Nro. Alerta:	AL-2024-007	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		V 1.1
Fecha:	10-may-2024	LockBit 3.0 Ransomware	Pág.: **1** of **10**

I. DATOS GENERALES:

Clase de alerta: Malware

Tipo de incidente: Ransomware

Nivel de riesgo: Alto

II. ALERTA

El Centro de Respuestas a Incidentes Informáticos de la ARCOTEL recibe de fuentes internaciones información del incremento de ataques de ransomware Lockbit 3.0, en el periodo de 8 al 10 de mayo del 2024.

El ransomware LockBit es un software malicioso diseñado para bloquear el acceso de los usuarios a los sistemas informáticos y pedir el pago de un rescate para restablecerlo. LockBit busca automáticamente objetivos valiosos, propaga la infección y cifra todos los sistemas informáticos accesibles en una red.

Figura 1.- ***CVE-2023-35636*** *– figura referencial*

III. INTRODUCCIÓN

LockBit es una familia de ransomware que ha evolucionado significativamente desde su primera aparición en 2020. Una de sus variantes más conocidas, LockBit 3.0, se distingue frente a sus predecesoras por su sofisticación y capacidad mejorada para evadir las medidas de detección y seguridad.

Esta versión ha introducido métodos de cifrado más robustos, tácticas avanzadas de exfiltración de datos y una estructura de ransomware como servicio (RaaS) más refinada que atrae a un número creciente de afiliados

IV. VECTOR DE ATAQUE:

Sus técnicas para penetrar en los sistemas también evolucionaron y se refinaron con cada versión, abarcando desde el uso de conexiones remotas inseguras, hasta la propagación de correos electrónicos con contenido dañino.

Pero, además, LockBit, a lo largo de su historia, se ha caracterizado por utilizar un arsenal de *exploits* muy nutrido.

Entre los CVE más representativos y vinculados a este malware destacan:

- ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207),
- PaperCut (CVE-2023-27350),
- BlueKeep (CVE-2019-0708),
- Apache Log4j (CVE-2021-44228) y
- Citrix Bleed (CVE-2023-4966).

V. IMPACTO:

Antes de iniciar el proceso de cifrado, LockBit 3.0 ejecuta varias acciones para garantizar su eficacia:

- **Finaliza servicios y procesos específicos**: detecta y finaliza una serie de procesos y servicios relacionados con la seguridad, la copia de seguridad, la gestión de bases de datos y otras aplicaciones que

podrían detener o interferir en el proceso de cifrado. Por ejemplo, interrumpe servicios vinculados a programas antivirus, sistemas de copia de seguridad y bases de datos activas para facilitar el cifrado sin interrupciones de los archivos críticos, utilizando técnicas de evasión de análisis como el API NtTerminateProcess, que finaliza procesos para eludir análisis.

- **Deshabilita y altera servicios de seguridad**: modifica la configuración del sistema para desactivar herramientas de seguridad capaces de detectar su presencia. Un caso notable es el bloqueo del Windows Defender mediante alteraciones en el registro del sistema, o la paralización de servicios relacionados con otros productos de seguridad, con el objetivo de crear un entorno donde el *ransomware* pueda operar sin ser descubierto ni bloqueado por las defensas de seguridad.

- **Elimina las copias de seguridad**: la estrategia de LockBit 3.0 se realiza utilizando la Instrumentación de Administración de Windows (*Windows Management Instrumentation*, WMI) a través de objetos COM. Este método aprovecha las capacidades administrativas de WMI para manipular y eliminar las copias de seguridad del sistema operativo de manera eficiente, dificultando la recuperación de archivos por parte de las víctimas del ataque de *ransomware*.

- **Elimina y altera registros**: tras ejecutar sus operaciones malintencionadas, el *ransomware* se esfuerza por borrar o cambiar registros de eventos del sistema para obstaculizar la investigación forense y el análisis posterior a la infección. También vacía el contenido de la papelera de reciclaje.

- **Cifrado:** LockBit 3.0 implementa un mecanismo para su proceso de desempaquetado y descifrado, utilizando una contraseña específica de RC4 KSA para descifrarse a sí mismo. Esta contraseña inicia la primera etapa del proceso de desempaquetado, que se desarrolla en varias capas, comenzando con cierto código fuente y luego aplicando el algoritmo RC4.

  Finalmente, el proceso identifica y ejecuta funciones de la API de Windows, completando así su preparación para la ejecución del ataque. Adicionalmente, también emplea algoritmos, como AES-256, ChaCha20 y RSA-2048, en sus operaciones de cifrado, ya que ChaCha20 ofrece una alternativa de alto rendimiento para el cifrado especialmente útil en entornos donde el rendimiento de AES puede no ser óptimo y RSA, por otro lado, se utiliza para el cifrado de claves.

VI. INDICADORES DE COMPROMISO

DOMINIOS
lockbit7z2jwcskxpbokpemdxmltipntwlkmidcll2qirbu7ykg46eyd.onion
lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion
lockbitsupa7e3b4pkn4mgkgojrl5iqgx24clbzc4xm7i6jeetsia3qd.onion

lockbitsupdwon76nzykzblcplixwts4n4zoecugz2bxabtapqvmzqqd.onion
lockbitsupn2h6be2cnqpvncyhj4rgmnwn44633hnzzmtxdvjoqlp7yd.onion
lockbitsupo7vv5vcl3jxpsdviopwvasljqcstym6efhh6oze7c6xjad.onion
lockbitsupq3g62dni2f36snrdb4n5qzqvovbtkt5xffw3draxk6gwqd.onion
lockbitsupqfyacidr6upt6nhhyipujvaablubuevxj6xy3frthvr3yd.onion
lockbitsupt7nr3fa6e7xyb73lk6bw6rcneqhoyblniiabj4uwvzapqd.onion
lockbitsupuhswh4izvoucoxsbnotkmgq6durg7kficg6u33zfvq3oyd.onion
lockbitsupxcjntihbmat4rrh7ktowips2qzywh6zer5r3xafhviyhqd.onion
info.openjdklab.xyz
orangebronze.com

SHA1
371353e9564c58ae4722a03205ac84ab34383d8c
c2a321b6078acfab582a195c3eaf3fe05e095ce0
ced1c9fabfe7e187dd809e77c9ca28ea2e165fa8
0815277e12d206c5bbb18fd1ade99bf225ede5db
091b490500b5f827cc8cde41c9a7f68174d11302
10039d5e5ee5710a067c58e76cd8200451e54b55
729eb505c36c08860c4408db7be85d707bdcbf1b
82bd4273fa76f20d51ca514e1070a3369a89313b
a512215a000d1b21f92dbef5d8d57a420197d262
e35a702db47cb11337f523933acd3bce2f60346d
eed31d16d3673199b34b48fb74278df8ec15ae33
ff01473073c5460d1e544f5b17cd25dadf9da513
d826a846cb7d8de539f47691fe2234f0fc6b4fa0

SHA256
a56b41a6023f828cccaaef470874571d169fdb8f683a75edd430fbd31a2c3f6e
d61af007f6c792b8fb6c677143b7d0e2533394e28c50737588e40da475c040ee
f9b9d45339db9164a3861bf61758b7f41e6bcfb5bc93404e296e2918e52ccc10

Nro. Alerta:	AL-2024-007	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		V 1.1
Fecha:	10-may-2024	LockBit 3.0 Ransomware	Pág.: **6** of **10**

IPV4
149.28.137.7
45.32.108.54
139.180.184.147
194.26.29.13

VII. RECOMENDACIONES:

Ante un ataque de ransomware, es fundamental actuar con rapidez y seguir un conjunto de pasos específicos para minimizar el daño y aumentar las posibilidades de recuperación. Algunos pasos a seguir son:

1. **Aislar el Sistema o Red:** Si se detecta actividad de ransomware en una computadora o en la red, aislar inmediatamente el sistema afectado desconectándolo de la red informática. Esto ayudará a evitar que el ransomware se propague a otros sistemas. **Recuerde** no apagar el equipo para no perder información que se almacena temporalmente en la memoria volátil, necesaria para la investigación; la cual se borra cuando se reinicia o apaga el equipo..
2. **Confirmar el Ataque:** Asegurarse de que se trata de un ataque de ransomware. Los ataques de ransomware suelen mostrar una nota de rescate en la pantalla de la víctima. Tomar capturas de pantalla o fotografías de la pantalla para documentar la nota de rescate.
3. **No Pagar el Rescate:** No pagar el rescate exigido por los atacantes. No hay garantía de que se obtendrá la clave de descifrado después de realizar el pago, y pagar solo alienta a los ciberdelincuentes.
4. **Informar del Ataque:** Notificar de inmediato al equipo de seguridad cibernética de la organización o a las autoridades locales. Cuanto antes se informe, mejor será la respuesta y la posibilidad de rastrear a los atacantes.

5. **Restauración desde una Copia de Seguridad:** Si se cuenta con copias de seguridad actualizadas y seguras, utilizar estas copias para restaurar los datos y sistemas afectados. Asegurarse de que las copias de seguridad sean de confianza y no estén comprometidas.
6. **No Borrar Evidencia:** No apagar los equipos afectados, no borrar ningún archivo o evidencia del ataque, hasta que se haya evaluado completamente la situación y se haya informado a las autoridades. La evidencia es necesaria para iniciar la investigación.
7. **Contactar con la autoridad:** De ser víctima, contacte a las Autoridades competentes en base a la Normativa Legal Vigente.
8. **Recopilar Información:** Documentar todos los detalles del ataque, incluyendo la nota de rescate, la dirección de Bitcoin utilizada para el rescate (si está disponible), y cualquier información sobre cómo se propagó el ransomware.
9. **Escanear y Limpiar el Sistema:** Escanear el sistema afectado en busca de malware residual y limpia cualquier instancia del ransomware. Utiliza herramientas de seguridad confiables y actualizadas.
10. **Mejorar la Seguridad:** Identificar las vulnerabilidades o puntos débiles que permitieron que el ransomware infectara el sistema y tomar medidas para mejorar la seguridad, como parchear software, fortalecer contraseñas y educar a los usuarios sobre la seguridad cibernética.
11. **Mejorar el Plan de Respuesta a Incidentes:** Desarrollar y revisar un plan de respuesta a incidentes que incluya los pasos específicos a seguir en caso de futuros ataques de ransomware.
12. **Monitoreo Continuo:** Implementar un monitoreo de seguridad continuo para detectar actividades inusuales en la red y sistemas que podrían indicar un ataque en curso o intentos de infiltración futuros.
13. **Concienciación de Usuarios:** Educar a los usuarios sobre cómo identificar el ransomware y los peligros del phishing, ya que la mayoría de los ataques de ransomware comienzan con correos electrónicos de phishing.

14. **Buscar información sobre el ransomware:** En el caso de que la organización se vea afectada por un ransomware, se puede visitar paginas especializadas en tratamiento de ransomware, a fin de establecer un panorama de la situación, algunas páginas pueden ser:

    - https://www.nomoreransom.org/es/decryptiontools.html#LockFile (herramientas de desencriptado en el caso de existir)
    - https://id-ransomware.malwarehunterteam.com/ (identificación de tipo de Ransomware y herramienta de desencriptado en el caso de existir)

La prevención es la clave para evitar ataques de ransomware. Considera las recomendaciones del Numeral III, de este documento. La respuesta efectiva a un ataque de ransomware es esencial para minimizar el impacto y recuperarse de manera más rápida y efectiva.

Adicional, se recomienda visitar la página web del Ecucert, la sección de "*CONSEJOS"*, en la cual se publica información relacionada con recomendaciones para la seguridad digital.

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:

https://latam.kaspersky.com/resource-center/threats/lockbit-ransomware

https://www.incibe.es/incibe-cert/blog/lockbit-acciones-de-respuesta-y-recuperacion#:~:text=LockBit%20es%20una%20familia%20de,medidas%20de%20detecci%C3%B3n%20y%20seguridad.

https://id-ransomware.malwarehunterteam.com/

https://www.nomoreransom.org/es/decryptiontools.html#LockFile

https://www.ecucert.gob.ec/consejos/#

https://www.ecucert.gob.ec/alertas/