Nro. Alerta:	EC-2022-22	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	07-febrero-2022	**Ransomware Sugar**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Contenido Dañino
Tipo de incidente: Malware
Nivel de riesgo: Alta

II. ALERTA

El equipo de investigación de seguridad de Walmart; dio a conocer el modo de operación de Sugar, un ransomware orientado a dispositivos individuales, probablemente pertenecientes a usuarios o a pequeñas empresas.

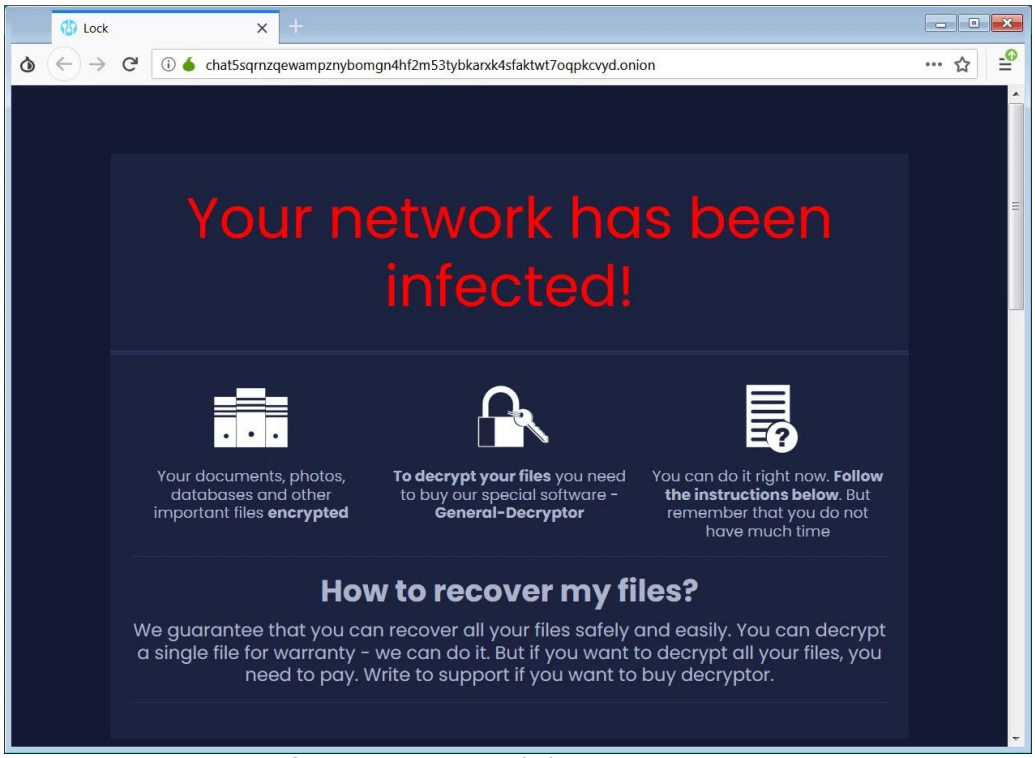


Figura 1. Imagen asociada a ransomware Sugar
Fuente: Bleepingcomputer

Nro. Alerta:	EC-2022-22	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	07-febrero-2022	**Ransomware Sugar**	Versión 1.0

III. INTRODUCCIÓN

Ransomware es un malware diseñado para cifrar archivos en un dispositivo, en donde los actores malintencionados exigen un rescate a cambio del descifrado. En este sentido, SUGAR es un nuevo Raas (Ransomware-as-a-Service) que opera desde noviembre de 2021; teniendo como principal característica, su enfoque de ataque a computadoras individuales en lugar de empresas enteras.

SUGAR cifra los archivos utilizando el algoritmo de cifrado SCOP[1], los archivos cifrados tienen la extensión .**encoded01**; así mismo, el valor que piden por entregar la información comprometida varía entre: unos cientos a unos pocos dólares en Bitcoins; este valor fluctuante estaría en función de la cantidad de información comprometida.

IV. VECTOR DE ATAQUE:

A continuación, se describen el vector de ataque del ransomware SUGAR.

1. Sugar Ransomware se conecta a whatismyipaddress.com e ip2location.com para obtener la dirección IP y la ubicación geográfica del dispositivo.
2. Posteriormente, se descarga el archivo: http://cdn2546713[.]cdnmegafiles[.]com/data23072021_1.dat
3. Se conecta al servidor de comando y control de la operación de ransomware en 179[.]43[.]160[.]195
4. El ransomware continuará llamando al servidor de comando y control a medida que se ejecuta.
5. SUGAR cifrará todos los archivos, excepto los que se enumeran en la siguiente tabla.

Carpetas Excluidas	Archivos Excluidos	
\windows\ \DRIVERS\ \PerfLogs\ \temp\ \boot\	BOOTNXT bootmgr pagefile .exe .dll .sys .lnk	.bat .cmd .ttf .manifest .ttc .cat .msi

Tabla 1. Carpetas y Archivos excluidos

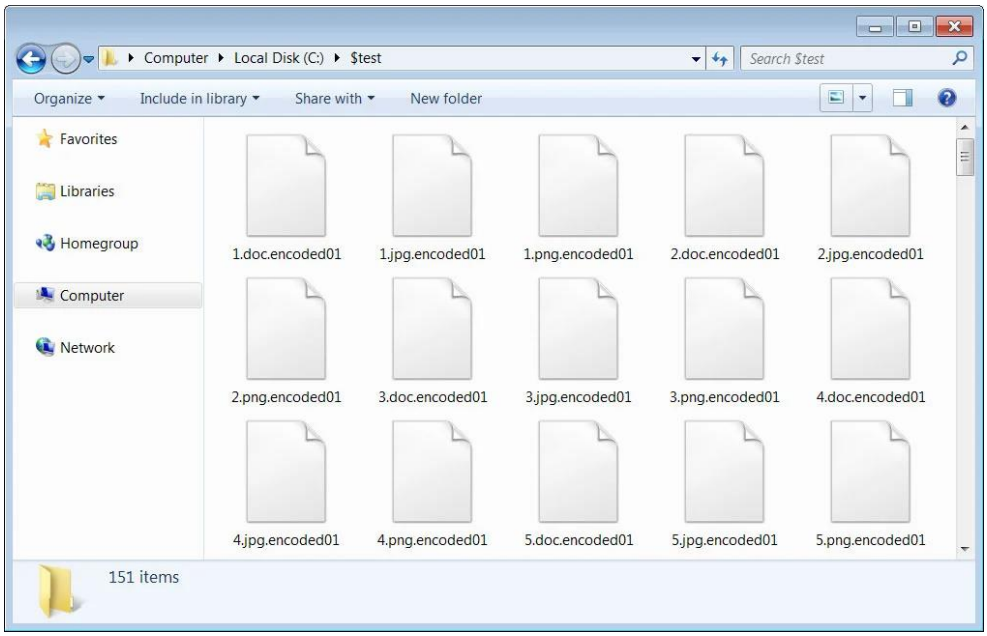
[1] SCOP es un cifrado de flujo que funciona en modo IFB y utiliza una clave de tamaño variable. El flujo de claves consta de palabras de 32 bits y es independiente del mensaje cifrado. El algoritmo tiene dos partes: clave expansión y encriptación de datos. El primero convierte la clave, que tiene una longitud de hasta 48 bytes, en una matriz de 1540 bytes.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-22	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	07-febrero-2022	**Ransomware Sugar**	Versión 1.0

6. Los archivos cifrados por el algoritmo SCOP poseen una extensión **.encoded01.**
7. Así mismo, se crearan notas de rescate: **BackFiles_encoded01.txt;** en donde se indica que los archivos se encuentran cifrados, una identificación única, un link a un sitio Tor con información de cómo pagar por el rescate.
8. En el sitio Tor se encuentra la dirección BitCoin para pagar pagar por el rescate de información, sección de chat y la capacidad de descifrar cinco (5) archivos de forma gratuita.

En la siguiente figura se observa los archivos cifrados y la nota de rescate correspondientes:



Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-22	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	07-febrero-2022	**Ransomware Sugar**	Versión 1.0

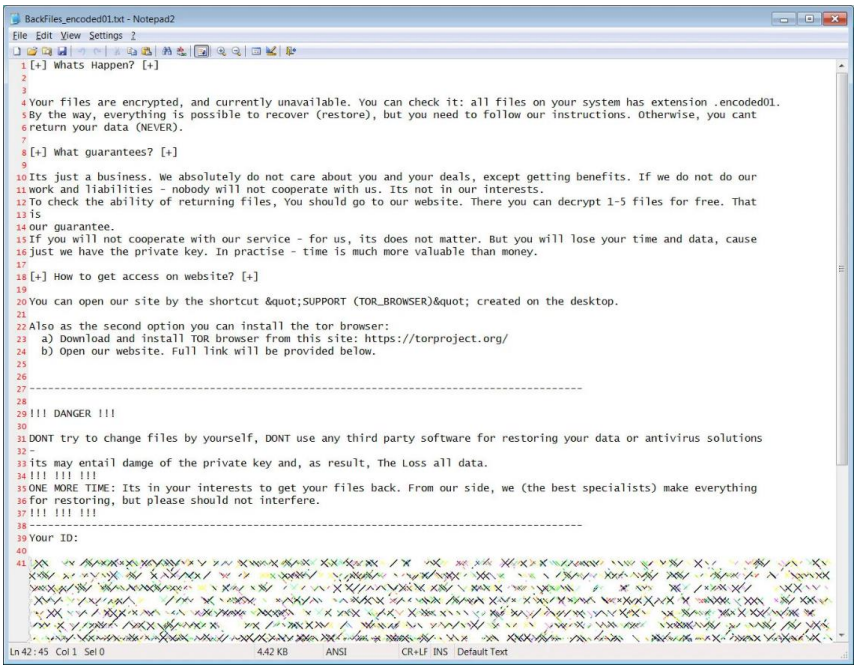


Figura 2. Archivos Cifrados y nota de rescate en referencia a SUGAR.
Fuente: Bleepingcomputer

V. INDICADORES DE COMPROMISO:

A continuación, se menciona indicadores de compromiso asociados a SUGAR:

Descripción	Detalle
MD5	17c7b47b68f75df9eec21698decad5b4
SHA1	a4854ce87081095ab1f1b26ff16817e446d786af
SHA256	4a97bc8111631795cb730dfe7836d0afac3131ed8a91db81dde5062bb8021058
SSDEEP	1536:WJ6miN/d+ucYLJrpTR/ky1lcSBdeKWFKVsu5jmZIFncKDCzHQvU/NjwGg64+:TmecYLN/ky1l1iClmZYfezHQvYdZ4+
Dominios	Bottomcdnfiles[.]com Cdnmegafiles[.]com d[.]onion sugarpanel[.]space
IP	179[.]43[.]160[.]195 82[.]146[.]53[.]237

Tabla 2. IOC de SUGAR

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-22	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	07-febrero-2022	**Ransomware Sugar**	Versión 1.0

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Tener actualizado un software anti-ransomware.
- Descargar programas y archivos de fuentes oficiales.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de información.
- En el caso de que la Organización/Institución se vea afectada por un ransomware, lo más importante es NO PAGAR nunca el rescate.
- Tener actualizado un software anti-ransomware.

VII. REFERENCIAS:

Abrams, L. (04 de 02 de 2022). *Bleepingcomputer*. Obtenido de Bleepingcomputer: https://www.bleepingcomputer.com/news/security/a-look-at-the-new-sugar-ransomware-demanding-low-ransoms/

EcuCERT. (03 de 02 de 2022). *EcuCERT*. Obtenido de EcuCERT: https://www.ecucert.gob.ec/wp-content/uploads/2022/02/EC-2022-20_PYSA_LOCKBIT_V1.pdf

Maltchev, S. (s.f.). Obtenido de https://groups.google.com/g/sci.crypt.research/c/ZD82NIacVmU/m/WDYm8_xmzTQJ?pli=1

Noticias de Seguridad Informática. (s.f.). Obtenido de Noticias de Seguridad Informática: https://noticiasseguridad.com/malware-virus/equipo-de-walmart-descubre-un-nuevo-ransomware-llamado-sugar/

Paganini, P. (02 de 02 de 2022). *Securityaffairs*. Obtenido de Securityaffairs: https://securityaffairs.co/wordpress/127545/malware/sugar-ransomware-a-new-raas-in-the-threat-landscape.html

Tutorialjinni. (06 de 02 de 2022). *Tutorialjinni*. Obtenido de Tutorialjinni: https://www.tutorialjinni.com/sugar-ransomware.html

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec