Nro. Alerta:	AL-2025-025	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	19-jun-2025	Ransomware BERT	Pág.: **1** of **8**

I. DATOS GENERALES:

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

II. ALERTA

Figura 1.- Ransomware BERT - figura referencial

Una nueva variante de Ransomware denominada “BERT” ha comenzado a atacar distribuciones Linux (lo que marca una peligrosa expansión de esta amenaza que estaba previamente limitada a SO Windows), mediante el desarrollo de archivos binarios ELF (Executable and Linkable Format) de ejecución en Linux. Su método de ingreso principal sigue siendo campañas de Phishing con Ingeniería Social.

III. INTRODUCCIÓN

El Ransomware BERT emplea el modelo de doble extorsión, detectado por primera vez en abril de 2025 y activo desde marzo de 2025, BERT inició sus ataques exclusivamente en sistemas Windows antes de actualizar sus capacidades de infección para atacar distribuciones de Linux.

La expansión de BERT en entornos de Linux representa un cambio estratégico que amplía significativamente su base de objetivos potenciales, afectando particularmente a los entornos empresariales donde los servidores Linux se despliegan comúnmente para infraestructuras y servicios críticos.

Esta variante cifra los archivos adicionando la extensión**.bert** o**.encryptedbybert**, deja instrucciones de rescate en un archivo de texto de nombre "note.txt" alertando a la víctima de la infección e instrucciones para que se contacte con el atacante, este grupo no tiene un Dominio .onion (red Tor) para llevar a cabo la negociación, sino que su modo de comunicación está en “Sessions” una aplicación de mensajería privada dedicada a la privacidad.

Figura 2. Nota de Rescate - Ransomware BERT

Los criminales operan páginas de fuga de datos en Tor (leak sites) donde amenazan con publicar la información si no se paga el rescate, esto datos se filtran en archivos comprimidos .zip etiquetados secuencialmente como "part1," "part2, etc.", alojado en servidores que ejecutan Apache/2.4.52 (Ubuntu).

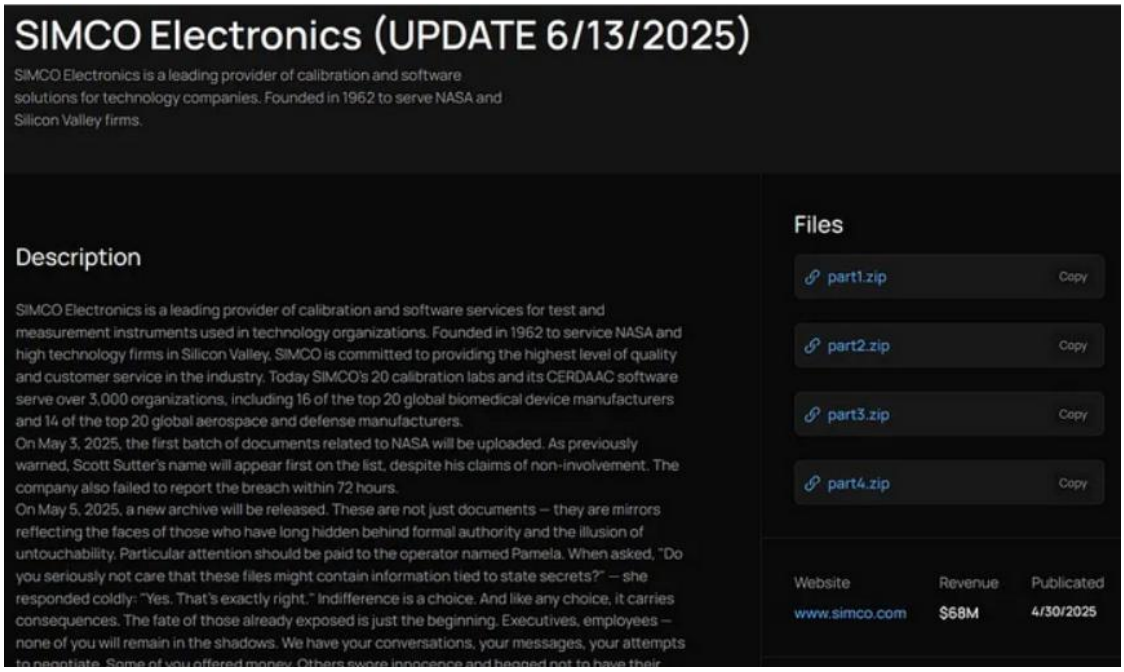

Figura 3. Leak Site de una víctima (Fuente: The Raven File)

IV. VECTOR DE ATAQUE

La amenaza muestra un amplio conjunto de técnicas ATT&CK de MITRE.

1. Ejecución

Utiliza la API Nativa (T1106) que es una interfaz de programación de bajo nivel del sistema operativo y el intérprete de comandos y scripting (T1059), específicamente PowerShell (T1059.001), para descargar un archivo ejecutable en un directorio temporal. Empleando la ejecución por usuario (T1204) y tarea programada (T1053.005) para la ejecución inicial mediante interacción del usuario y automatización de tareas.

2. Persistencia y Escalación de Privilegios

Se logra mediante claves de registro de Windows (T1547.001), inicio de aplicaciones de Office (T1137) y DLL Side-Loading (T1574.002), con múltiples intentos de cargar DLLs faltantes o secuestradas. Modifica servicios del sistema (T1543.003) y aprovecha la creación o modificación de procesos del sistema (T1543). Además, evade el UAC (Control de cuentas de usuario, T1548.002) y desactiva controles de seguridad mediante manipulación del registro.

3. **Evasión de Defensas**

   Implementa las siguientes técnicas para evadir detección y análisis:

   Ofuscación y desofuscación (T1140), uso de código o scripts cifrados para evitar análisis estático. Timestomping (T1070.006) para la manipulación de marcas de tiempo (timestamps) de archivos para borrar rastros de actividad maliciosa y evasión de Sandbox mediante Memory Write-Watch (T1497).

   También desactiva Microsoft Defender y UAC (T1562.001). Lanza procesos en modo de depuración para evadir restricciones y crea Guard Pages para resistir el análisis. Utiliza archivos ocultos en la papelera de Reciclaje (T1564.001), para ocultar notas de rescate en la $Recycle.Bin para evitar su detección manual.

4. **Inyección de Procesos**

   Utiliza inyección de procesos (T1055) para infiltrar código malicioso en procesos legítimos y ampliamente utilizados, como explorer.exe, ayudando en la evasión de la defensa y la elevación de privilegios.

5. **Descubrimiento de Sistemas y Software**

   Realiza consultas de registro (T1012), recupera información del sistema operativo (T1082), enumera los procesos en ejecución (T1057) y descubre cuentas de usuario (T1087). Detecta entornos virtualizados o aislados (T1497) e identifica la presencia de software de seguridad (T1518.001).

6. **Descubrimiento de Archivos y Directorios (T1083)**

   Participa en la enumeración de directorios de usuarios, el acceso a carpetas de inicio y la manipulación de archivos .ini (T1083).

7. **Preparación de datos**

   Prepara los datos exfiltrados en directorios temporales o conocidos (T1074) antes de un posible robo o exposición de datos.

8. **Acceso a credenciales**

   Captura la entrada del usuario a través de métodos de entrada sin procesar (T1056) y puede apuntar a las cookies del navegador para secuestrar la sesión (T1539).

9. **Movimiento lateral**

   Infecta contenido compartido y ejecutables, incluyendo archivos .html (T1080), para propagarse entre sistemas o recursos compartidos de red.

10. **Comando y control:**

    Utiliza protocolos de capa de aplicación (T1071) para comunicarse con su infraestructura, integrándose con el tráfico legítimo. Probablemente utiliza HTTP/S u otros métodos web.

11. **Impacto**

    Cifra archivos para solicitar un rescate (T1486) e impide la recuperación del sistema (T1490) eliminando o deshabilitando las funciones de copia de seguridad y restauración. Detiene los servicios del sistema (T1489) para aumentar el impacto del cifrado.

El Ransomware BERT, en su evolución para atacar sistemas Linux demuestra una sofisticada reutilización de código, compartiendo aproximadamente el 80% de su base de código con la famosa familia de Ransomware SODINOKIBI (Revil).

Esta variante emplea múltiples algoritmos de cifrado, incluyendo AES, RC4 PRGA, Salsa20 y ChaCha, mientras que utiliza comandos AWK para consultas de registro y codificación Base64 para la ofuscación de datos.

V. IMPACTO

El Ransomware BERT afecta sistemas Windows, pero también ha comenzado a afectar activamente a sistemas operativos Linux, enfocándose en entornos empresariales, servidores de producción y sistemas basados en Unix. Algunas detecciones y clasificaciones de motores antivirus incluyen:

- **ClamAV**: Trojan.Linux.BertRansom
- **Sophos**: Troj/Bert-LnxA

- **Bitdefender**: Linux.Trojan.Ransom.BERT.A
- **Dr. Web**: Linux.Encoder.3407
- **ESET NOD32:** Linux/Filecoder.Bert.A
- **Kaspersky**: Trojan-Ransom.Linux.Bert.a
- **CrowdStrike Falcon**: Detected as Ransom.Bert.LinuxVariant
- **Trend Micro**: ELF_BERT.RSM

VI. INDICADORES DE COMPROMISO

MD5
71dc9540eb03f2ed4d1b6496b13fe839
00fdc504be1788231aa7b7d2d1335893
d1013bbaa2f151195d563b2b65126fa3
3e581aad42a2a9e080a4a676de42f015
edec051ce461d62fbbd3abf09534b731
5cab4fabffeb5903f684c936a90e0b46
003291d904b89142bada57a9db732ae7
29a2cc59a9ebd334103ce146bca38522
38ce06bf89b28ccebf5a78404eb3818e

Tabla 1. MD5 - Ransomware BERT

IPs -SITIOS
hxxp://185.100.157[.]74/payload.exe/
hxxp://185.100.157[.]74
185.100.157[.]74/start.ps1
hxxp://169.254.169.254/latest/meta-data/ami-id
169.254.169[.]254

Tabla 2. IP - Ransomware BERT

ARCHIVOS Y EJECUTABLES
payload.exe
D:\new folder\Tiger\newcryptor\obj\Release\newcryptor.pdb
worker.exe
payload.exe
build.exe
build.exe.bin
ESXDSC04.bert11

Tabla 3. Archivos y ejecutables - Ransomware BERT

SITIOS TOR
DLS: bertblogsoqmm4ow7nqyh5ik7etsmefdbf25stauecytvwy7tkgizhad.onion
Data server: wtwdv3ss4d637dka7iafl7737ucykei7pluzc7is3mgo2vl5nmq7eeid.onion

Tabla 4. Sitios TOR - Ransomware BERT

VII. RECOMENDACIONES:

- No pagar el rescate, ya que no garantiza la recuperación de los archivos.
- Aislar inmediatamente los dispositivos comprometidos de la red.
- Eliminar el Ransomware con herramientas especializadas (Malwarebytes, ClamAV, Norton, etc.).
- Restaurar desde copias de seguridad limpias si están disponibles.
- Implementar medidas preventivas:
- Bloquear macros en documentos de Office (en estaciones de trabajo).
- Aplicar parches y actualizaciones del sistema operativo y software, tanto en Linux como Windows.
- Deshabilitar accesos remotos innecesarios o protegerlos con doble factor de autenticación (2FA).
- Configurar listas de control de acceso y firewalls para limitar servicios expuestos.
- Educar a los usuarios sobre Phishing y buenas prácticas de ciberhigiene.
- Monitorear indicadores de compromiso en sistemas SIEM, antivirus o EDR.
- Usar soluciones EDR/XDR que incluyan detección avanzada en entornos Linux.

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:

FORTRA (2025). BERT Ransomware: What You Need to Know. https://www.fortra.com/blog/bert-ransomware-what-you-need-know

CYBERSECURITY NEWS (2025). BERT Ransomware Upgrades to Attacks on Linux Machines. https://cybersecuritynews.com/bert-ransomware-upgrades-to-attacks-linux-machines

ENIGMA SECURITY (2025). BERT Ransomware intensifica sus ataques a máquinas Linux. https://enigmasecurity.cl/amenazas-1743/

GBHACKERS (2025). BERT Ransomware Escalates Attacks on Linux Machines. https://gbhackers.com/bert-ransomware-escalates-attacks-on-linux-machines/

THE RAVEN FILE (2025). BERT Ransomwarehttps://theravenfile.com/2025/06/16/bert-ransomware/

BROADCOM. (2025). Bert Ransomware https://www.broadcom.com/support/security-center/protection-bulletin/bert-ransomware

CYFIRMA (2025). Weekly Intelligence Report – 16 May 2025 - Ransomware of the week. https://www.cyfirma.com/news/weekly-intelligence-report-16-may-2025/