Nro. Alerta:	AL-2025-036	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	23-Jul-2025	Interlock Ransomware	Pág.: **1** of **13**

I. DATOS GENERALES:

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

II. ALERTA

Figura 1.- Interlock Ransomware - figura referencial

Los atacantes han adoptado la nueva técnica llamada “FileFix” en los ataques de Interlock Ransomware para lanzar un troyano de acceso remoto (RAT) en sistemas dirigidos.

III. INTRODUCCIÓN

Interlock Ransomware emplea el modelo de doble extorsión, cifran los archivos a una extensión .interlock o .1nt3rlock y exfiltran datos de sus víctimas hacia su DLS (Sitio de Filtración de Datos) en la Dark Web. A diferencia de otros Ransomware la nota de rescate de Interlock !README!.txt no incluye instrucciones de pago, sino que reciben un código único e instrucciones para contactar a los atacantes a través de una url .onion.

Un informe reciente de The DFIR Report, arrojan una nueva versión de RAT de Interlock Ransomware escrita en PHP. La campaña comienza con sitios web comprometidos, inyectados con un script escondido en el HTML de una página del cual propietarios y visitantes desconocen.

Cuando el sitio web infectado es visitado por un usuario, se levanta un CAPTCHA falso de "Verify you are human", seguido de pasos de verificación, después de hacer clic en el mensaje emergente, el usuario es engañado y se lo instruye para que copie y pegue un comando en Windows Run (Ejecutar de Windows) que descarga y ejecuta el Malware.

Este comando ejecuta un script de PowerShell que descarga e instala silenciosamente el RAT basado en PHP. Este nuevo método de infección, denominado "FileFix", disfraza el comando como una ruta de archivo en el Explorador de Windows, evitando las señales visuales habituales que alertarían sobre la actividad sospechosa.

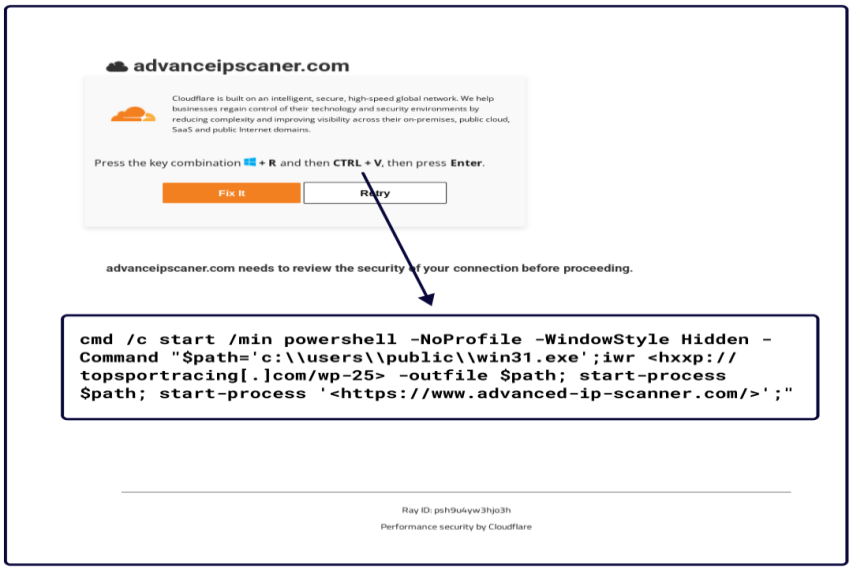

Figura 2. Ataque de FileFix - Interlock Ransomware

IV. VECTOR DE ATAQUE

Se detalla el proceso de infección de Interlock Ransomware:

Acceso Inicial

El FBI ha observado a actores Interlock Ransomware obteniendo acceso inicial [TA0001] vía drive-by download (Descarga Involuntaria) [T1189] de sitios web legítimos comprometidos.

Los métodos de Interlock Ransomware para el acceso inicial han disimulado previamente payloads maliciosos como: actualizaciones falsas de Google Chrome o el navegador Microsoft Edge y recientemente una compañía de ciberseguridad informó

un cambio a los nombres de archivos de payloads disfrazados de actualizaciones, como actualizaciones para software de seguridad.

Interlock Ransomware usa la técnica de ingeniería social ClickFix, en la que se incita a los usuarios desprevenidos a ejecutar un payload malicioso haciendo clic en un falso CAPTCHA [T1189] y este CAPTCHA contiene instrucciones para que los usuarios abran la ventana de Windows Run, peguen el contenido del portapapeles y luego ejecuten un proceso de PowerShell malicioso de Base64 [T1204.004]

Ejecución y persistencia

Basado en investigaciones del FBI, el falso navegador de Google Chrome ejecuta funciones como un troyano de acceso remoto (RAT) [T1105], diseñado para ejecutar un script de PowerShell [T1059.001] que deja caer un archivo en la carpeta de Windows Startup. A partir de ahí, el archivo está diseñado para ejecutar el RAT cada vez que la víctima inicia sesión [T1547.001], estableciendo la persistencia [TA0003].

El FBI también observó casos en los que los actores Interlock Ransomware ejecutaron un comando PowerShell diseñado para establecer la persistencia a través de una modificación de la clave del Registro de Windows [T1547.001]. Con ello, los actores de Interlock Ransomware utilizaron comandos de PowerShell [T1059.001] diseñado para añadir un valor de clave de ejecución llamado "Chrome Updater" [T1036.005] que utiliza un archivo de registro específico como argumento en el inicio de sesión del usuario.

Reconocimiento

Para facilitar el reconocimiento, un script de PowerShell ejecuta una serie de comandos [T1059.001] diseñado para reunir información sobre las máquinas víctimas, se detalla a continuación:

Comando Powershell	Descripción
WindowsIdentity.GetCurrent()	Devuelve un objeto de WindowsIdentity que representa al usuario actual de Windows [T1033]
systeminfo	Muestra información de configuración detallada [T1082] sobre una computadora y su sistema operativo, incluyendo la configuración del sistema operativo, información de seguridad, ID de producto y propiedades de hardware.
tasklist/svc	Lista información de servicio no abreviada (unabridge) [T1007] para cada proceso actualmente en ejecución en el equipo local.
Get-Service	Obtiene objetos que representan los servicios [T1007] en una computadora, incluyendo servicios de ejecución y parada.

Comando Powershell	Descripción
Get-PSDrive	Consigue las unidades [T1082] en el actual período de sesiones, como: ▪ Unidades lógicas de Windows en el equipo, incluyendo unidades asignadas a recursos compartidos de red. ▪ Unidades expuestas por proveedores de PowerShell. ▪ Unidades temporales sesión específicas y unidades de red persistentes.
arp -a	Muestra y modifica las entradas en la tabla de caché del Protocolo de Resolución de Direcciones (ARP) [T1016], que contiene registros de direcciones IPv4 e IPv6 en los puntos finales del host

Tabla 1. Comandos de Powershell empleados - Interlock Ransomware

Comando y control (C2)

El FBI observó a actores interconectados usando comando y control (C2) [TA0011] aplicaciones como Cobalt Strike y SystemBC. Los actores de Interlock Ransomware también utilizaron Interlock RAT5 y NodeSnake RAT (a marzo de 2025) para C2 y ejecución de comandos.

Credenciales de Acceso, Movimiento Lateral y Escalada de Privilegios

El FBI observó que, una vez que los actores de Interlock Ransomware establecen control remoto de un sistema comprometido, usan una serie de comandos de PowerShell para descargar Stealers (o "ladrones de información", son un tipo de malware diseñado para robar datos sensibles de sistemas o cuentas infectadas) como cht.exe que usado de manera maliciosa se usa para el robo de datos y ejecuciones remota [TA0006] y binario de keylogger (klg.dll) [T1056.001],[T1105].

Según la información de código abierto, el administrador de credenciales recopila información de inicio de sesión y URLs asociadas para las cuentas en línea de las víctimas [T1555.003], mientras el keylogger de la biblioteca de enlaces dinámico (DLL) registra pulsaciones de teclas de los usuarios en un archivo nombrado conhost.txt [T1036.005]. A partir de febrero de 2025, los analistas privados de ciberseguridad también observaron infecciones de Interlock Ransomware ejecutando diferentes versiones de Stealers [TA0006], incluyendo *Lumma Stealer* y *Berserk Stealer*, para cosechar credenciales para movimiento lateral y escalamiento de privilegios [T1078].

Los actores Interlock Ransomware aprovechan credenciales comprometidas y el Protocolo de escritorio remoto (RDP) [T1021.001] para moverse entre sistemas. También utilizan herramientas como AnyDesk para permitir la conexión remota y PuTTY para ayudar con el movimiento lateral [T1219]. Además de robar credenciales en línea de los usuarios, los actores de Interlock Ransomware han comprometido

cuentas de administradores de dominios (posiblemente mediante el uso de un ataque de Kerberoasting [T1558.003] para obtener privilegios adicionales [T1078.002].

Colección y exfiltración

Los actores de Interlock Ransomware aprovechan Azure Storage Explorer (StorageExplorer.exe) para navegar por las víctimas [T1530] antes de exfiltrar los datos. Según los informes de código abierto, los actores de Interlock Ransomware ejecutan AzCopy para exfiltrar los datos subiéndolos Azure Storage Blob (servicio de almacenamiento en la nube de Microsoft Azure) [T1567.002]. Los actores entrelazados también exfiltran datos sobre las herramientas de transferencia de archivos, incluyendo WinSCP [T1048].

En resumen, se muestra la TABLA MITRE ATT&CK's

Acceso Inicial

Técnica	ID	USO
Drive-By Compromise (Compromiso por Navegación)	T1189	Los actores de Interlock Ransomware obtienen acceso inicial comprometiendo un sitio web legítimo que los usuarios de la red visitan o disfrazando payloads maliciosos como actualizaciones falsas del navegador o software de seguridad común, incluyendo lo siguiente: ▪ FortiClient.exe ▪ Ivanti-Secure-Access-Client.exe ▪ GlobalProtect.exe ▪ Webex.exe ▪ AnyConnectVPN.exe ▪ Cisco-Secure-Client.exe ▪ zyzoom_antimalware.exe Los actores de Interlock Ransomware también obtienen acceso a través de la técnica de ingeniería social **ClickFix**, en la que se engaña a los usuarios para que ejecuten una payloads maliciosos al hacer clic en un CAPTCHA falso que solicita a los usuarios que ejecuten un script de PowerShell malicioso.

Tabla 2. Acceso inicial - MITRE ATT&CK's

Ejecución

Técnica	ID	USO
Intérprete de comandos y scripts: PowerShell	T1059.001	Los actores de Interlock Ransomware: ▪ Implementan scripts de PowerShell para soltar un archivo malicioso en la carpeta de Windows Startup. ▪ Ejecutan un comando PowerShell para la modificación de la clave del registro. ▪ Utilizan un guión de PowerShell para ejecutar una serie de comandos para facilitar el reconocimiento.

Técnica	ID	USO
Ejecución de usuario: Copia y pega maliciosa	T1204.004	Mediante la técnica de ingeniería social **ClickFix**, se engaña a los usuarios para que hagan clic en un CAPTCHA falso y se les induce a ejecutar un proceso malicioso codificado en Base64 con PowerShell. Para ello, se les dan instrucciones para abrir la ventana 'Ejecutar' de Windows (tecla Windows + R), pegar el contenido del portapapeles ('CTRL + V') y luego ejecutar el script malicioso ('Enter').

Tabla 3. Ejecución - MITRE ATT&CK's

Persistencia

Técnica	ID	USO
Ejecución automática al arranque o inicio de sesión: Claves de registro 'Run' y carpeta de inicio (Startup Folder)	T1547.001	Los actores de Interlock Ransomware establecen persistencia al agregar un archivo en la carpeta de Inicio (StartUp) de Windows, el cual ejecuta un RAT (Remote Access Trojan) cada vez que un usuario inicia sesión. Además, modifican claves del Registro mediante un comando de PowerShell para agregar un valor en las claves de ejecución automática (llamado 'Chrome Updater'), que utiliza un archivo de registro (*log*) como argumento cada vez que un usuario inicia sesión.

Tabla 4. Persistencia - MITRE ATT&CK's

Escalamiento de privilegios

Técnica	ID	USO
Cuentas válidas: Cuentas de dominio	T1078.002	Comprometen cuentas de administradores de dominio para obtener privilegios adicionales.

Tabla 5. Escalamiento de privilegios - MITRE ATT&CK's

Escalada de Defensa

Técnica	ID	USO
Evasión de defensa	TA0005	Ejecutan la función ***removeme*** en sistemas Linux para eliminar el binario de cifrado, evadiendo así las defensas.
Enmascaramiento: Coincidir con nombres o ubicaciones de recursos legítimos	T1036.005	Los actores de Interlock Ransomware: Ocultan un valor malicioso en las claves de ejecución automática (run key) nombrándolo "Chrome Updater"; este valor utiliza un archivo de registro específico como argumento cuando el usuario inicia sesión. Ocultan archivos que registran pulsaciones de teclas capturadas por uno de sus stealers de credenciales, usando un nombre legítimo de Windows: **conhost.txt.** Disfrazan un binario de cifrado (un ejecutable de 64 bits) dándole el mismo nombre que el ejecutable legítimo del "Console Windows Host": **conhost.exe.**

Técnica	ID	USO
Ejecución por proxy de binarios del sistema: Rundll32	T1218.011	Utilizan **rundll32.exe** para ejecutar de forma proxy un binario DLL malicioso llamado **tmp41.wasd**
Eliminación de indicadores: Borrado de archivos	T1070.004	Ejecutan un binario DLL (**tmp41.wasd**) que utiliza la función **remove()** para eliminar su propio binario de cifrado, con el fin de evadir defensas.

Tabla 6. Escalada de defensa - MITRE ATT&CK's

Credenciales de Acceso

Técnica	ID	USO
Acceso a credenciales	TA0006	Los actores de Interlock Ransomware descargan el ladrón de credenciales **cht.exe** y ejecutan otras versiones de robadores de información (incluyendo **Lumma Stealer** y **Berserk Stealer**) para recolectar credenciales.
Credenciales de almacenes de contraseñas: Credenciales de navegadores web	T1555.003	Descargan un **stealer de credenciales** que recopila información de inicio de sesión (usuarios/contraseñas) junto con las **URLs asociadas** a las cuentas en línea de las víctimas.
Captura de entrada	T1056	Ejecutan los robadores de información **Lumma Stealer** y **Berserk Stealer** en sistemas de las víctimas.
Captura de entrada: Registro de pulsaciones (Keylogging)	T1056.001	Descargan el archivo **klg.dll** (un binario de keylogger) en sistemas comprometidos, donde registra las pulsaciones de teclado de los usuarios en un archivo llamado **conhost.txt**.
Stealer o falsificación de tickets Kerberos: Kerberoasting	T1558.003	Posiblemente utilizan un ataque de **Kerberoasting** para comprometer cuentas de administradores de dominio.

Tabla 7. Credenciales de Acceso - MITRE ATT&CK's

Descubrimiento

Técnica	ID	USO
Detección de propietarios/usuarios del sistema	T1033	Ejecutan el comando de PowerShell **WindowsIdentity.GetCurrent()** en sistemas víctimas para obtener un objeto **WindowsIdentity** que representa al usuario de Windows actual.
Descubrimiento de información del sistema	T1082	Ejecutan el comando de PowerShell **systeminfo** en sistemas comprometidos para obtener información detallada de configuración del sistema, incluyendo: ▪ Configuración del sistema operativo ▪ Información de seguridad ▪ ID del producto ▪ Características del hardware Además, ejecutan el comando de PowerShell **Get-PSDrive** en sistemas comprometidos para identificar las unidades de

Técnica	ID	USO
		almacenamiento disponibles en la sesión actual, como, por ejemplo: ▪ Unidades lógicas de Windows en el equipo, incluyendo unidades asignadas a recursos compartidos de red. ▪ Unidades expuestas por proveedores de PowerShell. ▪ Unidades temporales específicas de la sesión y unidades de red mapeadas persistentes.
Detección de servicios del sistema	T1007	Ejecutan el comando de PowerShell **tasklist /svc** en sistemas comprometidos, el cual muestra información de servicios asociados a cada proceso en ejecución en el sistema. También, ejecutan el comando de PowerShell **Get-Service** en sistemas comprometidos, el cual recupera objetos que representan los servicios del sistema (tanto en ejecución como detenidos).
Detección de configuración de red del sistema	T1016	Ejecutan el comando de PowerShell **arp -a** en sistemas comprometidos, el cual muestra y modifica entradas en la **tabla de caché ARP** (Protocolo de Resolución de Direcciones). Esta tabla contiene registros de direcciones **IPv4 e IPv6** en endpoints de la red.

Tabla 8. Descubrimiento - MITRE ATT&CK's

Movimiento Lateral

Técnica	ID	USO
Cuentas válidas	T1078	Recolectan y utilizan abusivamente credenciales legítimas para movimiento lateral y escalamiento de privilegios.
Servicios remotos: Protocolo de Escritorio Remoto (RDP)	T1021.001	Utilizan **RDP (Protocolo de Escritorio Remoto)** y credenciales válidas para moverse lateralmente entre sistemas.

Tabla 9. Movimiento Lateral - MITRE ATT&CK's

Colección

Técnica	ID	USO
Datos de almacenamiento en la nube	T1530	Utilizan **StorageExplorer.exe** (la herramienta oficial *Azure Storage Explorer*) para explorar cuentas de almacenamiento en **Microsoft Azure**.

Tabla 10. Colección - MITRE ATT&CK's

Comando y Control (C2)

Técnica	ID	USO
Comando y control	TA0011	Utilizan las aplicaciones **Cobalt Strike** y **SystemBC** para establecer comunicaciones de **comando y control (C2)**.
Transferencia de herramientas de acceso inicial	T1105	Utilizan una **falsa actualización de Google Chrome o Microsoft Edge** para engañar a los usuarios y hacer que ejecuten un **RAT**

Técnica	ID	USO
		(Remote Access Trojan - Troyano de Acceso Remoto) en los sistemas comprometidos. Tambien descargan **Stealers (**como cht.exe) y **binarios keyloggers** (como klg.dll) una vez que obtienen **control remoto** de un sistema comprometido.
Herramientas de acceso remoto	T1219	Utilizan herramientas legítimas de acceso remoto como **AnyDesk** para establecer conectividad remota y **PuTTY** para facilitar el **movimiento lateral** en la red.

Tabla 11.Comando y control (C2) - MITRE ATT&CK's

Exfiltración

Técnica	ID	USO
Exfiltración mediante servicios web: Exfiltración a almacenamiento en la nube	T1567.002	Exfiltran datos a **almacenamiento en la nube** ejecutando **AzCopy** para subir información a un **blob de almacenamiento de Azure**.
Exfiltración mediante protocolos alternativos	T1048	Utilizan herramientas de transferencia de archivos como **WinSCP** para exfiltrar datos.

Tabla 12. Exfiltración - MITRE ATT&CK's

V. IMPACTO

Además de tener impacto debido al uso de propios aplicativos del sistema

- Cht.exe
- AnyDesk.exe
- WinSCP.exe
- Putty.exe

Tienen su impacto en:

Técnica	ID	USO
Datos cifrados para impacto	T1486	Cifran datos de víctimas utilizando un **algoritmo combinado AES y RSA** en sistemas comprometidos, con el objetivo de interrumpir el acceso a **recursos del sistema y de red**. Los actores Interlock Ransomware programan los módulos de cifrado en **C/C++** y los adaptan para atacar tanto sistemas operativos **Windows como Linux**. Adicionalmente, utilizan un **cifrador ELF para FreeBSD** para comprometer datos en sistemas que ejecutan esta plataforma.
Robo financiero	T1657	Distribuyen una nota de rescate titulada **!README!.txt** mediante una **Política de Grupo (GPO)**, donde proporcionan a las víctimas instrucciones para contactarlos a través de una **URL .onion** en la red **Tor**. Emplean un **modelo de doble extorsión**: además de cifrar los datos de las víctimas, amenazan con filtrar la información en su **sitio de filtración (leak site)** alojado en Tor si no se paga el rescate.

Técnica	ID	USO
Exfiltración mediante protocolos alternativos	T1048	Utilizan herramientas de transferencia de archivos como **WinSCP** para exfiltrar datos.

Tabla 13. Impacto - MITRE ATT&CK's

VI. INDICADORES DE COMPROMISO

Nombre del archivo	Hash
1.ps1	fba4883bf4f73aa48a957d894051d78e0085ecc3170b1ff50e61ccec6aeee2cd
advanced_port_scanner.exe	4b036cc9930bb42454172f888b8fde1087797fc0c9d31ab546748bd2496bd3e5
Aisa.exe	18a507bf1c533aad8e6f2a2b023fbbcac02a477e8f05b095ee29b52b90d47421
AnyDesk.exe	1a70f4eef11fbecb721b9bab1c9ff43a8c4cd7b2cafef08c033c77070c6fe069
autoservice.dll	a4069aa29628e64ea63b4fb3e29d16dcc368c5add304358a47097eedafbbb565
Autostart.exe	d535bdc9970a3c6f7ebf0b229c695082a73eaeaf35a63cd8a0e7e6e3ceb22795
cht	FAFCD5404A992850FFCFFEE46221F9B2FF716006AECB637B80E5CD5AA112D79C
cht.exe	C20BABA26EBB596DE14B403B9F78DDC3C13CE9870EEA332476AC2C1DD582AA07
cleanup.dll (SystemBC)	1845a910dcde8c6e45ad2e0c48439e5ab8bbbeb731f2af11a1b7bbab3bfe0127
conhost	44887125aa2df864226421ee694d51e5535d8c6f70e327e9bcb366e43fd892c1
conhost.dll	a70af759e38219ca3a7f7645f3e103b13c9fb1db6d13b68f3d468b7987540ddf
conhost.dll	96babe53d6569ee3b4d8fc09c2a6557e49ebc2ed1b965abda0f7f51378557eb1
difxepi.dll (SystemBC)	1845a910dcde8c6e45ad2e0c48439e5ab8bbbeb731f2af11a1b7bbab3bfe0127
iexplore.exe	d0c1662ce239e4d288048c0e3324ec52962f6ddda77da0cb7af9c1d9c2f1e2eb
klg.dll	A4F0B68052E8DA9A80B70407A92400C6A5DEF19717E0240AC608612476E1137E
!!!OPEN_ME!!!.txt	68A49D5A097E3850F3BB572BAF2B75A8E158DADB70BADDC205C2628A9B660E7A
processhacker-2.39-bin.zip	88f26f3721076f74996f8518469d98bf9be0eaee5b9eccc72867ebfc25ea4e83
PsExec.exe	078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b
putty.exe	7a43789216ce242524e321d2222fa50820a532e29175e0a2e685459a19e09069
puttyportable.exe	97931d2e2e449ac3691eb526f6f60e2f828de89074bdac07bd7dbdfd51af9fa0
PuTTYPortable.zip	ff7ad2376ae01e4b3f1e1d7ae630f87b8262b5c11bc5d953e1ac34ffe81401b5
qrpce91.exe.asd	64a0ab00d90682b1807c5d7da1a4ae67cde4c5757fc7d995d8f126f0ec8ae983
ScreenConnect.ClientService.exe	2814b33ce81d2d2e528bb1ed4290d665569f112c9be54e65abca50c41314d462
SophosendpointAgent.exe	f51b3d054995803d04a754ea3ff7d31823fab654393e8054b227092580be43db
SophosScaner.exe	dfb5ba578b81f05593c047f2c822eeb03785aecffb1504dcb7f8357e898b5024
Starship.exe	94bf0aba5f9f32b9c35e8dfc70afd8a35621ed6ef084453dc1b10719ae72f8e2
start	28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f
start.exe	70bb799557da5ac4f18093decc60c96c13359e30f246683815a512d7f9824c8f
StorageExplorer.exe	73a9a1e38ff40908bcc15df2954246883dadfb991f3c74f6c514b4cffdabde66
Sysmon.sys	1d04e33009bcd017898b9e1387e40b5c04279c02ebc110f12e4a724ccdb9e4fb
upd_2327991.exe	7b9e12e3561285181634ab32015eb653ab5e5cfa157dd16cdd327104b258c332
webujgd.lnk	70EE22D394E107FBB807D86D187C216AD66B8537EDC67931559A8AEF18F6B5B3
WinSCP-6.3.5-Setup.exe	8eb7e3e8f3ee31d382359a8a232c984bdaa130584cad11683749026e5df1fdc3
Proxy Tool	e4d6fe517cdf3790dfa51c62457f5acd8cb961ab1f083de37b15fd2fddeb9b8f
Encryptor	e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1
Encryptor	c733d85f445004c9d6918f7c09a1e0d38a8f3b37ad825cd544b865dba36a1ba6
Encryptor	28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f

Tabla 14. Archivos SHA-256 - Interlock Ransomware

Nombre del archivo	Hash
autorun.log	514946a8fc248de1ccf0dbeee2108a3b4d75b5f6
jar.jar	b625cc9e4024d09084e80a4a42ab7ccaa6afb61d
pack.jar	3703374c9622f74edc9c8e3a47a5d53007f7721e

Tabla 15. Archivos SHA-1 - Interlock Ransomware

Direcciones IP
23.95.182[.]59
212.237.217[.]182
168.119.96[.]41
216.245.184[.]181
45.61.136[.]202
188.34.195[.]44
65.38.120[.]47

Tabla 16. Direcciones IP - Interlock Ransomware

URLs
hxxp[:]//23[.]95[.]182[.]59/31279geuwtoisgdehbiuowaehsgdb/cht
hxxp[:]//23[.]95[.]182[.]59/31279geuwtoisgdehbiuowaehsgdb/klg
hxxps[:]//apple-online[.]shop/ChromeSetup[.]exe
hxxps[:]//rvthereyet[.]com/wp-admin/images/rsggj[.]php

Tabla 17. URLs - Interlock Ransomware

VII. RECOMENDACIONES:

- Bloquear los indicadores de compromiso (IoCs) en soluciones EDR, SIEM y firewall.
- Capacitar al personal sobre técnicas de ingeniería social utilizadas en ataques FileFix y ClickFix.
- Mantener actualizado el sistema operativo y todas las aplicaciones críticas mediante parches de seguridad.
- Habilitar herramientas de protección como EDR, AMSI y antimalware, especialmente contra scripts maliciosos y uso de PowerShell.
- Restringir el acceso por RDP, AnyDesk, PuTTY y monitorear activamente su uso.
- Auditar el Directorio Activo (AD) y realizar rotación de credenciales luego de cualquier incidente de seguridad.
- Establecer políticas de respaldo periódico en medios offline, verificando la integridad y capacidad de recuperación.
- Supervisar la posible exfiltración de datos mediante herramientas como AzCopy o Azure Storage Explorer.
- Prevenir la ejecución de macros y herramientas legítimas abusadas (Living off the Land) como rundll32 y certutil.

- Detectar comportamientos anómalos en la red, como ejecución de tareas sospechosas (ej. “TaskSystem”), rundll32 o uso no autorizado de PuTTY.
- Deshabilitar macros en documentos y controlar el uso de binarios legítimos del sistema (LoLBins) para evitar ejecuciones no autorizadas.
- Tras aplicar parches, reiniciar servicios de IIS y rotar claves ASP.NET (MachineKey) en servidores SharePoint para invalidar persistencias.

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:

ANY.RUN (2025). Malware Trends – Interlock. https://any.run/malware-trends/interlock/

THE DFIR REPORT (2025). Kongtuke FileFix leads to new Interlock RAT variant. https://thedfirreport.com/2025/07/14/kongtuke-filefix-leads-to-new-interlock-rat-variant/

CISA (2025). Cybersecurity Advisory – #StopRansomware: Interlock. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-203a

BLEEPINGCOMPUTER (2025). Interlock ransomware adopts FileFix method to deliver malware. https://www.bleepingcomputer.com/news/security/interlock-ransomware-adopts-filefix-method-to-deliver-malware/

TECHRADAR (2025). Hackers are abusing FileFix technique to drop RATs during ransomware attacks. https://www.techradar.com/pro/security/hackers-are-abusing-filefix-technique-to-drop-rats-during-ransomware-attacks

CYBLE (2025). Interlock Ransomware Group – Threat Actor Profile. https://cyble.com/threat-actor-profiles/interlock-ransomware-group/

SEKOIA.IO (2025). Interlock ransomware evolving under the radar. https://blog.sekoia.io/interlock-ransomware-evolving-under-the-radar/

GBHACKERS (2025). Interlock ransomware uses multi-stage attack through legitimate websites. https://gbhackers.com/interlock-ransomware-uses-multi-stage-attack-through-legitimate-websites/

FORTINET (2024). Ransomware Roundup: Interlock. https://www.fortinet.com/blog/threat-research/ransomware-roundup-interlock

CISCO TALOS (2024). Emerging Interlock Ransomware. https://blog.talosintelligence.com/emerging-interlock-ransomware/

CISCO TALOS (2024). IOCs – Emerging Interlock Ransomware. https://github.com/Cisco-Talos/IOCs/blob/main/2024/11/emerging-interlock-ransomware.txt