Nro. Alerta:	AL-2026-050	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	2-oct-2026	Barracuda (BRKD): Nuevo grupo de ransomware con modelo de doble extorsión	Pág.: **1** of **6**

I. DATOS GENERALES:

Clase de alerta: Ransomware
Tipo de Incidente: Cifrado y posible exfiltración de información
Nivel de riesgo: Alta

II. ALERTA



Figura 1.- Barracuda (BRKD) – Ransomware emergente con doble extorsión - figura referencial

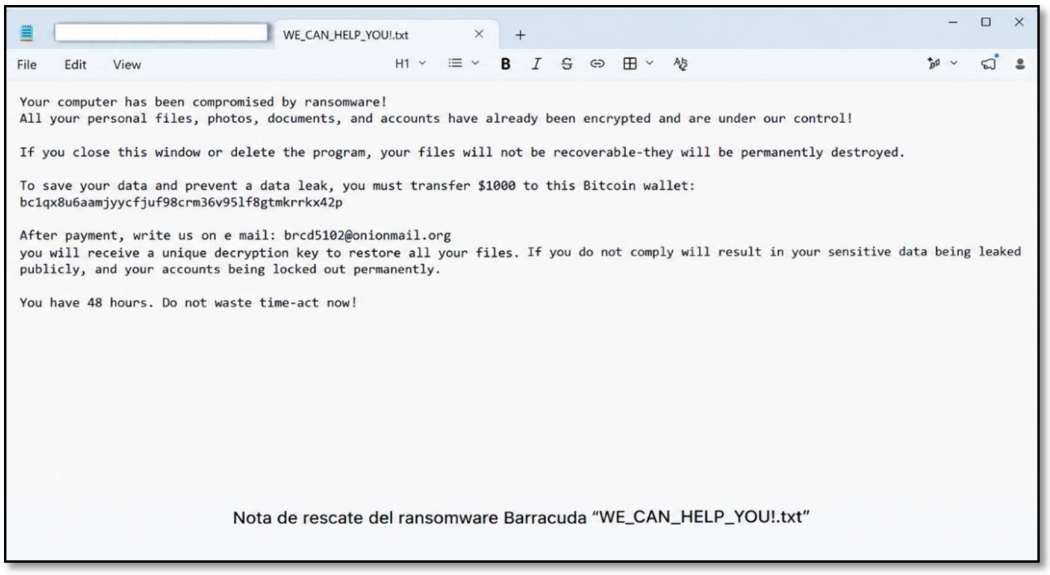
Se ha identificado un nuevo grupo de ransomware emergente denominado Barracuda, también asociado con el identificador BRKD, cuya actividad ha sido observada a comienzos del segundo semestre de 2026. La operación ha sido asociada con un modelo de doble extorsión y según evaluaciones de inteligencia disponibles, con un posible modelo Ransomware-as-a-Service (RaaS). Entre sus características observadas se encuentra el uso de la extensión .BRKD para los archivos cifrados y una nota de rescate denominada WE_CAN_HELP_YOU!

III. INTRODUCCIÓN

La aparición constante de nuevos grupos y actores de amenaza, especialmente tras el desmantelamiento o la fragmentación de operaciones de ransomware previamente establecidos, continúa impulsando la evolución del panorama de amenazas. En este contexto, Barracuda (BRKD) se perfila como una de las amenazas emergentes que ha ganado visibilidad durante 2026. Debido a su reciente aparición, las plataformas de

identificación y recuperación de ransomware, como No More Ransom e ID Ransomware, pueden no reconocer de forma inmediata sus indicadores característicos, como extensiones de archivo o notas de rescate específicas, lo que dificulta la identificación temprana de la amenaza y puede generar incertidumbre en las organizaciones afectadas respecto a la recuperación de la información comprometida.

Las víctimas de Barracuda han reportado que miles de archivos han sido renombrados con la extensión .BRKD, incluyendo documentos, imágenes, hojas de cálculo e instaladores. En un caso documentado se registraron aproximadamente 9.592 archivos cifrados, mientras que la nota de rescate WE_CAN_HELP_YOU!.txt apareció 1.098 veces en todo el sistema afectado.



Nota de rescate del ransomware Barracuda "WE_CAN_HELP_YOU!.txt"

Figura 2.- Nota de Rescate - Barracuda (BRKD), ransomware emergente con doble extorsión.

El modelo operacional atribuido a Barracuda corresponde al esquema de Ransomware-as-a-Service (RaaS) y doble extorsión, mediante el cual los operadores exigen un pago de USD 1.000 en Bitcoin, con un plazo máximo de 48 horas. La amenaza contempla la posible publicación de los datos exfiltrados en su sitio de filtración de datos (DLS) y otras medidas de presión contra la víctima en caso de incumplimiento.

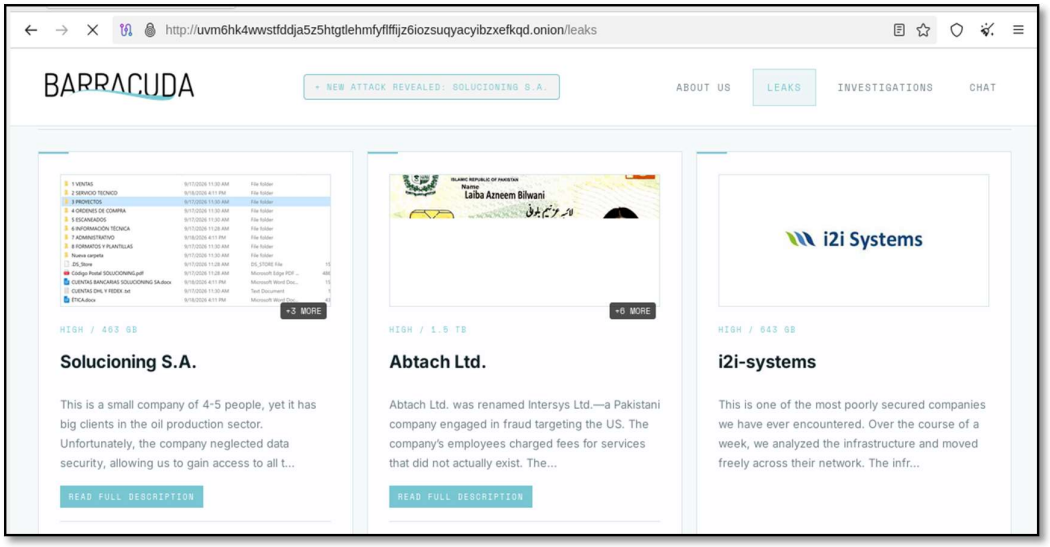


Figura 3.- Sitio de filtración de datos (DLS) - Barracuda (BRKD) – Ransomware emergente con doble extorsión.

IV. VECTOR DE ATAQUE

Lo que hace que Barracuda ransomware sea particularmente difícil de descifrar es el esquema criptográfico empleado. En lugar de implementar una biblioteca criptográfica personalizada, el análisis de los archivos afectados reveló que sus desarrolladores optaron por utilizar las funcionalidades criptográficas nativas de Windows, mediante la interfaz de programación de aplicaciones (API), CryptoAPI de Microsoft, para realizar operaciones relacionadas con la generación y gestión de claves, así como con el cifrado mediante un esquema AES-256 simétrico + RSA asimétrico.

En este esquema, AES-256 se utiliza para cifrar los archivos, mientras que las claves AES utilizadas durante el proceso de cifrado son protegidas mediante RSA. La mayoría de las muestras analizadas incluían un pie de página de 276 bytes, que contenía un SIMPLEBLOB de CryptoAPI, una clave protegida mediante RSA de 256 bytes y la longitud de los datos cifrados. Una vez completado el proceso de cifrado, los archivos afectados son renombrados utilizando la extensión .BRKD, identificándolos como archivos cifrados por Barracuda ransomware.

Este enfoque permite al malware aprovechar componentes criptográficos ya disponibles en el sistema operativo, reduciendo la necesidad de incorporar bibliotecas criptográficas de terceros dentro del ejecutable. No obstante, el uso de CryptoAPI por sí solo no garantiza la evasión de mecanismos de detección, ya que las soluciones de seguridad pueden identificar el ransomware mediante indicadores de comportamiento, patrones de cifrado, modificaciones masivas de archivos y otras características del código.

V. IMPACTO

Sector Empresarial
Educación
Tecnología
Fabricación
Salud

Tabla 1.- Sectores afectados - Barracuda (BRKD) – Ransomware emergente con doble extorsión

Países Afectados
Estados Unidos
Argentina
Brasil
Corea del Sur
China
Turquía
Pakistan

Tabla 2.- Países afectados - Barracuda (BRKD) – Ransomware emergente con doble extorsión

VI. INDICADORES DE COMPROMISO

Extensión
.BRKD

Tabla 3.- Extensión de archivos asociada - Barracuda (BRKD) – Ransomware emergente con doble extorsión

Emails
brcd5102@onionmail[.]org
writetousbrkd@2mail[.]co
cuda@paranoid[.]network

Tabla 4.- Direcciones de correo electrónico asociadas - Barracuda (BRKD) – Ransomware emergente con doble extorsión

DLS
hxxps[:]//barracuda[.]name
hxxp[:]//darkfoxaqhfpxkrbt7vxns2z2u2k72sgmqbzeorupaiottw3ecm2wgyd[.]onion/User-BRKD
hxxp[:]//uvm6hk4wwstfddja5z5htgtlehmfyflffijz6iozsuqyacyibzxefkqd[.]onion

Tabla 5.- Sitios de filtración de datos (DLS) asociados - Barracuda (BRKD) – Ransomware emergente con doble extorsión

VII. RECOMENDACIONES:

- 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.
- Utilizar EDR/XDR para detectar comportamientos como ejecución sospechosa, movimiento lateral, modificación masiva de archivos y actividades asociadas al cifrado.
- 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
- 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). *Barracuda Ransomware Gang: 3 New Victims Posted – Healthcare and Manufacturing Campaign Analysis with Detection Rules.*

https://securityarsenal.com/blog/barracuda-ransomware-gang-3-new-victims-posted-healthcare-and-manufacturing-campaign-analysis-with-detection-rules

MONSTER CLOUD. (2026). *Barracuda Ransomware (BRKD) Recovery.* https://monsterclouddecryptor.com/en/ransomware-recovery/barracuda-ransomware-brkd-recovery/

SOCRADAR. (2026). *Barracuda Ransomware Group.* https://socradar.io/free-tools/ransomware-intelligence/groups/barracuda

WATCHGUARD. (2026). *Barracuda Ransomware Tracker.* https://www.watchguard.com/es/wgrd-security-hub/ransomware-tracker/barracuda

BLEEPINGCOMPUTER. (2026). *Barracuda Ransomware (BRKD) – We Can Help You Support Topic.* https://www.bleepingcomputer.com/forums/t/818258/barracuda-ransomware-brkd%3B-we-can-help-you-support-topic/