I. DATOS GENERALES:

Clase de alerta: Amenaza activa
Tipo de Incidente: Ransomware
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Ransomware VECT- figura referencial

Se ha identificado la aparición de una nueva familia de ransomware denominada VECT, que opera bajo el modelo Ransomware-as-a-Service (RaaS). Esta amenaza permite que actores maliciosos afiliados ejecuten ataques de cifrado y extorsión contra organizaciones públicas y privadas.

Ransomware VECT emplea técnicas modernas de cifrado y mecanismos de evasión, permitiéndole comprometer sistemas Windows, Linux y entornos virtualizados (VMware ESXi), lo que incrementa su impacto en infraestructuras críticas y centros de datos.

III. INTRODUCCIÓN

Ransomware VECT al igual que los demás ransomware opera bajo el modelo de doble extorsión, es decir exfiltración de datos y su posterior encriptación de datos, el grupo opera bajo la red TOR donde incluye:

1. Un portal de reclutamiento de afiliados por un valor de ingreso de 250 USD pago en Monero (XMR), que es una criptomoneda enfocada en la privacidad y anonimato.

2. Un website público sobre filtraciones de datos llamado "VECT RANSOMWARE // DATA ARCHIVE" donde se publica la información de las victimas que NO cumplen las exigencias de rescate.

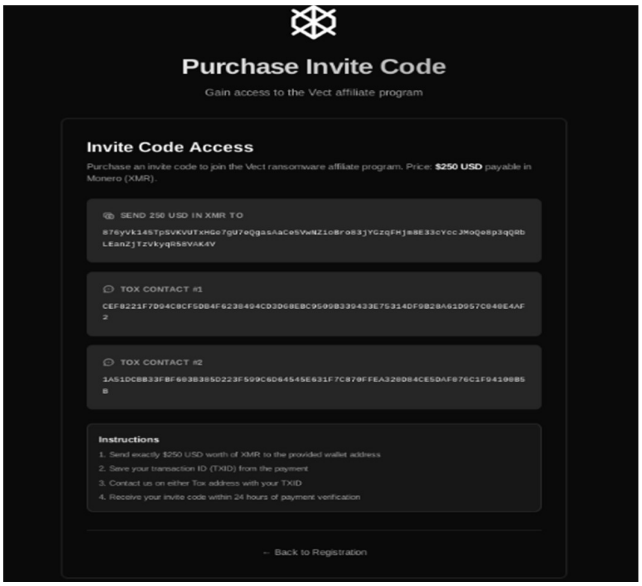

Figura 2.- Panel de adquisición de código de invitación del ransomware VECT (modelo RaaS).
Fuente: Red Piranha (2026), captura incluida en *Threat Intelligence Report – January 6 to January 12, 2026*.
https://redpiranha.net/news/threat-intelligence-report-january-6-january-12-2026

3. Los afiliados obtendrán comisiones proporcionadas, soporte de negociaciones dedicadas, capacidades multilenguaje y herramientas de gestión integral.

4. Una interfaz de negociación con victimas denominadas "Vect Secure Chat", aquí las victimas reciben identificadores de chat únicos en formato UUID (Universally Unique Identifier, es un identificador estándar de 128 bits usado para identificar información de manera única en sistemas) en las notas de rescate, utilizadas para la autenticación en el portal de negociaciones basados en TOR.

IV. VECTOR DE ATAQUE

El grupo de Ransomware VECT afirma que su malware fue construido en C++ de manera independiente sin la reutilización de código fuente filtrados de otros ransomware. Empleando el uso de ChaCha20-Poly1305 AEAD, este proceso se detalla que usa el

algoritmo chacha20 para el cifrado del contenido, Poly1305 genera un tag (etiqueta) de 128 bits, este tag es usado al momento de descifrar, en el caso de no coincidir con el archivo durante este proceso este es rechazado, AEAD se refiere a que lo realiza en un solo proceso. Las operaciones de Ransomware VECT destacan sofisticadas técnicas multiplataforma para Windows, Linux y VMWare ESXi, entras las funciones avanzadas está el arranque en modo seguro de Windows para evitar ser detectado por aplicaciones de seguridad, reconocimiento de red por medio de protocolos DFS y SMB, movimiento lateral automatizado para la propagación basada en SMB y la explotación de administración remota de Windows (WinRM).

Se describe el TTP del Ransomware VECT:

Táctica	Técnica	ID DE ATT&CK
Acceso Inicial	Cuentas válidas: credenciales robadas/débiles	T1078
Acceso Inicial	Servicios remotos externos: RDP/VPN	T1133
Acceso Inicial	Categoría: Phishing	T1566
Ejecución	Intérprete de comando y scripting	T1059
Persistencia	Tarea/trabajo programado (inferido)	T1053
Escalada de privilegios	Manipulación de tokens de acceso (inferido)	T1134
Evasión de Defensa	Arranque de modo seguro	T1562.009
Evasión de Defensa	Deterioro de las defensas: Desactivar herramientas	T1562.001
Acceso de credencia-les	Dumping de credenciales del sistema operativo (inferido)	T1003
Descubrimiento	Descubrimiento del servicio de red: DFS/SMB	T1046
Descubrimiento	Descubrimiento de información del	T1082
Descubrimiento	Descubrimiento de archivos y directorios	Categoría: T1083
Movimiento Lateral	Servicios Remotos: SMB/Admin Shares	T1021.002
Movimiento Lateral	Servicios remotos: WinRM	T1021.006
Colección	Datos del Sistema Local	Categoría: T1005
Colección	Datos de la unidad compartida de red	T1039
Comando y Control	Protocolo de la capa de aplicación: Web	T1071.001
Comando y Control	Canal encriptado: TOR	T1573
Exfiltración	Exfiltración Sobre El Canal C2	T1041
Impacto	Datos encriptados para el impacto	T1486
Impacto	Inhibir la recuperación del sistema	T1490
Impacto	Servicio Stop	T1489

Tabla 1.- Técnica y táctica de ataque – Ransomware VECT

V. IMPACTO

Los productos afectados son los siguientes:

Categoría	Producto / Tecnología	Descripción
Sistema Operativo	Windows (usuarios y servidores)	Sistemas operativos Windows susceptibles a cifrado, movimiento lateral y escalada de privilegios
Sistema Operativo	Linux	Servidores Linux vulnerables a acceso no autorizado y cifrado de información
Virtualización	VMware ESXi	Plataformas de virtualización expuestas a ataques de ransomware dirigidos a infraestructura crítica
Acceso Remoto	RDP, VPN, WinRM	Servicios utilizados como vector de acceso inicial y movimiento lateral
Servicios de Red	SMB y recursos compartidos	Servicios empleados para descubrimiento, propagación y cifrado de archivos
Infraestructura	Infraestructura expuesta a Internet	Sistemas con credenciales débiles o controles de acceso insuficientes

Tabla 2.- Productos afectados – Ransomware VECT

VI. INDICADORES DE COMPROMISO

Tipo	Indicador	Detalle
IP	158.94.210.11	Infraestructura asociada a ransomware Vect
Puerto	8000	Puerto utilizado para comunicaciones maliciosas

Tabla 3.- Infraestructura de comando y control (C2) – Ransomware VECT

Tipo	Indicador	Descripción
Dominio Onion	bu7zr6fotni3qxxoxlcm-pikwtp5mjzy7jkxt7akflnm2kwkbdtgtjuid[.]cebolla	Infraestructura primaria del grupo Vect
Servicio	/invitar	Panel de reclutamiento de afiliados
Servicio	/registrarse	Registro de nuevos afiliados
Servicio	/iniciar sesión	Acceso a panel de afiliados
Servicio	/chat	Portal de negociación con víctimas
Servicio	/	Sitio público de filtración de datos
Título	“VECT RANSOMWARE // ARCHIVO DE DATOS”	Página de publicación de información exfiltrada

Tabla 4.- Infraestructura de comando y control (C2) – Ransomware VECT

Tipo	Indicador	Propósito
Criptomoneda	Monero (XMR)	Moneda utilizada por el grupo
Dirección de monedero	876yVkL4S7p5rWKbTxHs6e7gbTeqqas4AcC6WwMZ1d8r0B31jYBzqJFHJ88E33cYcc3jfKjQcBp3oqN8bLEan2JTzYkyq8RdVAkTv	Compra de código de afiliación (~USD 250)

Tabla 5.- Criptomonedas (Monederos) – Ransomware VECT

Tipo	Indicador	Descripción
Protocolo	TOX	Medio de comunicación del actor
Contacto TOX #1	EEF8221F7D94C8CF0EBHF623B494C03D608EEC9649 D83A9433E75314DFB828A01DD57C8A9E4AF2	Comunicación con el grupo
Contacto TOX #2	1A51DCB233FB86038D802E23F599C6D64543E031FC 87dFFEA32D8064CE9D04f70C1F041988B8	Comunicación con el grupo

***Tabla* 6.-** Comunicaciones (Protocolo TOX) – Ransomware VECT

VII. RECOMENDACIONES:

- Mantener copias de seguridad actualizadas y almacenadas fuera de línea.
- Aplicar parches de seguridad y actualizaciones del sistema operativo y aplicaciones.
- Restringir y monitorear accesos remotos (RDP, VPN, SMB).
- Implementar controles de seguridad perimetral y detección de comportamiento anómalo.
- Capacitar al personal en buenas prácticas de ciberseguridad.

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:

HALCYON AI (2026). *Emerging ransomware group VECT*.
https://www.halcyon.ai/ransomware-alerts/emerging-ransomware-group-vect

RANSOMWARE.LIVE (2026). *Search results: VECT ransomware group*.
https://www.ransomware.live/search?q=vect&scope=group_name

RED PIRANHA (2026). *Threat intelligence report – January 6 to January 12, 2026*.
https://redpiranha.net/news/threat-intelligence-report-january-6-january-12-2026

SC WORLD (2026). *Nascent VECT RaaS operation examined*.
https://www.scworld.com/brief/nascent-vect-raas-operation-examined

INFOSECURITY MAGAZINE (2026). *Researchers warn new VECT RaaS variant*.
https://www.infosecurity-magazine.com/news/researchers-warn-new-vect-raas/