Nro. Alerta:	AL-2024-035	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	15-dic -2024	**RansomHub Ransomware**	Pág.: **1** of **14**

I. DATOS GENERALES:

Clase de alerta: Incidente
Tipo de incidente: Ransonware
Nivel de riesgo: Alto

II. INTRODUCCIÓN

Desde su creación, RansomHub ha cifrado y exfiltrado datos de al menos 210 víctimas que representan a los sectores de agua y aguas residuales, tecnología de la información, servicios e instalaciones gubernamentales, servicios de emergencia, alimentación y agricultura, servicios financieros, instalaciones comerciales, transporte y comunicaciones, fabricación crítica y atención médica y salud pública.

El software de RansomHub combina algunas características de cepas de ransomware más antiguas, como la capacidad de Knight para apagar las funciones de seguridad de un dispositivo resetear en modo seguro justo antes del cifrado. También comparte un lenguaje de programación con Snatch, pero con algunas diferencias como comandos configurables y una ofuscación de código más pesada. Al igual que sus predecesores; RansomHub, se basa en la doble extorsión, en la que un afiliado (hacker que compra el ransonware o malware para su propio ataque) obtiene acceso inicial, roba la mayor cantidad posible de datos confidenciales y luego desata una carga útil de ransomware en su salida. La víctima tiene que lidiar con la doble pesadilla de no solo descodificar sus sistemas para devolver el acceso de empleados y clientes, sino también el dilema moral de pagar a los delincuentes para que impidan que se publiquen datos confidenciales.

RansomHub es un RaaS, al que se sienten atraídos de participar como aliados por el enfoque singular en las ganancias financieras..

III. VECTOR DE ATAQUE

Los afiliados de RansomHub suelen comprometer los sistemas conectados a Internet y los usuarios finales mediante métodos de Pishing [T1566], explotación de vulnerabilidades conocidas [T1190] y difusión de contraseñas [T1110.003]. La difusión de contraseñas se dirige a las cuentas comprometidas a través de violaciones de datos. Los exploits de prueba de concepto se obtienen de fuentes como ExploitDB y GitHub [T1588.005]. Se han observado exploits basados en los siguientes CVE:

- CVE-2023-3519 (CWE-94)
- CVE-2023-27997 (CWE-787 | CWE-122)
- CVE-2023-46604 (CWE-502)
- CVE-2023-22515

- CVE-2023-46747 (CWE-306 | CWE-288)
- CVE-2023-48788 (CWE-89)
- CVE-2017-0144
- CVE-2020-1472
- CVE-2020-0787

En la fase de descubrimiento de RansomHub realizan escaneos de red con herramientas como AngryIPScanner, Nmap y métodos basados en PowerShell que aprovechan recursos propios del sistema para realizar el escaneo de redes [T1018][T1046][T1059.001].

Los investigadores de ciberseguridad han observado que como evasión de defensa renombran el ejecutable del ransomware con nombres de archivo inofensivos, como Windows.exe, que se dejan en el escritorio del usuario (C:\Users\%USERNAME%\Desktop) o en las descargas (C:\Users\%USERNAME%\Downloads) [T1036]. También han borrado los registros del sistema de Windows y Linux para inhibir cualquier posible respuesta a incidentes [T1070]. Utilizaron el Instrumental de administración de Windows [T1047] para desactivar los productos antivirus. En algunos casos, se implementaron herramientas específicas de RansomHub para desactivar las herramientas de detección y respuesta de endpoints (EDR) [T1562.001]

Posteriormente, RansomHub crea cuentas de usuario para persistencia [T1136], reactivaron cuentas deshabilitadas [T1098] y utilizaron Mimikatz [S0002] en sistemas Windows para recopilar credenciales [T1003] y escalar privilegios a SYSTEM [T1068]. Luego, se movieron lateralmente dentro de la red a través de métodos que incluyen el Protocolo de escritorio remoto (RDP) [T1021.001], PsExec [S0029], Anydesk [T1219], Connectwise, N-Able, Cobalt Strike [S0154], Metasploit u otros métodos de comando y control (C2) ampliamente utilizados.

Los métodos de exfiltración de datos dependen en gran medida de cómo se lleva a cabo la vulneración de la red. El binario del ransomware normalmente no incluye ningún mecanismo para la exfiltración de datos. La exfiltración de datos se ha observado mediante el uso de herramientas como PuTTY [T1048.002], buckets/herramientas de Amazon AWS S3 [T1537], solicitudes HTTP POST [T1048.003], WinSCP, Rclone, Cobalt Strike, Metasploit y otros métodos.

IV. IMPACTO

El ransomware RansomHub ha aprovechado un algoritmo de cifrado de curva elíptica llamado -Curve 25519- para cifrar los archivos a los que el usuario puede acceder en el

sistema [T1486]. Curve 25519 utiliza una clave pública/privada que es única para cada organización víctima. Para cifrar correctamente los archivos que se encuentran en uso, el binario del ransomware normalmente intentará detener los siguientes procesos:

- Vmms.exe
- Msaccess.exe
- Mspub.exe
- Svchost.exe
- Vmcompute.exe
- Notepad.exe
- Ocautoupds.exe
- Ocomm.exe
- Ocssd.exe
- Oracle.exe
- Onenote.exe
- Outlook.exe
- Powerpnt.exe
- Explorer.exe
- Sql.exe
- Steam.exe
- Synctime.exe
- Vmwp.exe
- Thebat.exe
- Thunderbird.exe
- Visio.exe
- Winword.exe
- Wordpad.exe
- Xfssvccon.exe
  TeamViewer.exe
- Agntsvc.exe
- Dbsnmp.exe
- Dbeng50.exe
- Encsvc.exe

El binario del ransomware intentará cifrar todos los archivos a los que el usuario tenga acceso, incluidos los archivos de usuario y los recursos compartidos en red.

RansomHub implementa un cifrado intermitente, cifrando los archivos en fragmentos de 0x100000 bytes y omitiendo cada 0x200000 bytes de datos entre los fragmentos cifrados. Los archivos con un tamaño inferior a 0x100000 bytes se cifran por completo. A los

archivos se les añaden 58 bytes (0x3A) de datos al final. Estos datos contienen un valor que probablemente forme parte de una clave de cifrado/descifrado. La estructura de los bytes 0x3A adjuntos se muestra a continuación con imágenes de tres archivos cifrados diferentes.

Figura 1: Los primeros ocho bytes tienen el tamaño del archivo cifrado

Los siguientes 8 bytes son el tamaño de los bloques cifrados. Si todo el archivo está cifrado, esta sección está formada únicamente por ceros. En este ejemplo, cada sección cifrada tiene una longitud de 0x100000 bytes, con 0x100000 bytes entre cada bloque cifrado. Se observó que este número cambiaba en función del tamaño del archivo cifrado.

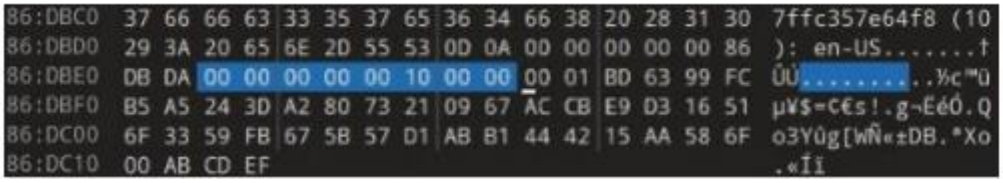

Figura 2: El tamaño de los bloques cifrados.

Los siguientes dos bytes siempre se consideraron 0x0001

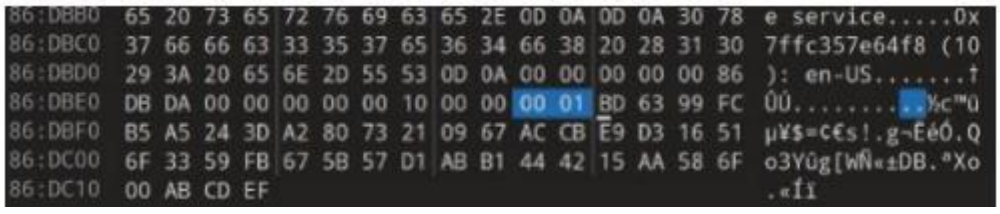

Figura 3: Los siguientes dos bytes son siempre 0x0001.

Los siguientes 32 bytes son la clave de cifrado pública del archivo.

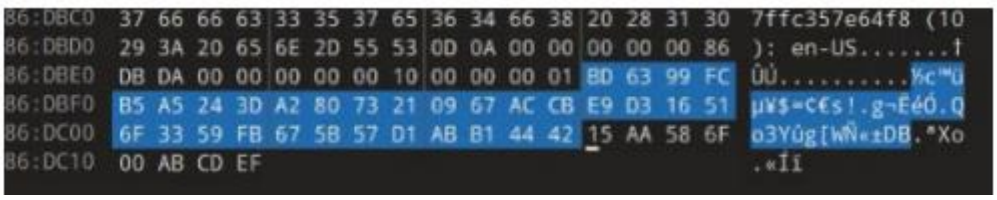

Figura 4: Clave de cifrado pública para el archivo.

Los siguientes 4 bytes son un valor de suma de comprobación.

Figura 5: Valor de la suma de comprobación.

Los últimos 4 bytes siempre se consideran la secuencia 0x00ABCDEF.

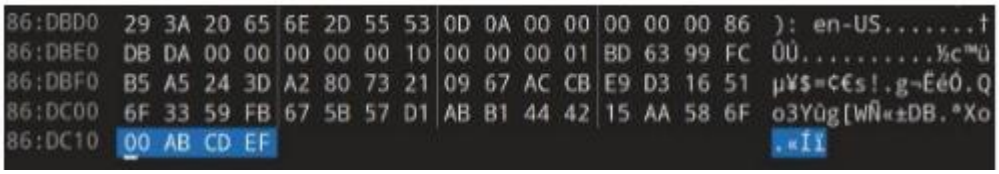

Figura 6: Los últimos cuatro bytes.

El ejecutable del ransomware no suele cifrar los archivos ejecutables. Se añade una extensión de archivo aleatoria a los nombres de archivo y se deja una nota de rescate generalmente titulada “How To Restore Your Files.txt” en el Sistema Operativo afectado. Para inhibir aún más la recuperación del sistema, el ejecutable del ransomware normalmente aprovecha el programa vssadmin.exe para eliminar las instantáneas de volumen [T1490].

V. INDICADORES DE COMPROMISO

Descargo de responsabilidad: Se recomienda investigar o verificar estos indicadores antes de tomar medidas, como bloquearlos.

Archivo	Descripción
C:\Users\%USERNAME%\AppData\Local\Programs\Python\Python311\Scripts\crackmapex ec.exe	CrackMapExec
C:\Users\%USERNAME%\AppData\Local\Programs\Python\Python311\Scripts\kerbrute.exe	Kerberoasti g
C:\Users\%USERNAME%\Downloads\Anydesk.exe	Anydesk C2
C:\Users\%USERNAME%\Desktop\IamBatMan.exe	Ransomware
C:\Users\backupexec\Desktop\stealer_cli_v2.exe	Info Stealer
C:\Users\%USERNAME%\Downloads\nmap-7.94-setup.exe	Nmap
C:\Program Files (x86)\Nmap\nmap.exe	Nmap
C:\Users\%USERNAME%\Downloads\mimikatz_trunk\x64\mimikatz.exe	Mimikatz

Archivo	Descripción
C:\Users\backupexec\Downloads\x64\mimikatz.exe	Mimikatz
C:\Users\%USERNAME%\AppData\Local\Programs\Python\Python311\Scripts\crackmapex ec.exe	CrackMapExec

Las organizaciones autoras recomiendan que los defensores de la red investiguen o examinen las direcciones IP antes de tomar medidas, como bloquearlas. Se sabe que muchos cibeatacantes que cambian las direcciones IP, a veces a diario, y algunas direcciones IP pueden albergar dominios válidos.

Direcciones IP
8.211.2[.]97
45.95.67[.]41
45.134.140[.]69
45.135.232[.]2
89.23.96[.]203
188.34.188[.]7
193.106.175[.]107
193.124.125[.]78
193.233.254[.]21

URL conocidas relacionadas con actividades maliciosas (2023-2024)

Solicitudes Web
http[:]//188.34.188[.]7/555
http[:]//188.34.188[.]7/555/
http[:]//188.34.188[.]7/555/amba16.ico
http[:]//188.34.188[.]7/555/bcrypt.dll
http[:]//188.34.188[.]7/555/CRYPTSP.dll
http[:]//188.34.188[.]7/555/en
http[:]//188.34.188[.]7/555/en-US
http[:]//188.34.188[.]7/555/NEWOFFICIALPROGRAMCAUSEOFNEWUPDATE.exe
http[:]//188.34.188[.]7/555/NEWOFFICIALPROGRAMCAUSEOFNEWUPDATE.exe.Config
http[:]//188.34.188[.]7/555/NEWOFFICIALPROGRAMCAUSEOFNEWUPDATE.INI
http[:]//89.23.96[.]203/

Solicitudes Web
http[:]//89.23.96[.]203/333
http[:]//89.23.96[.]203/333/
http[:]//89.23.96[.]203/333/1.exe
http[:]//89.23.96[.]203/333/1.exe.Config
http[:]//89.23.96[.]203/333/10.exe
http[:]//89.23.96[.]203/333/12.exe
http[:]//89.23.96[.]203/333/12.exe.Config
http[:]//89.23.96[.]203/333/2.exe
http[:]//89.23.96[.]203/333/2.exe.Config
http[:]//89.23.96[.]203/333/2wrRR6sW6XJtsXyPzuhWhDG7qwN4es.exe
http[:]//89.23.96[.]203/333/2wrRR6sW6XJtsXyPzuhWhDG7qwN4es.exe.Config
http[:]//89.23.96[.]203/333/3.exe
http[:]//89.23.96[.]203/333/3.exe.Config
http[:]//89.23.96[.]203/333/4.exe
http[:]//89.23.96[.]203/333/4.exe.Config
http[:]//89.23.96[.]203/333/5.exe
http[:]//89.23.96[.]203/333/5.exe.Config
http[:]//89.23.96[.]203/333/6.exe
http[:]//89.23.96[.]203/333/7.exe
http[:]//89.23.96[.]203/333/8.exe
http[:]//89.23.96[.]203/333/9.exe
http[:]//89.23.96[.]203/333/92.exe
http[:]//89.23.96[.]203/333/AmbaPDF.ico
http[:]//89.23.96[.]203/333/ambapdf.ico.DLL
http[:]//89.23.96[.]203/333/bcrypt.dll

Solicitudes Web
http[:]//89.23.96[.]203/333/Cabinet.dll
http[:]//89.23.96[.]203/333/CRYPTBASE.DLL
http[:]//89.23.96[.]203/333/cryptnet.dll
http[:]//89.23.96[.]203/333/CRYPTSP.dll
http[:]//89.23.96[.]203/333/cv4TCGxUjvS.exe
http[:]//89.23.96[.]203/333/DPAPI.DLL
http[:]//89.23.96[.]203/333/en
http[:]//89.23.96[.]203/333/en/d%E5%AD%97%E5%AD%97.resources.dll
http[:]//89.23.96[.]203/333/en/d%E5%AD%97%E5%AD%97.resources.exe
http[:]//89.23.96[.]203/333/en/d%E5%AD%97%E5%AD%97.resources/d%E5%AD%97%E5%AD%97.resources.dll
http[:]//89.23.96[.]203/333/en/d%E5%AD%97%E5%AD%97.resources/d%E5%AD%97%E5%AD%97.resources.exe
http[:]//89.23.96[.]203/333/en-US
http[:]//89.23.96[.]203/333/en-US/d%E5%AD%97%E5%AD%97.resources.dll
http[:]//89.23.96[.]203/333/en-US/d%E5%AD%97%E5%AD%97.resources.exe
http[:]//89.23.96[.]203/333/en-US/d%E5%AD%97%E5%AD%97.resources/d%E5%AD%97%E5%AD%97.resources.dll
http[:]//89.23.96[.]203/333/en-US/d%E5%AD%97%E5%AD%97.resources/d%E5%AD%97%E5%AD%97.resources.exe
http[:]//89.23.96[.]203/333/iertutil.dll
http[:]//89.23.96[.]203/333/information.exe
http[:]//89.23.96[.]203/333/information.exe.Config
http[:]//89.23.96[.]203/333/information.INI
http[:]//89.23.96[.]203/333/IPHLPAPI.DLL

Solicitudes Web
http[:]//89.23.96[.]203/333/mshtml.dll
http[:]//89.23.96[.]203/333/msi.dll
http[:]//89.23.96[.]203/333/SspiCli.dll
http[:]//89.23.96[.]203/333/TmsLA6kdcU8jxKzpMvbUVweTeF5YcR.exe
http[:]//89.23.96[.]203/333/TmsLA6kdcU8jxKzpMvbUVweTeF5YcR.exe.Config
http[:]//89.23.96[.]203/333/2wrRR6sW6XJtsXyPzuhWhDG7qwN4es.exe
http[:]//89.23.96[.]203/333/xwenxub285p83ecrzvft.exe
http[:]//89.23.96[.]203/333/cv4TCGxUjvS.exe
http[:]//89.23.96[.]203/333/urlmon.dll
http[:]//89.23.96[.]203/333/USERENV.dll
http[:]//89.23.96[.]203/333/webio.dll
http[:]//89.23.96[.]203/333/winhttp.dll
http[:]//89.23.96[.]203/333/WININET.dll
http[:]//89.23.96[.]203/333/WINMM.dll
http[:]//89.23.96[.]203/333/WINMMBASE.dll
http[:]//89.23.96[.]203/333/winnlsres.dll
http[:]//89.23.96[.]203/333/xwenxub285p83ecrzvft.exe
http[:]//89.23.96[.]203/333/xwenxub285p83ecrzvft.exe.Config
http[:]//temp.sh/KnCqD/superloop.exe
https[:]//grabify.link/Y33YXP
https[:]//i.ibb.co/2KBydfw/112882618.png
https[:]//i.ibb.co/4g6jH2J/2773036704.png
https[:]//i.ibb.co/b1bZBpg/2615174623.png
https[:]//i.ibb.co/Fxhyq6t/2077411869.png
https[:]//i.ibb.co/HK0jV1G/534475006.png

Solicitudes Web
https[:]//i.ibb.co/nbMNnW4/2501108160.png
https[:]//i.ibb.co/p1RCtpy/2681232755.png
https[:]//i.ibb.co/SxQLwYm/1038436121.png
https[:]//i.ibb.co/v1bn9ZK/369210627.png
https[:]//i.ibb.co/V3Kj1c2/1154761258.png
https[:]//i.ibb.co/X2FR8Kz/2113791011.png
https[:]//i.ibb.com:443/V3Kj1c2/1154761258.png
https[:]//12301230[.]co/npm/module.tripadvisor/module.tripadvisor.css
https[:]//12301230[.]co/npm/module.external/jquery.min.js
https[:]//12301230[.]co/npm/module.external/moment.min.js
https[:]//12301230[.]co/npm/module.external/client.min.js
https[:]//12301230[.]co/npm/module.tripadvisor/module.tripadvisor.js
https[:]//samuelelena[.]co/npm/module.tripadvisor/module.tripadvisor.js
https[:]//samuelelena[.]co/npm/module.external/jquery.min.js
https[:]//samuelelena[.]co/npm/module.external/moment.min.js
https[:]//samuelelena[.]co/npm/module.external/client.min.js
https[:]//samuelelena[.]co/
http[:]//samuelelena[.]co/
https[:]//samuelelena[.]co/npm
https[:]//samuelelena[.]co/npm/module.tripadvisor/module.tripadvisor.js
http[:]//samuelelena[.]co/npm/
http[:]//samuelelena[.]co/npm/module.tripadvisor/module.tripadvisor.js
http[:]//samuelelena[.]co/npm/module.external/client.min.js
https[:]//samuelelena[.]co/npm/module.tripadvisor/module.tripadvisor.
https[:]//samuelelena[.]co/npm/module.external/jquery.min.js

Solicitudes Web
https[:]//samuelelena[.]co/npm/module.external
https[:]//samuelelena[.]co/np
https[:]/samuelelena[.]co/npm/module.tripadvisor/module.tripadvisor.js
https[:]//samuelelena[.]co/npm/module[.]tripadvisor/module[.]tripadvisor[.]js
https[:]//samuelelena[.]co/npm/module[.]external/client.min.js
https[:]//samuelelena[.]co/npm/module.external/jquery.min.js
http[:]//samuelelena[.]co:443/
http[:]//samuelelena[.]co/npm/module.external/jquery.min.js
https[:]//40031[.]co/npm/module.tripadvisor/module.tripadvisor.css
https[:]//40031[.]co/npm/module.external/jquery.min.js
https[:]//40031[.]co/npm/module.external/moment.min.js
https[:]//40031[.]co/npm/module.external/client.min.js
https[:]//40031[.]co/npm/module.tripadvisor/module.tripadvisor.js

Correos electrónicos relacionados con RansomHub

Direcciones de correo electrónico - Email
brahma2023[@]onionmail.org
<victim_organization_name>[@]protonmail.com

VI. 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:

- Implementar un plan de recuperación de datos para mantener, conservar múltiples copias de los datos y servidores confidenciales o de propiedad exclusiva en una ubicación físicamente aislada, segmentada y segura (ya sea en disco duro, dispositivo de almacenamiento, la nube).

- Exigir que todas las cuentas de inicio de sesión con contraseña, por ejemplo, cuentas de servicio, cuentas de administrador y cuentas de administrador de dominio) cumplan con estándares y se mantenga una gestión de políticas de contraseñas:

  1. Utilice contraseñas más largas que consten de al menos 8 caracteres y no más de 64 caracteres de longitud
  2. Almacene las contraseñas en formato hash utilizando administradores de contraseñas reconocidos.
  3. Agregue “salt” a las contraseñas de usuario de contraseña a las credenciales de inicio de sesión compartidas.
  4. No reutilicé contraseñas.
  5. Implemente bloqueos de cuenta en caso de múltiples intentos fallidos de inicio de sesión.
  6. Desactive “hints” de contraseña.
  7. Absténgase de solicitar cambios de contraseña con una frecuencia mayor a una vez al año.

- Mantener los sistemas operativos, software y firmware actualizados. La aplicación oportuna de parches o actualizaciones de seguridad es una de las medidas más eficientes y rentables de la organización para minimizar su exposición a amenazas de ciberseguridad. Priorice la aplicación de parches a las vulnerabilidades explotadas conocidas en los sistemas conectados a Internet.

- Exigir autenticación multifactor para todos los servicios en la medida de lo posible, en particular para correo web, redes privadas virtuales y cuentas que acceden a sistemas críticos.
- Segmentar las redes de datos para evitar la propagación de ransomware. La segmentación de redes puede ayudar a prevenir la propagación de ransomware al controlar los flujos de tráfico entre varias subredes y el acceso a ellas y al restringir el movimiento lateral del adversario.

- Identifique, detecte e investigue la actividad anormal y el posible tránsito del ransomware indicado con una herramienta de monitoreo de redes.

- Para ayudar a detectar el ransomware, implemente una herramienta que registre e informe todo el tráfico de red, incluida la actividad de movimiento lateral en una red. Las herramientas de detección y respuesta de endpoints

(EDR) son particularmente útiles para detectar conexiones laterales, ya que tienen información sobre las conexiones de redes comunes y no comunes para cada host.

- Instalar, actualizar periódicamente y habilitar la detección en tiempo real del software antivirus en todos los hosts.
- Implemente prácticas seguras de recopilación y almacenamiento de registros.
- Revise los controladores de dominio, servidores, estaciones de trabajo y directorios activos en busca de cuentas nuevas o no reconocidas.
- Auditar cuentas de usuario con privilegios administrativos y configurar controles de acceso de acuerdo con el principio de mínimo privilegio.
- Deshabilitar los puertos no utilizados.
- Implementar y aplicar políticas de seguridad de correo electrónico.
- Deshabilitar macros de forma predeterminada.
- Considere agregar un banner de correo electrónico a los correos electrónicos recibidos desde fuera de su organización.
- Deshabilitar hipervínculos en los correos electrónicos recibidos.
- Implemente el acceso basado en el tiempo para las cuentas configuradas en el nivel de administrador y superior. Por ejemplo, el método de acceso Just-inTime (JIT) proporciona acceso privilegiado cuando es necesario y puede respaldar la aplicación del principio de privilegio mínimo (así como el modelo Zero Trust). Este es un proceso en el que se establece una política para toda la red para deshabilitar automáticamente las cuentas de administrador en el nivel de Active Directory cuando la cuenta no tiene una necesidad directa. Los usuarios individuales pueden enviar sus solicitudes a través de un proceso automatizado que les otorga acceso a un sistema específico durante un período de tiempo determinado cuando necesitan respaldar la finalización de una determinada tarea.
- Desactive las actividades y permisos de línea de comandos y secuencias de comandos. La escalada de privilegios y el movimiento lateral a menudo dependen de utilidades de software que se ejecutan desde la línea de

comandos. Si los actores de amenazas no pueden ejecutar estas herramientas, tendrán dificultades para escalar privilegios y/o moverse lateralmente.

- Mantener copias de seguridad de los datos sin conexión y realizar copias de seguridad y restauraciones de forma regular. Al implementar esta práctica, la organización ayuda a garantizar que no se verán gravemente interrumpidas y/o que solo tendrán datos irrecuperables.

- Garantizar que todos los datos de copia de seguridad estén cifrados, sean inmutables (es decir, no se puedan alterar ni eliminar) y cubran toda la infraestructura de datos de la organización.

- Generar un informe y mantener la cadena de custodia de la evidencia digital a fin de denunciar a las autoridades correspondientes.

VII. DESCARGO 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.

VIII. REFERENCIAS

Cisa (2024) *#StopRansomware: RansomHub Ransomware*
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a

Check Point *What is RansomHub Ransomware?*
https://www.checkpoint.com/es/cyber-hub/threat-prevention/ransomware/what-is-ransomhub-ransomware/

IBM (2024) *¿Qué es el ransomware como servicio (RaaS)?*
https://www.ibm.com/mx-es/topics/ransomware-as-a-service

CVE MITRE
https://cve.mitre.org