Alerta

Ransomware dirigido a sistemas Linux -Linux Locker-

COLCERT AL – 20260908 - 117

TIC

TLP:CLEAR

Resumen Ejecutivo

El ColCERT identificó y analizó un ransomware dirigido a sistemas operativos Linux, denominado «Linux Locker». El artefacto cifra los archivos del equipo, elimina los originales y ataca de forma activa los mecanismos de respaldo local, afectando gravemente la disponibilidad de la información y de los servicios del sistema.

Este boletín resume, para las áreas de TI, las características más relevantes de la amenaza evidenciadas durante el análisis técnico, así como las recomendaciones preventivas y respuesta ante una posible infección.

¿Qué le hace a un equipo infectado?

- Cifra los archivos del sistema, dejándolos inaccesibles.
- Elimina los archivos originales una vez son cifrados.
- Ataca y destruye los respaldos (backups) o copias de seguridad locales disponibles.

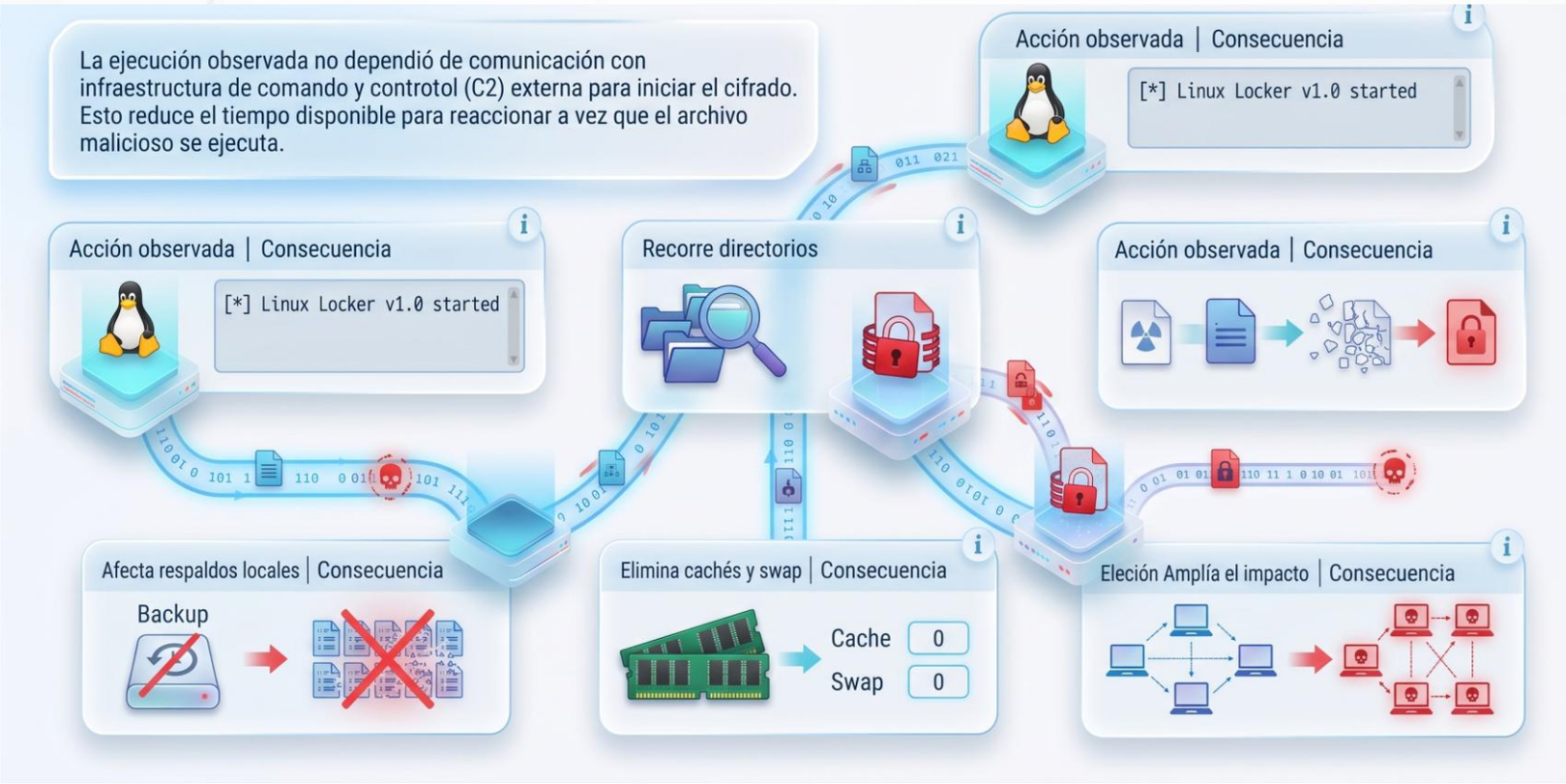
¿Por qué esta amenaza puede causar una interrupción grave?

- Bloquea los elementos del sistema y les añade la extensión .linux.
- Suprime las versiones iniciales tras el compromiso de los datos.
- Inutiliza los repositorios y recursos locales de recuperación.
- Puede dejar plataformas y servidores sin información operativa, paralizando la actividad.

NIVEL DE RIESGO

ALTO

¿Cómo actúa el ransomware una vez ejecutado?



Lo que confirmó el análisis de la muestra

La ejecución observada no dependió de una comunicación con servidores externos para iniciar el cifrado, esto reduce el tiempo disponible para reaccionar una vez que el archivo malicioso se ejecuta.

Resultados observados en el entorno controlado

- Los archivos comprometidos terminaron con extensión .linux.
- Los archivos originales fueron eliminados durante la ejecución.
- Se observó afectación directa sobre /var/backups/, /swap.img y la caché local de paquetes.
- El barrido alcanzó información de usuario, aplicaciones y componentes del sistema.

Uno de los primeros indicios de la intrusión es un mensaje que el propio artefacto imprime en la consola del sistema al iniciar su ejecución: **[*] Linux Locker v1.0 started**

Resultados observado en el entorno controlado

- Los archivos comprometidos terminaron con extensión .linux.
- Los archivos originales fueron eliminados durante la ejecución.
- Se observó afectación directa sobre /var/backups/, /swap.img y la caché local de paquetes.
- El barrido alcanzó información de usuario, aplicaciones y componentes del sistema.

Uno de los primeros indicios de la intrusión es un mensaje que el propio artefacto imprime en la consola del sistema al iniciar su ejecución: **[*] Linux Locker v1.0 started**

Señales de alerta: ¿Qué otros indicacores debo observar?

- Aparición de elementos con una extensión adicional distinta a la legítima, producto del cifrado.
- Desaparición o corrupción repentina de copias de seguridad locales.
- Alto uso de CPU o disco originado por procesos desconocidos que corren desde rutas temporales.
- Imposibilidad de acceder a documentos, bases de datos o directorios de uso habitual.

Matriz MITRE ATT & CK

Táctica	Técnica (ID)	Observación
Descubrimiento	File and Directory Discovery (T1083)	Exploración del árbol de directorios locales y archivos de usuario.
Ejecución	Command and Scripting Interpreter: Unix Shell (T1059.004)	Uso de /bin/sh y xterm para orquestar la ejecución del binario.
Evasión de defensa	Indicator Removal on Host: Clear Linux or Mac System Logs (T1070.002)	Rotación de rsyslog.service observada durante la ejecución; la atribución directa a la muestra, frente a actividad propia de mantenimiento del sistema, queda pendiente de validación.
Evasión de defensa	Obfuscated Files or Information (T1027)	Se identificaron cuatro técnicas de cifrado/ofuscación en el ejecutable: AES-NI, XOR, Base64 y RC4.
Impacto	Data Encrypted for Impact (T1486)	Cifrado masivo de archivos del sistema, con asignación de la extensión .linux.
Impacto	Data Destruction (T1485)	Eliminación de los archivos originales y borrado del archivo /swap.img.
Impacto	Inhibit System Recovery (T1490)	Destrucción de los respaldos locales y archivos de restauración disponibles en el sistema.

Indicadores de Compromiso (IoC)

Binario principal — Linux Locker v1.0

Indicador	Valor
SHA-256	`f1e1ac594f43f8b38be222c2b6b256f4aaf3d22d2c67f92f8953a929f2e3fa87`
SHA-1	`d52d735e470e2fde4ae66b519747687b4dc3e823`
MD5	`629358fb9b1bd8958be61462133ac255`
Formato	`ELF 64-bit LSB executable, AMD x86-64, static-pie linked, stripped`
Extensión de cifrado	`.linux`
Banner en consola	`[*] Linux Locker v1.0 started`
Correo embebido	`Enigma_2@aol[.]com`

Nota importante: la muestra también contiene una dirección IP de infraestructura compartida de Cloudflare y los dominios docs[.]rs y aol[.]com, correspondientes a servicios legítimos de uso masivo (documentación de crates de Rust y correo AOL).

No se recomienda su bloqueo genérico; se listan únicamente como artefactos embebidos en el binario, sin evidencia de infraestructura maliciosa dedicada.

Recomendaciones para detección y monitoreo

Las organizaciones deben prestar especial atención a comportamientos inusuales que puedan sugerir una infección por ransomware, entre los cuales se destacan:

- ❑ Cambios masivos en nombres o extensiones de archivos.
- ❑ Procesos anómalos con alto consumo de recursos (CPU o disco).
- ❑ Eliminación o modificación inesperada de los repositorios de almacenamiento locales.
- ❑ Ejecución de binarios desde directorios temporales o rutas de escritura de usuarios.
- ❑ Pérdida repentina de acceso a bases de datos u otros archivos críticos.

La detección temprana de estos eventos puede ayudar a reducir el impacto y facilitar la activación oportuna de los procedimientos de respuesta a incidentes.

Recomendaciones de prevención

Regla de oro: Asegure su continuidad operativa, implemente de inmediato la estrategia de respaldo 3-2-1 garantizando que al menos una copia permanezca aislada de la red (offline). Asimismo, bloquee sistemáticamente cualquier ejecutable de origen dudoso e implemente la verificación obligatoria antes de ejecutar comandos o binarios recibidos por correo electrónico.

Medidas específicas para entornos Linux

- Restringir la ejecución de binarios en /tmp y otros directorios de escritura de usuario (empleando el montaje con la opción noexec).
- Exigir autenticación mediante llave SSH y múltiple factor (MFA) para el acceso remoto administrativo; deshabilitar el acceso por contraseña cuando sea posible.
- Mantener el sistema operativo y el kernel actualizados con los últimos parches de seguridad.
- Aplicar el principio de menor privilegio a cuentas de servicio y auditar periódicamente los permisos de sudo.

Protección de las copias de seguridad

Dado que el comportamiento de esta amenaza incluye la destrucción de recursos locales de recuperación, se recomienda:

- Conservar múltiples copias de la información siguiendo la regla 3-2-1.
- Mantener una copia desconectada o aislada del entorno operativo.
- Probar periódicamente los procedimientos de restauración.
- Restringir el acceso a los repositorios de respaldo mediante el principio de mínimo privilegio.
- Verificar que una infección en un equipo o servidor no pueda eliminar o modificar automáticamente todas las copias disponibles.

¿Qué hacer si sospecha una infección?

- **Aislar el equipo:** desconectar la interfaz de red, el Wi-Fi y cualquier montaje compartido.
- Evitar la conexión de discos de almacenamiento u otros periféricos al host comprometido.
- Abstenerse de borrar evidencias, reinstalar el sistema o ejecutar herramientas improvisadas.
- No apagar,ni reiniciar sin la orientación del equipo de respuesta (la memoria puede contener evidencia forense útil).
- No pagar el rescate ni establecer contacto con los atacantes.
- Documentar la hora del evento, mensajes en pantalla, nombres de archivos y acciones realizadas.
- Notificar el incidente al área de seguridad de la información interna y tras su clasificación, escalarlo al CSIRT Gobierno / ColCERT.

¿Sabe si su organización está expuesta?

El ColCERT incluye, dentro de su portafolio de servicios, la ejecución de análisis especializados de vulnerabilidades en sitios web, servidores y demás activos de información. Estos escaneos permiten identificar de manera proactiva brechas de seguridad, configuraciones deficientes y exposiciones críticas, entregando los insumos técnicos necesarios para que las organizaciones puedan aplicar medidas de mitigación y fortalecer su postura de ciberseguridad.

Adicionalmente, el ColCERT, tiene la capacidad de efectuar revisiones específicas sobre entornos institucionales de Active Directory (Directorio Activo) para evaluar su nivel de hardening (endurecimiento) y la configuración básica de seguridad.

Para más información, le invitamos a comuníquese a través de los canales oficiales del CSIRT Gobierno / ColCERT.

contacto@colcert.gov.co

Línea directa:
+57 601 344 2222

Fuentes

Análisis dinámico interno del artefacto – CSIRT Gobierno / ColCERT (agosto de 2026).
MITRE ATT&CK®
https://attack.mitre.org/
CISA StopRansomware Guide
cisa.gov/stopransomware
CIS Controls v8
cisecurity.org/controls

Buenas prácticas de respaldo 3-2-1, aislamiento y recuperación segura.
Portal oficial CSIRT Gobierno / ColCERT –
www.colcert.gov.co
Gestión de Threat Intelligence (GTI) – CSIRT Gobierno / ColCERT
Herramienta DetecTIC – CSIRT Gobierno / ColCERT.
https://detectic.colcert.gov.co/