## I. DATOS GENERALES:

**Clase de alerta:** Ransomware
**Tipo de Incidente:** Posible exfiltración o publicación de información
**Nivel de riesgo:** Alta

## II. ALERTA


***Figura 1.-*** Ransomware VEXY - figura referencial

Ransomware VEXY es una amenaza emergente identificada en septiembre de 2026, con actividad registrada principalmente contra organizaciones de América Latina. Se han reportado incidentes asociados al grupo en Brasil y Ecuador, así como la publicación de información de posibles víctimas en sitios de filtración. Debido a su reciente aparición, aún existe información limitada sobre sus herramientas y técnicas de ataque, por lo que se recomienda mantener vigilancia ante posibles compromisos de sistemas o exposición de información.

## III. INTRODUCCIÓN

Ransomware VEXY es un grupo de amenazas emergente, identificado recientemente en septiembre de 2026. El grupo mantiene actividad mediante un sitio de filtraciones en la red Tor, donde publica organizaciones que presuntamente han sido comprometidas y utiliza la exposición de información como mecanismo de presión.

La información disponible indica actividad contra organizaciones de diferentes sectores y países, incluyendo Ecuador. Sin embargo, debido a su reciente

aparición, aún existe información limitada y parcialmente no verificada sobre su infraestructura, herramientas, métodos de acceso inicial y capacidades técnicas.

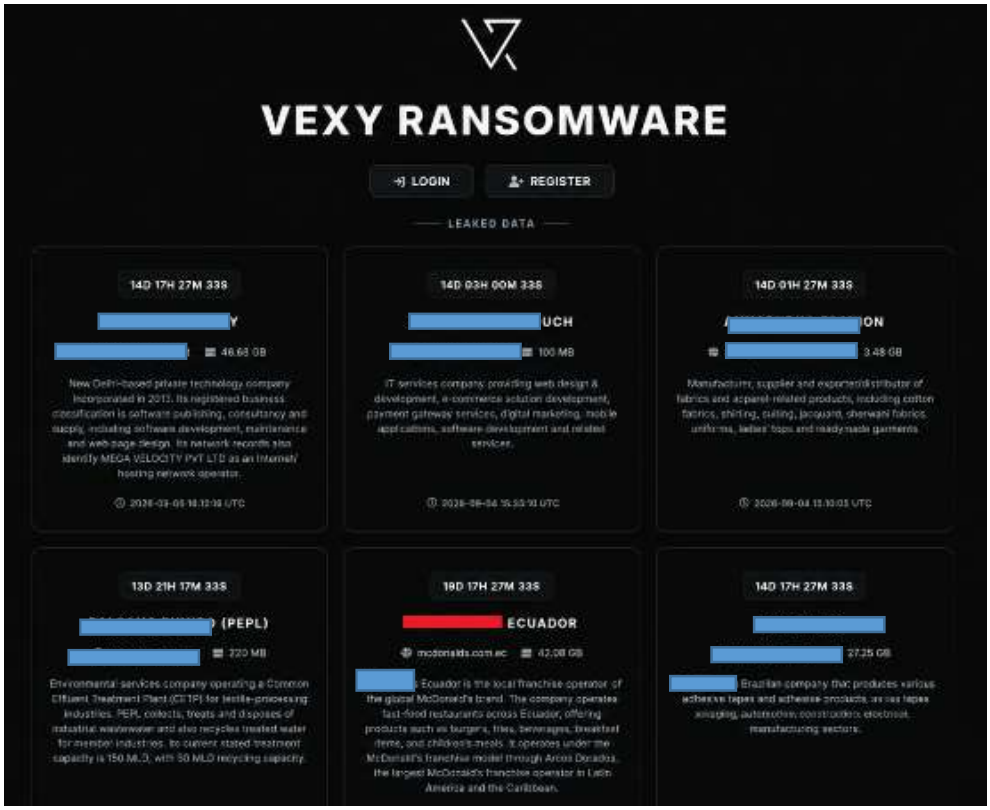


***Figura 2.***- Sitio DLS - Ransomware VEXY

## IV. VECTOR DE ATAQUE

Se detalla TTP:

| Táctica | Técnica MITRE ATT&CK | Descripción |
|---|---|---|
| Persistencia | T1078 | Uso de cuentas válidas para mantener el acceso. |
| | T1547 | Ejecución automática al iniciar el sistema o sesión. |
| Ejecución | T1059 | Ejecución de comandos y scripts. |
| Evasión de defensas | T1562 | Debilitamiento o desactivación de mecanismos de seguridad. |

| Táctica | Técnica MITRE ATT&CK | Descripción |
|---|---|---|
| Movimiento lateral | T1021 | Uso de servicios remotos para acceder a otros sistemas. |
| | T1080 | Propagación mediante contenido compartido. |
| Impacto | T1486 | Cifrado de datos para afectar la disponibilidad de la información. |
| | T1490 | Interferencia con mecanismos de recuperación del sistema. |

***Tabla 1.-*** TTP - Ransomware VEXY

## V. IMPACTO

| Sector Empresarial |
|---|
| Energía y servicios públicos |
| Administración pública y defensa |
| Hostelería |
| Fabricación |
| Comercio minorista y electrónico |
| Transporte |

***Tabla 2.-*** Organizaciones objetivos - Ransomware VEXY

| Paises Afectados |
|---|
| Argentina |
| Brasil |
| Ecuador |
| México |
| India |

***Tabla 3.-*** Países afectados - Ransomware VEXY

## VI. INDICADORES DE COMPROMISO

| Tipo | Indicador |
|---|---|
| Tox ID | C32355C829A3CC4B320D4E78634FB4113B4B2918B383BB7AEAA48BDAAA4A0146E99B45A2A4C9 |
| DLS | vexytsr3chimdz6siwaqi2lvxxwfkxvffkpwyanr2llequ2hkm56jvqd[.]onion |

***Tabla 4.-*** Indicadores de Compromiso - Ransomware VEXY

| Nro. Alerta: | AL-2026-047 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR<br>**ALERTAS DE SEGURIDAD** | ecucert<br>V 1.1 |
|---|---|---|---|
| TLP: | TLP:CLEAR | | |
| Fecha: | 18-sep-2026 | Ransomware VEXY | Pág.: **4** of **6** |

## VII. RECOMENDACIONES:

- Realizar monitoreo continuo de fuentes de inteligencia y sitios de filtración para identificar posibles credenciales comprometidas, información expuesta o publicaciones relacionadas con la organización.
- Realizar una evaluación técnica del incidente para determinar el posible mecanismo de acceso, identificar los sistemas afectados, verificar si existió exfiltración de información y detectar posibles mecanismos de persistencia.
- Validar que las copias de seguridad de la información crítica se encuentren actualizadas, protegidas y, de ser posible, almacenadas de forma aislada o mediante mecanismos de inmutabilidad que impidan su modificación o eliminación por actores maliciosos.
- Integrar los Indicadores de Compromiso (IoC) disponibles en las herramientas de monitoreo y seguridad de la organización, como SIEM, EDR o XDR, para facilitar la detección de actividad asociada a la amenaza.
- Reforzar la seguridad de las cuentas mediante autenticación multifactor (MFA), especialmente en accesos administrativos, servicios remotos y sistemas críticos. Asimismo, evitar el uso de contraseñas débiles o reutilizadas.
- Realizar actividades de concientización y simulaciones de phishing dirigidas al personal para reducir el riesgo de compromiso de credenciales mediante técnicas de ingeniería social.
- En caso de identificar indicios de compromiso, aislar los sistemas afectados, preservar los registros y evidencias disponibles y activar los procedimientos internos de respuesta a incidentes.

## 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:

**SECURITY ARSENAL. (2026).** *VEXY Ransomware Gang: 5 New Victims in 4 Days – India and LATAM Campaign, Sector Analysis and Detection Rules.*

https://securityarsenal.com/blog/vexy-ransomware-gang-5-new-victims-in-4-days-india-and-latam-campaign-sector-analysis-and-detection-rules

**SOCRADAR. (2026).** *VEXY Ransomware.* https://socradar.io/free-tools/ransomware-intelligence/groups/vexy-ransomware

**DEXPOSE. (2026).** *VEXY Ransomware Strikes McDonald's Ecuador.* https://www.dexpose.io/vexy-ransomware-strikes-mcdonalds-ecuador/

**DARKFIELD. (2026).** *VEXY Ransomware.* https://darkfield.orizon.one/groups/vexy

**THREADLINQS. (2026).** *VEXY Ransomware – Threat Intelligence.* https://intel.threadlinqs.com/threat/TL-2026-2363