## I. DATOS GENERALES:

**Clase de alerta:** Amenaza Cibernética
**Tipo de Incidente:** Ransomware
**Nivel de riesgo:** Alto

## II. ALERTA


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

Investigadores han identificado un nuevo grupo de ransomware denominado Wallstreet. Este actor de amenaza opera bajo un esquema de doble extorsión, combinando la exfiltración de información hacia su Data Leak Site (DLS) con el cifrado de sistemas y datos comprometidos, con el objetivo de aumentar la presión sobre las víctimas para que efectúen el pago del rescate.

## III. INTRODUCCIÓN

La reciente actividad de Ransomware Wallstreet fue observada los meses de abril y junio de 2026, analistas de ciberseguridad observaron que el grupo tiene como objetivo organizaciones de los sectores manufactureros, salud y entidades gubernamentales, debido a que estas empresas administran grandes volúmenes de información sensible.

La información exfiltrada por el grupo de Ransomware Wallstreet es publicada en su Data Leak Site (DLS) alojada en la red Tor, como parte de su estrategia de doble extorsión. Asimismo, el grupo utiliza la plataforma de mensajería cifrada TOX para

establecer comunicación directa con las víctimas e iniciar el proceso de negociación del rescate.

Uno de los últimos ataques registrados por parte del Ransomware Wallstreet es una empresa del sector de Asistencia Médica en Ecuador.

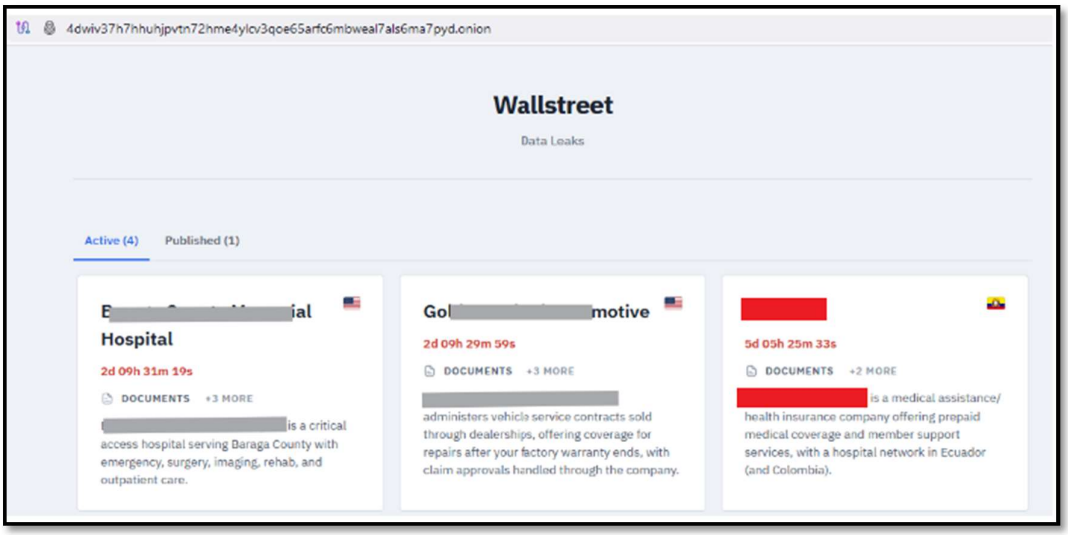


***Figura 2.-*** Sitio DLS - Ransomware Wallstreet

## IV. VECTOR DE ATAQUE

El acceso inicial inicia mediante el uso de credenciales comprometidas obtenidas de filtraciones previas, campañas de phishing dirigidas o la explotación de vulnerabilidades en servicios expuestos a Internet. Tras ganar el acceso, los actores de amenaza llevan a cabo actividades de reconocimiento y enumeración para identificar activos críticos, relaciones de confianza, servicios accesibles y cuentas privilegiadas dentro del entorno comprometido. Posteriormente, emplean técnicas de escalamiento de privilegios y acceso a credenciales para ampliar su control sobre la infraestructura.

Posteriormente, los atacantes realizan movimientos laterales mediante protocolos de administración remota, como Remote Desktop Protocol (RDP), así como otras herramientas legítimas de gestión del sistema. Durante esta fase, localizan y recopilan información sensible, la cual es agregada y comprimida para su exfiltración hacia

infraestructura controlada por el atacante mediante canales cifrados. Tras completar la extracción de datos, ejecutan la fase de impacto mediante el despliegue del ransomware o el inicio de la extorsión basada en la divulgación de información robada, estableciendo plazos de negociación de aproximadamente cuatro a cinco días antes de publicar los datos comprometidos en su Data Leak Site (DLS).

## V. IMPACTO

| Sector Empresarial |
|---|
| Manufactura |
| Salud |
| Gubernamentales |

***Tabla 1.-*** Organizaciones objetivos - Ransomware Wallstreet.

| Países afectados |
|---|
| India |
| Estados Unidos |
| Ecuador |

***Tabla 2.-*** Países afectados - Ransomware Wallstreet.

## VI. INDICADORES DE COMPROMISO

| Dirección TOR (.onion) |
|---|
| http[://]4dwiv37h7hhuhjpvtn72hme4ylcv3qoe65arfc6mbweal7als6ma7pyd.onion/ |

***Tabla 3.-*** Direcciones TOR - Ransomware Wallstreet.

## VII. RECOMENDACIONES

- Revisar los registros de autenticación y accesos privilegiados para identificar actividades inusuales o accesos no autorizados.
- Cambiar credenciales administrativas y habilitar MFA en todos los accesos críticos y remotos.
- Validar la integridad y disponibilidad de las copias de seguridad, asegurando que se encuentren aisladas y libres de cifrado.
- Monitorear la dark web y fuentes de inteligencia para detectar posibles publicaciones de información relacionada con la organización.
- Mantener actualizados los sistemas operativos y aplicaciones, corrigiendo vulnerabilidades conocidas que puedan ser utilizadas para obtener acceso inicial.

- Segmentar la red para limitar el movimiento lateral en caso de compromiso.
- Implementar monitoreo continuo mediante EDR/XDR y SIEM, priorizando la detección de comportamientos asociados a ransomware.
- Activar el plan de respuesta a incidentes si se identifican evidencias de compromiso, preservando registros y evidencias para el análisis forense.
- Verificar la existencia de indicadores de compromiso (IoC) en servidores, estaciones de trabajo y servicios expuestos.

## 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:

**EL UNIVERSO. (2026).** *La amenaza cibernética que ronda a Ecuador: el modus operandi del grupo Wallstreet que aterroriza a las empresas.* https://www.eluniverso.com/noticias/ecuador/la-amenaza-cibernetica-que-ronda-a-ecuador-el-modus-operandi-del-grupo-wallstreet-que-aterroriza-a-las-empresas-nota/

**SOCRADAR. (2026).** *Wallstreet – Ransomware Intelligence.* https://socradar.io/free-tools/ransomware-intelligence/groups/wallstreet

**WATCHGUARD TECHNOLOGIES. (2026).** *Wallstreet – Ransomware Tracker.* https://www.watchguard.com/es/wgrd-security-hub/ransomware-tracker/wallstreet

**RANSOMWARE.LIVE. (2026).** *Wallstreet.* https://www.ransomware.live/group/Wallstreet