Nro. Alerta:	AL-2025-024	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	17-jun-2025	INC Ransomware	Pág.: **1** of **15**

I. DATOS GENERALES:

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

II. ALERTA

Figura 1.- INC Ransomware - figura referencial

INC Ransomware explota la vulnerabilidad CVE-2023-3519 y utiliza herramientas como HackTool.Win32.ProcTerminator.A para evadir defensas y HackTool.PS1.VeeamCreds para robar credenciales en sus distintas cadenas de ataque.

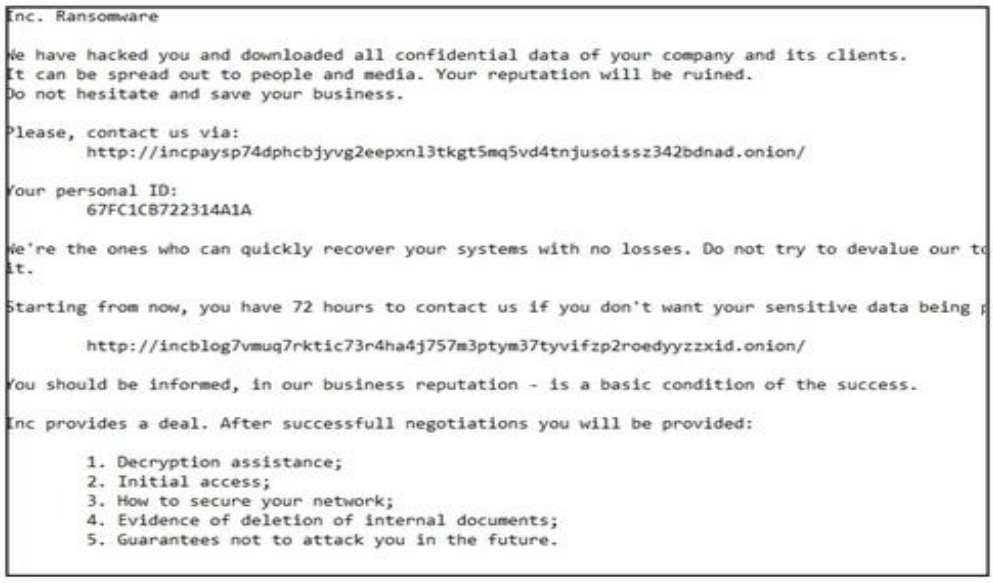
III. INTRODUCCIÓN

Activo desde julio de 2023, INC Ransomware tiene su esquema de doble extorsión, bajo el pretexto de "salvaguardar la reputación" de sus víctimas para presionarlas a pagar rescate. Utiliza dos sitios de filtración: el primero es un sitio que requiere credenciales de inicio de sesión que el atacante proporciona a sus víctimas y que funciona como medio de comunicación; y el segundo es un sitio web de acceso público donde se alojan los datos filtrados.

En diciembre de 2023 se publicó una versión de Linux para el binario del INC Ransomware.

En marzo de 2024, se lanzó otra versión de su variante para Windows.

INC Ransomware, al igual que los demás cifran archivos en sistemas Windows usando el algoritmo AES, modifica el fondo de escritorio para mostrar la nota de rescate. Al mismo tiempo trata de enviar la nota de rescate a las impresoras conectadas.



```
Inc. Ransomware

We have hacked you and downloaded all confidential data of your company and its clients.
It can be spread out to people and media. Your reputation will be ruined.
Do not hesitate and save your business.

Please, contact us via:
        http://incpaysp74dphcbjyvg2eepxnl3tkgt5mq5vd4tnjusoissz342bdnad.onion/

Your personal ID:
        67FC1CB722314A1A

We're the ones who can quickly recover your systems with no losses. Do not try to devalue our to
it.

Starting from now, you have 72 hours to contact us if you don't want your sensitive data being p

        http://incblog7vmuq7rktic73r4ha4j757m3ptym37tyvifzp2roedyyzzxid.onion/

You should be informed, in our business reputation - is a basic condition of the success.

Inc provides a deal. After successfull negotiations you will be provided:

        1. Decryption assistance;
        2. Initial access;
        3. How to secure your network;
        4. Evidence of deletion of internal documents;
        5. Guarantees not to attack you in the future.
```

Figura 2.- La nota de rescate - INC Ransomware (README.TXT)

IV. VECTOR DE ATAQUE

TrendMicro hace referencia a las tácticas y técnicas de MITRE y detallan el proceso de ataque de INC Ransomware:

a) Persistencia

- **T1543 - Crear o modificar proceso del sistema**

  El ransomware INC añade los siguientes servicios para permitir la ejecución automática en modo seguro:
  - Nombre: dmksvc
  - Tipo de inicio: Inicio automático
  - Ruta binaria: {Ruta del archivo de malware}\{Nombre del archivo de malware)

La variante de Linux del ransomware INC añade el comando "-daemon", lo que permite que la muestra se separe de su proceso principal y se convierta en un proceso principal propio (esta línea de código podría sugerir que el atacante usará una conexión SSH con la víctima para ejecutar la muestra).

b) Defensa Evasión

- **T1562.009 - Debilitar defensas**

  Arranque en modo seguro
  El ransomware INC puede arrancar el equipo en modo seguro mediante el parámetro '--safe-mode'.

- **T1070 - Eliminación del indicador**

  El ransomware INC vacía la papelera de reciclaje.

c) Descubrimiento

- **T1057 - Descubrimiento de procesos**

  Finaliza los siguientes procesos:
  • SQL
  • Veeam
  • Backup
  • Exchange
  • Java

d) Impacto

- **T1486 - Datos cifrados para mayor impacto**

  El ransomware INC evita el cifrado de los siguientes archivos con la siguiente extensión:
  - .msi
  - .exe
  - .dll
  - .inc

Las nuevas muestras del ransomware INC evitan el cifrado de los siguientes archivos con la siguiente extensión:

- .exe
- .msi
- .dll
- .inc

El ransomware INC evita las siguientes carpetas que contienen las siguientes cadenas en su ruta de archivo:

- Windows
- Archivos de programa
- Archivos de programa (x86)
- $RECYCLE.BIN
- Appdata

Las muestras más recientes evitan las siguientes carpetas que contienen las siguientes cadenas en su ruta de archivo:

- Windows
- Archivos de programa
- Archivos de programa (x86)
- $RECYCLE.BIN
- Appdata
- Microsoft SQL Server

El ransomware INC añade la extensión .inc a sus archivos cifrados.

El ransomware INC publica una nota de rescate:

- INC-README.txt
- INC-README.html

Nuevas muestras del ransomware INC añaden la siguiente extensión a sus archivos cifrados: {nombre del archivo original}.{extensión original}.INC

Nuevas muestras del ransomware INC publican las siguientes notas de rescate**:**

- {Directorio cifrado}\INC-README.txt
- {Directorio cifrado}\INC-README.html

Para acelerar el cifrado, las versiones anteriores del ransomware INC emplean cifrado parcial combinado con un enfoque multihilo. El

ransomware genera una clave aleatoria para el cifrado de archivos y la API, CryptGenRandom, utiliza las siguientes cadenas como parámetros.

El ransomware INC utiliza el algoritmo AES para el cifrado de archivos. Cifra todas las unidades, incluidas las montadas, y luego envía la nota de ransomware a todas las impresoras de la red para su impresión.

Nuevas muestras del ransomware INC siguen utilizando el siguiente método de cifrado de versiones anteriores. El ransomware INC emplea cifrado parcial combinado con un enfoque multihilo. Genera una clave aleatoria para el cifrado de archivos mediante la API CrypGenRandom con los siguientes parámetros:

- Utiliza el algoritmo AES para el cifrado de archivos.
- Ofrece tres modos de cifrado: rápido (cifra con un valor fijo de 1 000 000 de bytes y omite un byte mayor), medio (cifra con un valor fijo de 1 000 000 de bytes y omite un byte menor) y lento (cifra todo el archivo).

A continuación, envía la nota del ransomware a todas las impresoras de la red y las imprime.

- **T1490 - Inhibir la recuperación del sistema**

  El ransomware INC intenta eliminar las instantáneas del sistema.

- **T1491.001 - Desfiguración interna**

  El ransomware INC cambia el fondo de pantalla del equipo víctima por una nota que declara que la información del equipo ha sido confiscada y comprometida.

Así también se debe considerar las siguientes:

ID	Nombre	Uso
T1486	Datos cifrados para impacto	INC Ransomware puede cifrar datos en los sistemas de las víctimas, utilizando técnicas como el cifrado parcial y el uso de múltiples hilos para acelerar el proceso.
T1491.001	Desfiguración: Desfiguración interna	INC Ransomware puede cambiar el fondo de pantalla del sistema para mostrar la nota de rescate.
T1140	Desofuscación / Decodificación de	INC Ransomware puede ejecutar `CryptStringToBinaryA` para descifrar contenido codificado en base64 que contiene la nota de rescate.

ID	Nombre	Uso
	archivos o información	
T1652	Descubrimiento de controladores de dispositivos	INC Ransomware puede verificar la presencia de ciertos controladores en los sistemas comprometidos, como Microsoft Print to PDF y Microsoft XPS Document Writer.
T1083	Descubrimiento de archivos y directorios	INC Ransomware puede recibir argumentos de línea de comandos para explorar y encontrar archivos y carpetas específicas.
T1490	Inhibición de la recuperación del sistema	INC Ransomware puede eliminar las copias de seguridad de volumen shadow (instantáneas del sistema) para evitar la recuperación del sistema por parte de la víctima.
T1570	Transferencia lateral de herramientas	INC Ransomware puede transferir su ejecutable de cifrado a múltiples dispositivos dentro de una red comprometida.
T1106	API nativa	INC Ransomware puede usar la API `DeviceIoControl` para cambiar el tamaño del espacio asignado y provocar la eliminación de las copias de seguridad del sistema (shadow copies).
T1135	Descubrimiento de recursos compartidos en red	INC Ransomware puede buscar carpetas o discos compartidos en red para cifrarlos.
T1120	Descubrimiento de dispositivos periféricos	INC Ransomware puede identificar discos duros o USB externos, así como impresoras, para cifrarlos o imprimir notas de rescate.
T1566	Phishing	Las campañas de INC Ransomware han utilizado correos de phishing (spearphishing) como vector de acceso inicial.
T1057	Descubrimiento de procesos	INC Ransomware puede usar el administrador de reinicio de Windows (Win32 Restart Manager) para identificar procesos específicos que quiere detener antes de cifrarlos.
T1489	Detención de servicios	INC Ransomware puede emitir comandos para detener servicios en los sistemas comprometidos.
T1082	Descubrimiento de información del sistema	INC Ransomware puede recopilar y analizar información del sistema, ocultando unidades para cifrarlas.
T1047	Instrumentación de administración de Windows (WMI)	INC Ransomware puede utilizar `wmic.exe` para propagarse a otros dispositivos dentro del entorno comprometido.

Tabla 1.- Técnicas y procesos de ataque - INC Ransomware

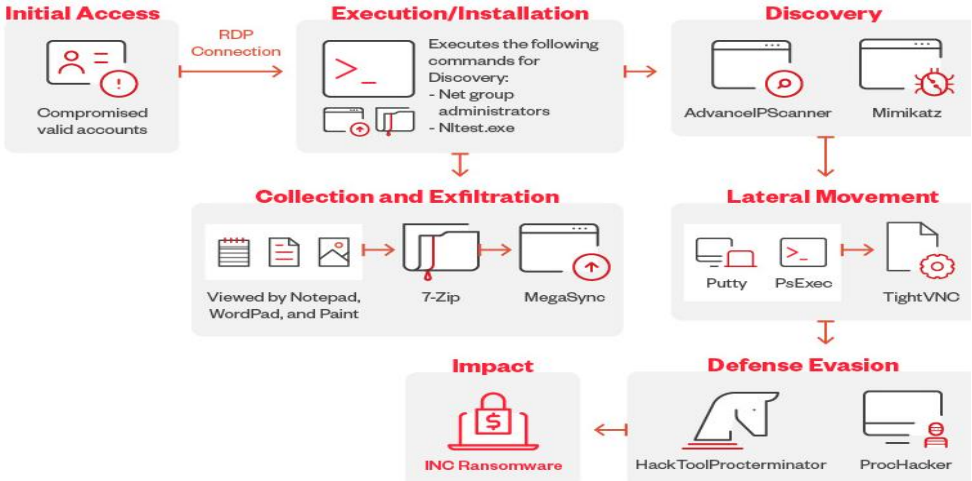


Figura 3.- Cadena de infección observada - INC Ransomware

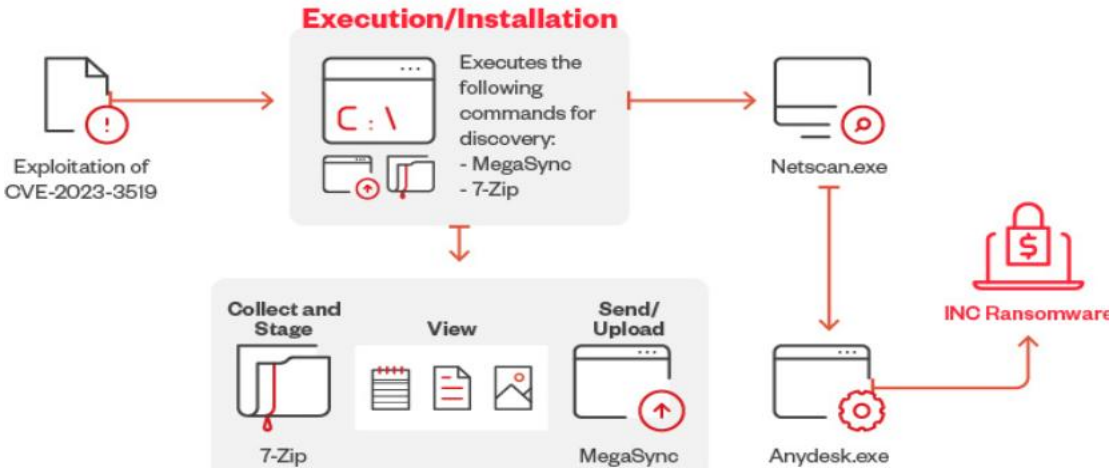


Figura 4.- Infección de INC Ransomware vía exploit CVE-2023-3519 emplea nuevas herramientas para ejecutar su ataque.

1. Acceso Inicial

INC. Ransomware emplea dos métodos para ganar el acceso inicial de los sistemas de sus víctimas:

a. Uso de correos de Spear Phishing (ataque de phishing dirigido y personalizado a una víctima en concreto) son un vector común, aprovechando las vulnerabilidades humanas para engañar a las personas y hacer que hagan clic en enlaces maliciosos o descarguen archivos adjuntos infectados.

b. Explotación de la vulnerabilidad CVE-2023-3519 en Citrix NetScaler para obtener ese acceso inicial a los dispositivos de red de las víctimas.

2. Persistencia y Evasión

Crea o modifica procesos del sistema, INC Ransomware agrega el siguiente servicio para permitir su ejecución automática en modo seguro:

- **Nombre:** dmksvc
- **Tipo de inicio:** AutoStart (Inicio automático)
- **Ruta del binario:** {Malware File Path}\{Malware FileName}

En la variante de Linux, INC Ransomware añade el comando **"daemon"**, lo que permite que la muestra se desvincule de su proceso padre para convertirse

en un proceso independiente (esta línea de código podría sugerir que el actor de amenazas utilizará una conexión SSH a la víctima para ejecutar la muestra).

Como métodos de evasión, INC Ransomware, utiliza HackTool.Win32.ProcTerminator.A y ProcessHacker para evadir la detección, también tiene la capacidad de iniciar la máquina en modo seguro utilizando el parámetro -“safe-mode”.

3. Reconocimiento Interno y Movimiento Lateral

Tras establecerse en el sistema, INC Ransomware, realiza un reconocimiento exhaustivo dentro de la red de la víctima, utilizando herramientas como NETSCAN.EXE para el descubrimiento de servicios de red y RDP (Escritorio Remoto) para probar conexiones. Además, buscan cuentas de administrador de dominio y llevan a cabo una enumeración de grupos del dominio, todo con el objetivo de preparar el movimiento lateral dentro del entorno, usando herramientas como:

- NETSCAN.EXE, escáner y perfilador de red (software diseñado para analizar, mapear y documentar las características de una red), realiza tareas como escaneo de puertos, detección de servicios y creación de perfiles de red. Además, puede utilizarse tanto para escaneo local (dentro de la misma red) como remoto (en diferentes redes).

- MINIKATZ, herramienta de Windows permite extraer las contraseñas de inicio de sesión, tickets de kerberos, hashes NTLM y certificados en Windows.

- ESENTUTL.EXE, utilidad de Microsoft utilizada principalmente para la gestión y recuperación de bases de datos. Permite a los administradores realizar tareas como la reparación, compactación y comprobaciones de integridad de bases de datos. Es esencial para mantener el estado y la fiabilidad de las bases de datos ESE.

- ANYDESK.EXE, aplicación de administración y escritorio remoto. Permite a los usuarios acceder y controlar un ordenador remoto desde otro dispositivo, independientemente de su ubicación física.

- PSEXEC, herramienta de línea de comandos desarrollada por Microsoft Sysinternals que permite ejecutar procesos de forma remota en otros equipos de una red.

- TIGHTVNC, Software gratuito y de código abierto (GPL) permite el control remoto de computadoras mediante el protocolo VNC (*Virtual Network Computing*). Está diseñado para acceder y administrar equipos de forma remota.

4. Recopilación y exfiltración de datos

INC Ransomware, almacena temporalmente los datos en los equipos comprometidos, comprimiéndolos con herramientas como 7-Zip o WinRAR, antes de exfiltrarlos a almacenamiento en la nube mediante Megasync. Este proceso no solo busca presionar a las víctimas mediante la amenaza de filtrar información confidencial, sino que también aumenta el impacto financiero potencial del ataque.

5. Encriptación y entrega de notas de rescate

INC Ransomware, excluye las siguientes extensiones del cifrado:

- **.**msi (paquetes de instalación de Windows)
- .exe (archivos ejecutables)
- .dll (bibliotecas dinámicas)
- .inc (archivos de inclusión, comunes en programación)

También, excluye de su cifrado las carpetas que contienen las siguientes cadenas en su ruta:

- Windows
- Program files
- Program files (x86)
- $RECYCLE.BIN
- Appdata
- Microsoft SQL server

INC Ransomware usa el algoritmo de cifrado AES, para encriptar todas las unidades detectadas en la maquina víctima, inclusive las unidades montadas.

Para acelerar este cifrado, INC Ransomware emplea el cifrado parcial también llamado cifrado selectivo o progresivo, combinado con un enfoque multihilo, generando una clave aleatoria para el cifrado de archivos utilizando la API CryptGenRandom con un string como parámetro.

Las muestras evidencian que para este, INC Ransomware usa tres modos de cifrado para optimizar su ataque, estos son:

- **Modo rápido,** cifra con un valor fijo de 1.000.000 de bytes y omite bytes más grandes, como ventaja infecta el sistema en corto tiempo dejando archivos inaccesibles, pero sin cifrarlos completamente, evita su detección y se propaga antes de que se active una respuesta.

- **Modo medio,** cifra con un valor fijo de 1.000.000 de bytes y omite bytes más pequeños, hay equilibrio entre velocidad y daño irreversible, emplea cifrado completo con AES-256 omite archivos temporales o del sistema, cifra completamente archivos como .xlsx, .sql, .pdf.

- **Modo lento,** cifra todo el archivo de manera silencioso en segundo plano, con pausas entre archivos, para evadir soluciones EDR/antivirus y evitar saturación del sistema.

Luego de cifrar los archivos, INC Ransomware deja una marca distintiva en su nota de rescate al colocarla en cada carpeta encriptada (README.TXT y NC-README.HTML), como imagen de fondo de pantalla y también él envió a cualquier impresora o fax acce.

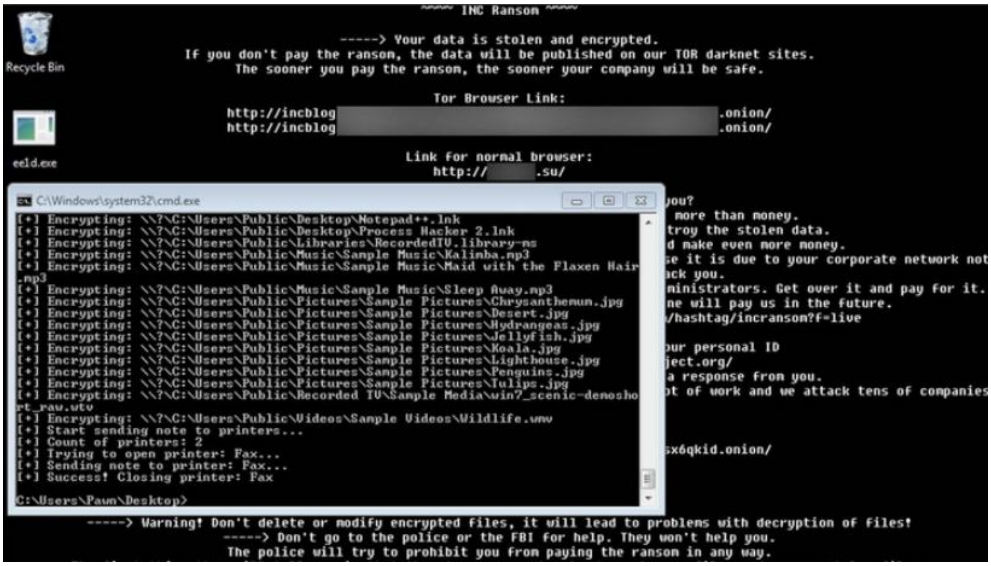


Figura 5.- Nota de rescate como fondo de escritorio - INC Ransomware

Para afianzar aún más su control sobre los datos de la víctima, INC Ransomware intenta eliminar las Copias de Sombra de Volumen (VSS),

aunque este comportamiento no se produce de manera consistente, es un inicio claro de que el ransomware busca eliminar posibles vías de recuperación de datos, aumentando así la presión sobre la víctima para que acceda a pagar el rescate.

V. IMPACTO

INC Ransomware afecta principalmente a Microsoft Windows, algunas detecciones del sistema:

- **Avast Win32**: RansomX-gen [Ransom]
- **Emsisoft Gen**: Heur. Ransom.Imps.1 (B)
- **Kaspersky**: Trojan-Ransom.Win32.Inc.a
- **Malwarebytes:** Ransom.IncRansom
- **Microsoft:** Ransom:Win32/IncRansom.YAA!MTB
- **Sophos:** Troj/Ransom-GYR

Aplicativos usados para la persistencia y movimiento lateral:

- NETSCAN
- ESENTUTL
- ANYDESK
- PSexec
- TightVNC
- 7-zip
- WinRAR
- Megasync
- Minikatz.

VI. INDICADORES DE COMPROMISO

DIRECCIONES IP	CODIGO PAIS	TIPO DE USO	ISP	DOMINIO
62.113.109.238	RU	Data Center/Web Hosting/Transit	Beget LLC	beget.ru
196.32.195.78	AO	Fixed Line ISP	Network Assigned to MULTITEL ANGOLA	multitel.co.ao
31.128.46.144	RU	Data Center/Web Hosting/Transit	Beget LLC	beget.ru
62.113.111.128	RU	Data Center/Web Hosting/Transit	Beget LLC	beget.ru
196.32.195.78	AO	Fixed Line ISP	Network Assigned to MULTITEL ANGOLA	multitel.co.ao

DIRECCIONES IP	CODIGO PAIS	TIPO DE USO	ISP	DOMINIO
45.131.41.207	RU	Data Center/Web Hosting/Transit	Selectel Network	selectel.ru
185.68.93.122	BG	Data Center/Web Hosting/Transit	Relink LTD	cishost.ru
185.68.93.233	BG	Data Center/Web Hosting/Transit	Relink LTD	cishost.ru
31.41.44.202	RU	Data Center/Web Hosting/Transit	Relink LTD	relink.nl
77.88.44.55	RU	Content Delivery Network	Yandex enterprise network	yandex.net
199.232.177.229	CO	Data Center/Web Hosting/Transit	Fastly, Inc.	fastly.com
64.190.113.159	US	Data Center/Web Hosting/Transit	BL Networks	blnwx.com
147.135.36.162	US	Data Center/Web Hosting/Transit	OVH SAS	ovhcloud.com

Tabla 2.- Direcciones IP - INC Ransomware

DOMINIOS
incapt.su
inccdn1.lol
inccdn2.lol
inccdn3new.lol
lynxback.pro
incback.su
incblog.su
lynxstorage1.net
lynxblog.net
incapt.blog
incadmin.su
lynxchat.net
lynxpanel.net
incblog7vmuq7rktic73r4ha4j757m3ptym37tyvifzp2roedyyzzxid.onion
incblog6qu4y4mm4zvw5nrmue6qbwtgjsxpw6b7ixzssu36tsajldoad.onion

Tabla 3.- Dominios - INC Ransomware

SUBDOMINIOS
admin.inccdn1.lol
admin.inccdn3new.lol
admin.lynxback.pro
api.incback.su
api.inccdn1.lol
api.lynxback.pro
app.inccdn1.lol
app.inccdn3new.lol
app.lynxback.pro

SUBDOMINIOS
backend.incback.su
backend.inccdn1.lol
demo.inccdn1.lol
demo.lynxback.pro
www.inccdn3new.lol
www.lynxback.pro
dev.inccdn1.lol
staging.inccdn1.lol
staging.incback.su
admin.incback.su
app.incback.su
dev.lynxback.pro
demo.incback.su
staging.inccdn3new.lol
staging.lynxback.pro
random.lynxpanel.net
meradmin.lynxblog.net
meradmin.lynxchat.net
navigation.lynxchat.net
random.lynxstorage1.net
random.lynxpanel.net

Tabla 4.- Subdominios - INC Ransomware

SHA256
6bc8b8f260f9f9bfea69863ef8d3c525568676ddadc09c14655191cad1acdb5b
fcefe50ed02c8d315272a94f860451bfd3d86fa6ffac215e69dfa26a7a5deced
a0ceb258924ef004fa4efeef4bc0a86012afdb858e855ed14f1bbd31ca2e42f5
e2370ef066df692317a5f9d739120e467144cfdcd9a4dd7dd562ebdbf5f0778c
1754c9973bac8260412e5ec34bf5156f5bb157aa797f95ff4fc905439b74357a
f96ecd567d9a05a6adb33f07880eebf1d6a8709512302e363377065ca8f98f56
11cfd8e84704194ff9c56780858e9bbb9e82ff1b958149d74c43969d06ea10bd
869d6ae8c0568e40086fd817766a503bfe130c805748e7880704985890aca947
0cb4e7d35eb3f4585c6168988247e30d99ef24d3ef006d91971e3913ef593c42
47873072a0ed065e2f240da3e8b10e7251b9596a82cf0375bfc17f60708b8f74
3c4e8f6a5dc94966483069b68981b0ad77ff9c547e8ec3d74ed207e3f037ece6
c41ab33986921c812c51e7a86bd3fd0691f5bba925fae612f1b717afaa2fe0ef
36e3c83e50a19ad1048dab7814f3922631990578aab0790401bc67dbcc90a72e
508a644d552f237615d1504aa1628566fe0e752a5bc0c882fa72b3155c322cef
d147b202e98ce73802d7501366a036ea8993c4c06cdfc6921899efdd22d159c6
5e3c44ac77cba228f54304f7f1f9ee4d86099950f230186f11fffaa76c86a5db
463075274e328bd47d8092f4901e67f7fff6c5d972b5ffcf821d3c988797e8e3

Tabla 5.- SHA256 - INC Ransomware

VII. RECOMENDACIONES:

- Aislar inmediatamente los sistemas comprometidos para evitar la propagación del ransomware dentro de la red.
- Verificar y actualizar las copias de seguridad, asegurándose de que estén desconectadas de la red (offline o en entornos separados).
- Cambiar todas las contraseñas administrativas y de usuarios que hayan podido estar comprometidas, especialmente en sistemas expuestos.
- Realizar un escaneo completo de la red con herramientas antivirus/antimalware actualizadas y EDR para detectar procesos o archivos maliciosos activos.
- Revisar logs de eventos, tráfico de red y accesos remotos, buscando patrones inusuales o conexiones a direcciones IP sospechosas.
- Parchear y actualizar todos los sistemas vulnerables, especialmente aquellos accesibles desde internet (servidores, aplicaciones web, VPN, RDP).
- Deshabilitar servicios innecesarios o inseguros, como Escritorio Remoto (RDP), SMBv1, u otros comúnmente usados en ataques de ransomware.
- Capacitar al personal sobre ingeniería social, correos de phishing y prácticas de ciberseguridad básicas.
- Pagar no garantiza la recuperación y financia actividades delictivas. Se debe priorizar restaurar desde respaldos.

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:

- CVEDetails.com (2025). Vulnerability Details: CVE-2023-3519. https://www.cvedetails.com/cve/CVE-2023-3519/
- CVE (2024). CVE-2023-3519. https://www.cve.org/CVERecord?id=CVE-2023-3519

- TREND MICRO (2024). Ransomware Spotlight INC. https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-inc

- CYBLE (2025.). Threat Actor Profile: INC Ransom. https://cyble.com/threat-actor-profiles/inc-ransom/

- FORTINET (2025). Ransomware Roundup - Lynx. https://www.fortinet.com/blog/threat-research/ransomware-roundup-lynx