential Dumping
Discovery	**T1018** — Remote System Discovery **T1046** — Network Service Discovery **T1082** — System Information Discovery
Lateral Movement	**T1021.002** — Remote Services: SMB/Windows Admin Shares
Collection	**T1005** — Data from Local System
Command and Control	**T1071** — Application Layer Protocol **T1105** — Ingress Tool Transfer
Exfiltration	**T1041** — Exfiltration Over C2 Channel
Impact	**T1486** — Data Encrypted for Impact **T1490** — Inhibit System Recovery **T1489** — Service Stop

Medidas de mitigación

Proactivas

- ❑ Implementar autenticación multifactor (MFA) para evitar accesos no autorizados. (T1078 – Valid Accounts)
- ❑ Limitar los privilegios de las cuentas de usuario utilizando el principio de mínimos privilegios. (T1489 – Service Stop)
- ❑ Actualizar el software periódicamente empleando una correcta gestión de parches. (T1190 – Exploit Public-Facing Application)
- ❑ Mantener copias de seguridad seguras y probar restauraciones periódicas. (T1486 – Data Encrypted for Impact)
- ❑ Realizar una segmentación de red y aplicar políticas de mínimo privilegios (T1021.002 – Remote Services: SMB/Windows Admin Shares)

Reactivas

- ❑ Utilizar un antivirus para poner en cuarentena automáticamente archivos sospechosos, desactivar PowerShell cuando no sea necesario o usar el modo "Constrained Language“ para restringir el acceso. (T1059.001 – Command and Scripting Interpreter: PowerShell)
- ❑ Monitorizar tráfico saliente y bloquear conexiones SMTP/FTP/HTTP no autorizadas usados para exfiltración. (T1041 - Exfiltration Over C2 Channel)
- ❑ Implementar sistemas de detección y prevención de intrusiones que permitan identificar tráfico anómalo o patrones de red asociados a malware. (T1071 – Application Layer Protocol / Web Protocols)

Conclusiones y recomendaciones

DevMan es un grupo que pasó de ser un afiliado en operaciones RaaS a construir su propia infraestructura de ransomware. Debido a este cambio, **ha logrado posicionarse entre los grupos de ransomware más activos de 2025 y actualmente es una de las amenazas de mayor impacto para organizaciones de todo tipo**. Esto es debido a su capacidad para llevar a cabo la inhabilitación de equipos, la exposición pública de información confidencial y el daño reputacional contra sus victimas.

Por ello, es recomendable que las organizaciones adopten una **postura defensiva proactiva**, implementando la protección de sus accesos mediante **autenticación multifactor**, **instalando soluciones EDR** para monitorización de anomalías, **manteniendo actualizados los dispositivos**, realizando **segmentación de la red** para restringir movimientos laterales y realizando una protección correcta de los **backups**, asegurando que estén aislados e inmutables. Finalmente, es necesario contar con **planes de contingencia y planes de gestión de crisis** que permitan operar incluso ante la indisponibilidad de los sistemas críticos.

