Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

GUNRA RANSOMWARE: NUEVA VARIANTE PARA LINUX REFUERZA CAPACIDADES DE CIFRADO MASIVO Y PERSONALIZACIÓN

02/ 08 / 2025

CONTENIDO

INTRODUCCIÓN

La aparición de una nueva variante del ransomware Gunra dirigida a sistemas Linux representa una evolución significativa dentro del panorama de amenazas cibernéticas actuales. Con capacidades avanzadas de cifrado altamente configurables y multihilo, esta versión demuestra una clara estrategia por parte del grupo atacante de ampliar su alcance operativo hacia infraestructuras críticas basadas en Linux, tradicionalmente consideradas más resistentes frente a este tipo de ataques. Este cambio no solo incrementa el riesgo para organizaciones con entornos híbridos, sino que también pone en evidencia la creciente sofisticación de los grupos de ransomware contemporáneos.

Desde su detección inicial en abril de 2025, Gunra ha expandido rápidamente sus operaciones a escala global, afectando sectores sensibles como salud, manufactura, TI y servicios legales. La nueva variante, que prescinde de elementos comunes como la nota de rescate y prioriza la velocidad y la flexibilidad del cifrado, plantea desafíos significativos en términos de detección y contención. Este informe examina los aspectos técnicos de la variante para Linux, su impacto potencial en el entorno empresarial y las medidas que las organizaciones deben adoptar para mitigar su riesgo.

GUNRA RANSOMWARE: NUEVA VARIANTE PARA LINUX REFUERZA CAPACIDADES DE CIFRADO MASIVO Y PERSONALIZACIÓN

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_08_02_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	02/08/2025
Es día cero (0 day):	No

RESUMEN

Una reciente investigación ha revelado una variante del ransomware Gunra diseñada específicamente para sistemas Linux, lo que confirma la intención del grupo de expandirse más allá de su enfoque inicial sobre entornos Windows. Esta nueva versión introduce mejoras técnicas significativas que optimizan el proceso de cifrado, lo hacen más rápido, más flexible y, sobre todo, más difícil de mitigar.

Desde su primera actividad identificada en abril de 2025, Gunra ha impactado a organizaciones en sectores críticos y en múltiples regiones geográficas. Su evolución hacia una arquitectura de ransomware multiplataforma representa una amenaza seria para la continuidad operativa de las empresas.

Alcance internacional y víctimas reportadas
El grupo Gunra ha sido vinculado con campañas contra empresas en Brasil, Japón, Canadá, Turquía, Corea del Sur, Taiwán y Estados Unidos, abarcando sectores como manufactura, salud, tecnologías de la información, derecho, agricultura y consultoría. Según reportes de inteligencia, el grupo también habría filtrado 40 terabytes de información perteneciente a un hospital ubicado en Dubái, lo que muestra su capacidad de generar impacto a gran escala.

Desde abril de 2025, su sitio de filtraciones ha publicado detalles de 14 víctimas confirmadas, lo que sugiere una campaña activa y sostenida.

Características técnicas de la variante Linux
Esta nueva variante presenta elementos avanzados que incrementan su eficacia y flexibilidad operativa:

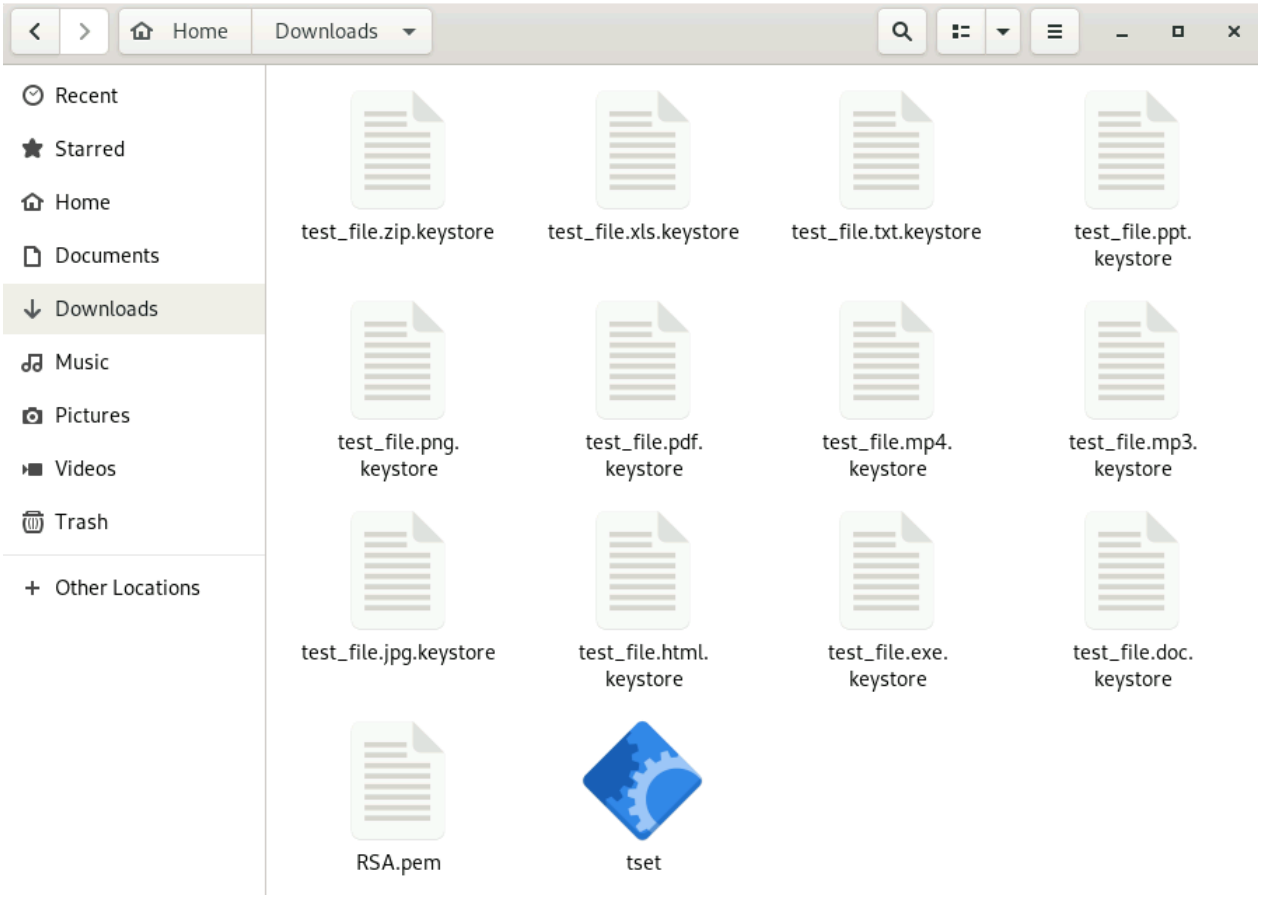
Cifrado multihilo configurable
La versión para Linux permite configurar hasta 100 hilos de cifrado en paralelo, una capacidad superior a la mayoría de ransomware conocidos hasta la fecha. Esto permite acelerar la operación de cifrado en entornos de alto rendimiento.

Soporte para cifrado parcial
A través de parámetros específicos, los atacantes pueden controlar qué porcentaje de cada archivo es cifrado, así como establecer un límite máximo por archivo, lo que permite realizar ataques más rápidos y menos detectables.

Personalización del objetivo
La variante puede cifrar archivos individuales, directorios completos e incluso dispositivos de bloque, como discos duros. El ransomware acepta listas de extensiones o configuraciones amplias como “all” para cifrar todos los archivos detectados.

Manejo de claves cifradas en keystores externos

De forma opcional, la variante puede guardar el blob cifrado con clave RSA en un archivo separado (keystore) en lugar de incluirlo en el archivo cifrado, lo que complica los esfuerzos de recuperación.



Ausencia de nota de rescate

A diferencia de muchas otras familias de ransomware, Gunra en su variante para Linux no deja una nota de rescate, priorizando la velocidad y sigilo del ataque.

Algoritmo de cifrado utilizado

La rutina de cifrado emplea una combinación de ChaCha20 y RSA. Para cada archivo, se generan materiales criptográficos únicos: una clave ChaCha20 de 32 bytes, un nonce de 12 bytes y datos de relleno de 256 bytes. Esta información se cifra con la clave pública RSA proporcionada en un archivo PEM. El proceso permite cifrado parcial o completo, según los parámetros definidos en tiempo de ejecución.

Implicaciones para la ciberseguridad empresarial

La aparición de esta variante para Linux representa un cambio táctico importante en la evolución de Gunra. Su capacidad de operar en múltiples sistemas operativos refuerza una tendencia creciente entre grupos de ransomware: diversificar vectores de ataque y aumentar la eficiencia técnica.

Organizaciones con entornos mixtos Windows/Linux o con infraestructura crítica basada en Linux deben tomar medidas proactivas. La posibilidad de cifrado rápido y personalizado, sin dejar evidencia inmediata

(como una nota de rescate), aumenta el riesgo de que un ataque pase desapercibido hasta que el daño sea irreversible.

Recomendaciones para mitigar riesgos

Las siguientes medidas de seguridad pueden ayudar a reducir la superficie de ataque ante amenazas como Gunra:

- Realizar inventario y auditoría continua de activos, sistemas y registros de eventos.
- Controlar configuraciones de hardware y software, así como servicios, puertos y protocolos abiertos.
- Aplicar configuraciones seguras en dispositivos de red como firewalls y routers.
- Ejecutar evaluaciones de vulnerabilidades y aplicar parches de seguridad de manera oportuna.
- Capacitar al personal regularmente en buenas prácticas de ciberseguridad y gestión de incidentes.
- Implementar ejercicios de red team y pruebas de penetración periódicas.
- Utilizar plataformas de detección avanzada basadas en inteligencia artificial y análisis comportamental.

Conclusión

Gunra ransomware continúa su evolución agresiva y se posiciona como una amenaza seria para entornos empresariales modernos. La aparición de esta variante Linux reafirma la necesidad de estrategias de ciberdefensa integrales, que consideren tanto la diversificación de sistemas operativos como el incremento en la sofisticación técnica de los ataques. Las organizaciones deben prepararse con capacidades de prevención, detección y respuesta basadas en inteligencia contextualizada y tecnología avanzada.

Indicadores de compromiso

NOTICIA COMPLETA

https://devel.group/blog/gunra-ransomware-nueva-variante-para-linux-refuerza-capacidades-de-cifrado-masivo-y-personalizacion/

CONTACTOS DE SOPORTE

Correo electrónico: cti@devel.group

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group/