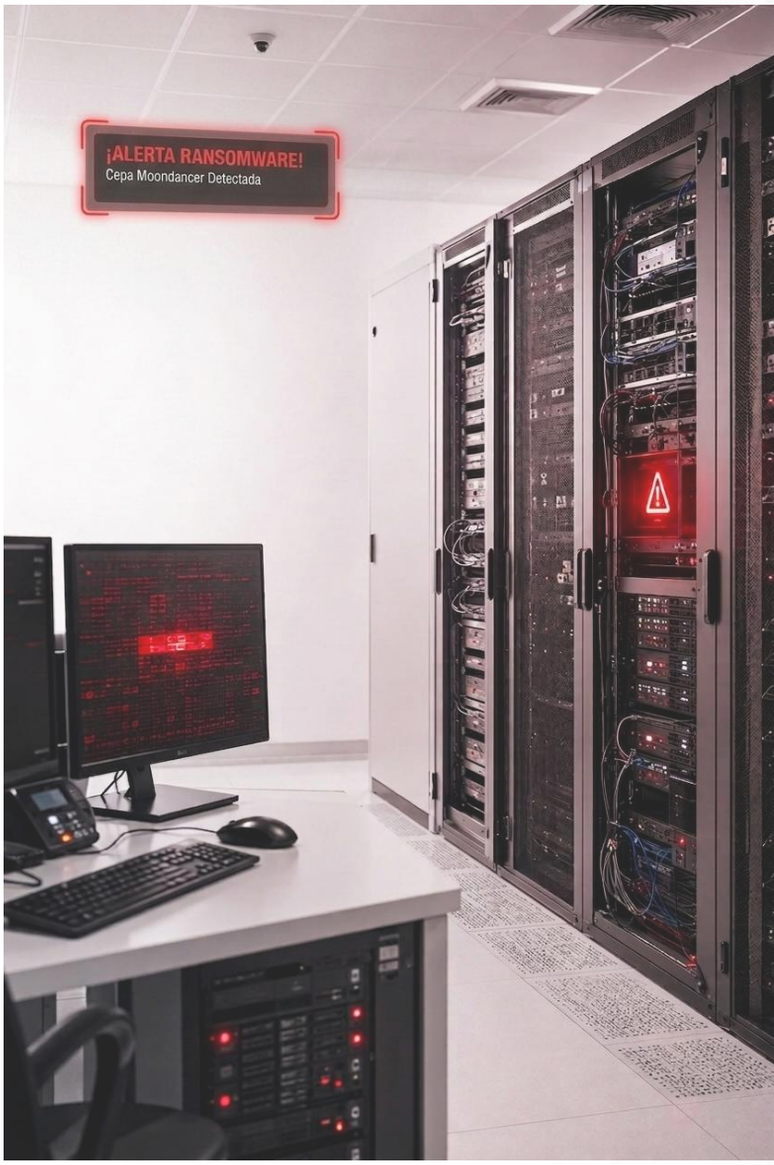
Alerta

Campaña de Ransomware – as – Service (RaaS) ”Moondancer”

COLCERT AL – 20260825 - 115

TLP:CLEAR

Resumen Ejecutivo



El grupo de amenaza conocido como EXILIADOS (identificado en Telegram y en foros clandestinos de la Dark Web bajo el alias Straightonnumberone) ha lanzado una campaña activa de reclutamiento de afiliados para Moondancer, una nueva variante de ransomware operada bajo el modelo Ransomware-as-a-Service (RaaS) y orientada a operaciones de Big Game Hunting.

Esta campaña se dirige explícitamente a organizaciones de América Latina que operan infraestructura crítica, con la excepción declarada del sector salud, al cual el grupo afirma no atacar. El proceso de reclutamiento se está desarrollando a través del canal de Telegram de la organización y en el foro clandestino darkforums[.]ru, donde el actor de amenazas inauguró públicamente su programa de afiliados el 16 de agosto de 2026, reiterando la convocatoria el 20 de agosto.

Para consolidar sus capacidades de intrusión, el grupo busca vincular tres perfiles específicos de colaboradores: Initial Access Brokers (IABs) con capacidad para proveer acceso inicial, preferentemente mediante credenciales legítimas; operadores de pentesting con experiencia avanzada en Active Directory, entornos híbridos (Azure, AWS, Google Cloud) y plataformas de virtualización (VMware ESXi, vCenter); y desarrolladores con dominio de C, ASM o Rust, orientados a Windows Internals, desarrollo a nivel de kernel, criptografía e ingeniería inversa.

NIVEL DE RIESGO

ALTO

Como contraprestación, EXILIADOS ofrece a sus afiliados un porcentaje variable de las ganancias producto de los rescates, sumado a asesoramiento técnico en tiempo real durante las fases de reconocimiento, movimiento lateral y despliegue. Cabe destacar que la herramienta de cifrado promocionada opera exclusivamente sobre arquitecturas Windows, emplea el esquema criptográfico XChaCha20 + ECDH y, según las afirmaciones del grupo, posee capacidades probadas para evadir o deshabilitar soluciones EDR/XDR líderes en el mercado, tales como CrowdStrike, SentinelOne y Sophos.

Contexto de la amenaza

El actor de amenazas que motiva esta alerta opera bajo el nombre de grupo EXILIADOS en Telegram y utiliza el alias Straightonnumberone en foros de la Dark Web. De acuerdo con la inteligencia disponible, su actividad fue detectada por primera vez el 16 de agosto de 2026, fecha en la que el grupo anunció oficialmente en el foro clandestino darkforums[.]ru la apertura de su programa de afiliados para el ransomware Moondancer.

La aparición de este actor representa un riesgo inminente para Colombia, dado que su campaña está dirigida explícitamente a organizaciones de América Latina que operan infraestructuras críticas. Este alcance abarca sectores estratégicos como el energético, financiero, gubernamental, de telecomunicaciones y de transporte, con la única excepción declarada del sector salud. Asimismo, el modelo de reclutamiento RaaS amplía de manera significativa la capacidad operativa del grupo al integrar a especialistas externos (IABs, pentesters y desarrolladores), lo que incrementa tanto la probabilidad como la velocidad de materialización de ataques de Big Game Hunting contra entidades de la región.

Motivaciones y objetivos

La principal motivación documentada de este actor es de carácter estrictamente económico. Al operar bajo un esquema Ransomware-as-a-Service (RaaS) orientado al Big Game Hunting, el grupo focaliza sus esfuerzos en comprometer víctimas de alto valor estratégico que posean la capacidad financiera para afrontar el pago de rescates significativos. El objetivo central de su programa de afiliados es escalar su capacidad operativa de manera acelerada. Para lograrlo, buscan incorporar a su ecosistema criminal a terceros altamente especializados en la provisión de acceso inicial, técnicas de pentesting y el desarrollo de herramientas ofensivas, garantizando así operaciones más eficientes y sostenidas en el tiempo.

Perfil de colaboradores buscados

Para materializar sus operaciones, el grupo busca reclutar activamente tres perfiles específicos de afiliados, detallados a continuación según la inteligencia recopilada en sus comunicados:

- **Initial Access Brokers (IABs):** Especialistas enfocados en la provisión de acceso inicial a redes corporativas, priorizando explícitamente la obtención y el uso de credenciales legítimas comprometidas.

- **Operadores de Pentesting:** Expertos con habilidades avanzadas en la explotación de redes basadas en Windows Active Directory, entornos híbridos (arquitecturas on-premise y nube: Azure, AWS, Google Cloud) y plataformas de virtualización críticas (VMware ESXi, vCenter).

- **Desarrolladores**: Programadores con dominio de lenguajes como C, ASM y/o Rust, que acrediten experiencia en *Windows Internals*, desarrollo a nivel de *kernel*, implementaciones criptográficas e ingeniería inversa (mediante el uso de herramientas como IDA Pro).

Como esquema de retribución, el grupo ofrece a sus miembros un porcentaje variable de las ganancias derivadas de los rescates extorsivos. Adicionalmente, garantizan soporte y asesoramiento técnico continuo por parte de sus operadores principales durante las fases de reconocimiento, movimiento lateral y despliegue del arsenal de Moondancer.

Este modelo de afiliación se promociona sin costo de ingreso, quedando supeditado de manera exclusiva a la capacidad demostrada del candidato para "aportar valor" estratégico y operativo a la organización criminal.

Técnicas y Tácticas – MITRE ATT&CK

Corresponde a las capacidades y el modus operandi promocionados por el grupo para sus afiliados.

Táctica	ID	Técnica / Subtécnica	Detalle documentado
Acceso Inicial (Initial Access)	T1078	Valid Accounts	Búsqueda y uso de credenciales legítimas entregadas por Initial Access Brokers (IABs) afiliados para obtener acceso a las redes objetivo.
Ejecución (Execution)	T1204	User Execution	Ejecución del binario de cifrado de Moondancer en los sistemas objetivo (mecanismo de disparo no detallado en la fuente).
Evasión de Defensas (Defense Evasion)	T1685	Disable or Modify Tools	Módulos anunciados para neutralizar/evadir soluciones EDR/XDR, con pruebas reclamadas contra CrowdStrike, SentinelOne y Sophos.
Descubrimiento (Discovery)	T1087 / T1069	Account Discovery / Permission Groups Discovery	Reconocimiento de cuentas y grupos en Active Directory y entornos en la nube (AWS, Azure, GCP) y de virtualización (VMware ESXi, vCenter).
Movimiento Lateral (Lateral Movement)	T1021	Remote Services	Despliegue de herramientas y pivoteo dentro de la red interna mediante protocolos remotos, con asesoramiento en tiempo real de los operadores de EXILIADOS.
Impacto (Impact)	T1486	Data Encrypted for Impact	Cifrado de archivos con el esquema criptográfico XChaCha20 + ECDH (cifrado simétrico de flujo combinado con intercambio de claves de curva elíptica).

Infraestructura de promoción reclutamiento

- **Canal de Telegram:** EXILIADOS — canal principal de promoción del RaaS y punto de contacto para interesados en afiliarse.
- **Foro clandestino:** darkforums[.]ru (servicio interno referenciado como forum_darkforums), hilo "[RaaS] Moondancer Ransomware", accesible mediante la URL hxxps://darkforums[.]ru/Thread-RaaS-Moondancer-Ransomware.

Herramienta de cifrado/descifrado (Moondancer)

- **Plataforma objetivo:** Windows, exclusivamente (según lo declarado por el propio grupo).
- **Esquema criptográfico:** XChaCha20 (cifrado simétrico de flujo, variante extendida de ChaCha20) combinado con ECDH (Elliptic-curve Diffie–Hellman, para el intercambio de claves).
- **Distribución declarada:** El grupo ofrece "acceso gratuito" a la herramienta de cifrado/descifrado a los afiliados que se vinculen al programa; no se documenta comercialización directa a terceros no afiliados.

Capacidades de evasión de defensas reclamadas

El grupo afirma ofrecer "desprotección inmediata y garantizada de cualquier endpoint con una solución de seguridad de tipo EDR/XDR", mencionando explícitamente pruebas exitosas contra las siguientes soluciones:

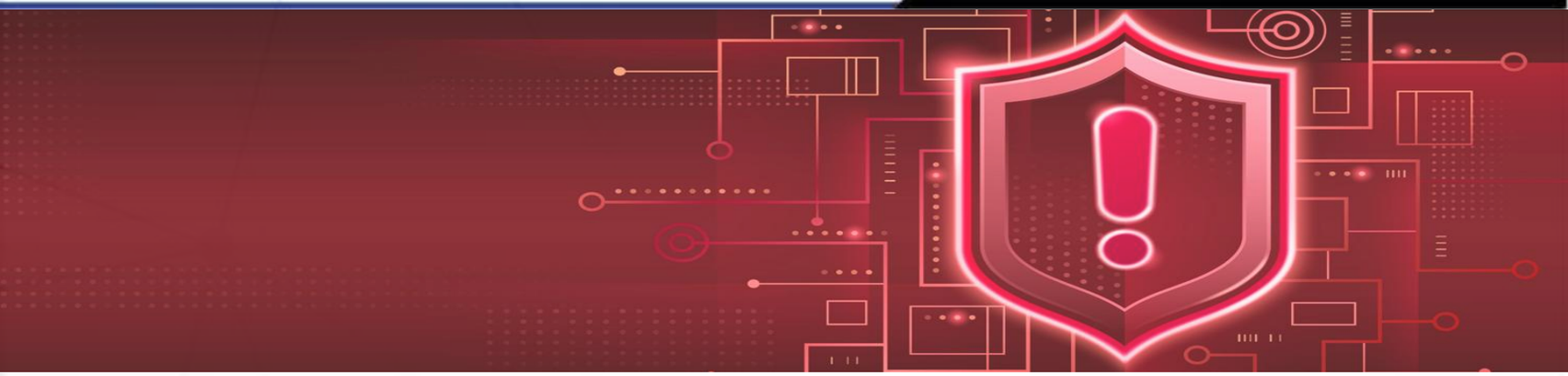
- **CrowdStrike (EDR/XDR).**
- **SentinelOne (EDR/XDR).**
- **Sophos (EDR/XDR).**

Recomendaciones técnicas

Las siguientes recomendaciones se formulan a partir de las tácticas, técnicas y capacidades descritas anteriormente.

Control de acceso y gestión de credenciales (frente a T1078 – Valid Accounts)

- Aplicar autenticación multifactor (MFA) resistente a phishing en todos los accesos remotos, VPN, VDI y consolas de administración (incluyendo vCenter, ESXi y consolas de nube AWS/Azure/GCP).
- Rotar credenciales privilegiadas de forma periódica y monitorear el uso de cuentas de servicio o cuentas legítimas desde ubicaciones, horarios o dispositivos atípicos.
- Implementar el principio de privilegio mínimo y revisar cuentas con acceso privilegiado a Active Directory y a plataformas de virtualización/nube.
- Monitorear activamente foros clandestinos y mercados de acceso inicial (Initial Access Brokers) en busca de ofertas de venta de accesos a la organización propia.



Detencción y respuesta en endpoint (frente a T1685 – Disable or Modify Tools)

- ❑ Habilitar y auditar la protección contra manipulación (tamper protection) en las soluciones EDR/XDR desplegadas, en particular CrowdStrike, SentinelOne y Sophos, dado que el actor reclama capacidad de evasión sobre estos productos específicos.
- ❑ Configurar alertas de alta prioridad ante intentos de detención de servicios de seguridad, desinstalación de agentes EDR o carga de controladores no firmados o no reconocidos (posible indicio de técnicas BYOVD, aunque no confirmado en la fuente para Moondancer).
- ❑ Verificar que las políticas de EDR/XDR estén administradas de forma centralizada, con protección por contraseña o token contra modificación local, y sin posibilidad de desactivación desde el propio endpoint por usuarios no autorizados.

Segmentación de red y hardening de infraestructura híbrida (frente a T1087/T1069, T1021)

- ❑ Segmentar la red de forma que los sistemas de gestión de virtualización (vCenter, hosts ESXi) no sean accesibles desde segmentos de usuario final ni expuestos a internet.
- ❑ Restringir y monitorear el uso de protocolos de administración remota (RDP, WinRM, SSH, PowerShell remoting) mediante listas de control de acceso, autenticación reforzada y registro centralizado.
- ❑ Aplicar hardening a Active Directory: auditoría de grupos privilegiados, protección de cuentas, y monitoreo de consultas masivas de reconocimiento (enumeración de cuentas y grupos).
- ❑ Revisar la configuración de seguridad de las cuentas de administración de AWS, Azure y Google Cloud (IAM), incluyendo la eliminación de credenciales de larga duración innecesarias y la aplicación de MFA obligatorio.

Protección de datos y respaldo (frente a T1486 – Data Encrypted for Impact)

- ❑ Mantener copias de respaldo (backups) desconectadas de la red (offline) o inmutables, con pruebas periódicas de restauración.
- ❑ Verificar que los backups no sean accesibles con las mismas credenciales administrativas utilizadas en producción.

Conclusión

La campaña de reclutamiento de afiliados para el ransomware Moondancer, atribuida al grupo EXILIADOS (Straightonnumberone), representa una amenaza emergente con un nivel de impacto Alto para las organizaciones de infraestructura crítica en Colombia y América Latina. Aunque hasta la fecha no se han confirmado víctimas, ni se han aislado muestras del malware o identificado infraestructura de Comando y Control (C2) operativa en las fuentes de inteligencia, el reclutamiento activo de Initial Access Brokers (IABs), pentesters y desarrolladores especializados constituye una clara señal de alerta temprana. Esta fase de preparación evidencia la consolidación de una capacidad ofensiva estructurada, con objetivos estratégicos y un modus operandi que ya han sido declarados abiertamente por el propio actor de amenazas.

Fuentes

Google. (s. f.). Google Threat Intelligence. Google Cloud.
https://cloud.google.com/security/products/threat-intelligence

Google. (s. f.). VirusTotal
https://www.virustotal.com/

MITRE. (s. f.). MITRE ATT&CK®.
https://attack.mitre.org/