

ALERTA DE SEGURIDAD



CSIRT-RD

Equipo Nacional de Respuestas a Incidentes
Cibernéticos del CNCS

FECHA DE PUBLICACIÓN: 23 DE ENERO 2022

© Todos los derechos reservados



MINISTERIO DE LA PRESIDENCIA



CSIRT-RD

Equipo Nacional de Respuestas a Incidentes
Cibernéticos del CNCS



El presente documento es propiedad del Centro Nacional de Ciberseguridad (CNCS), y fue generado mediante el análisis de varias fuentes de terceras partes y una investigación del equipo CSIRT-RD.

ALERTA DE SEGURIDAD

- TLP Blanco
- Tipo de incidente Ransomware
- Categoría Código Malicioso
- Nivel de peligrosidad **CRITICO**

DETALLES DE ALERTA

El Equipo Nacional de Respuesta a Incidentes CSIRT- RD, comparte los indicadores de compromiso conocidos del Ransomware Hive, el cual funciona a través de Phishing con archivos maliciosos adjuntos y RDP para movimiento lateral.

INDICADORES DE COMPROMISO (IoC)

MD5

- b5045d802394f4560280a7404af69263
- 04FB3AE7F05C8BC333125972BA907398
- BEE9BA70F36FF250B31A6FDF7FA8AFEB

SHA256

- 321d0c4f1bbb44c53cd02186107a18b7a44c840a9a5f0a78bdac06868136b72c
- 1e21c8e27a97de1796ca47a9613477cf7aec335a783469c5ca3a09d4f07db0ff
- 3a402af7a583471187bf9fc7872560aaacf5e3d8c99ca5404c3f157c06fba454
- b214c1bbcc7b0c2a4a47134d6009594a4d30bd7d5e363a41603de6b5b8de18ca

Dominios Tor

- http[:]//hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd[.]onion
- http[:]//hivecust6vhkekztbqgdnkks64ucehqacge3dij3gyrrpdp57zoq3ooq[.]onion

Ejecutables

- Winlo.exe
- 7zG.exe
- Winlo_dump_64_SCY.exe

Otros IoCs

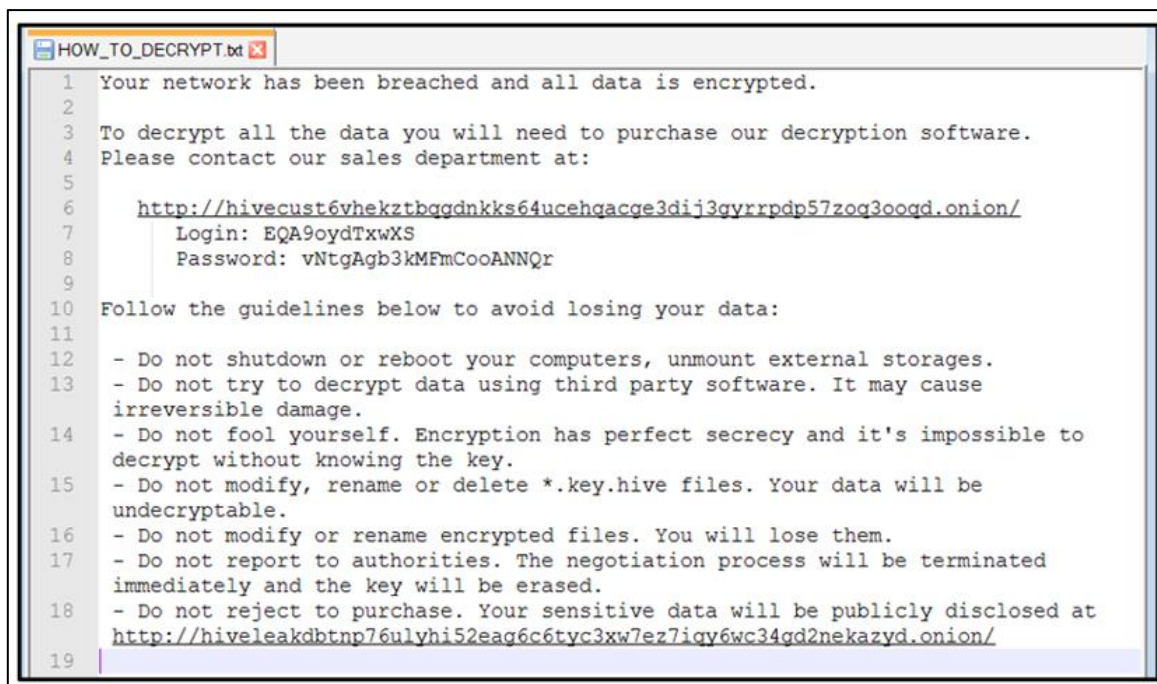
- *.key.hive
- *.key.*
- HOW_TO_DECRYPT.txt
- hive.bat
- shadow.bat
- vssadmin.exe delete shadows /all /quiet
- wmic.exe SHADOWCOPY /nointeractive
- wmic.exe shadowcopy delete
- wevtutil.exe cl system
- wevtutil.exe cl security
- wevtutil.exe cl application
- bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
- bcdedit.exe /set {default} recoveryenabled no

Funcionamiento

El ransomware Hive fue visto por primera vez en el 2021, este emplea una gran variedad de tácticas, técnicas y procedimientos (TTP), haciendo que las defensas sean más fáciles de evadir. Hive Ransomware utiliza el Phishing con archivos maliciosos adjuntos como entrada y luego utiliza RDP para realizar movimiento lateral. Durante el proceso de encriptado, los archivos afectados se renombran siguiendo este patrón: nombre de archivo original, cadena de caracteres aleatorios y extensión ".hive".

Mensaje de Rescate

Nota que explica a los usuarios el procedimiento para pagar el rescate de los datos comprometidos:



```
HOW_TO_DECRYPT.txt
1 Your network has been breached and all data is encrypted.
2
3 To decrypt all the data you will need to purchase our decryption software.
4 Please contact our sales department at:
5
6 http://hivecust6vhekztbqgdnkks64ucehgacge3dij3gyrrpdp57zoq3ooqd.onion/
7   Login: EQA9oydTxxXS
8   Password: vNtgAgb3kMFmCooANNQr
9
10 Follow the guidelines below to avoid losing your data:
11
12 - Do not shutdown or reboot your computers, unmount external storages.
13 - Do not try to decrypt data using third party software. It may cause
14   irreversible damage.
15 - Do not fool yourself. Encryption has perfect secrecy and it's impossible to
16   decrypt without knowing the key.
17 - Do not modify, rename or delete *.key.hive files. Your data will be
18   undecryptable.
19 - Do not modify or rename encrypted files. You will lose them.
20 - Do not report to authorities. The negotiation process will be terminated
21   immediately and the key will be erased.
22 - Do not reject to purchase. Your sensitive data will be publicly disclosed at
23   http://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqv6wc34gd2nekazyd.onion/
```

RECOMENDACIONES

1. Realizar el análisis correspondiente para el bloqueo a los indicadores de compromiso (IoC) citados en este documento.
2. Recomendamos tener precaución al momento de acceder a enlaces suministrados mediante medios de mensajería.
3. Mantener actualizadas las plataformas y sistemas de información según las recomendaciones del proveedor y en especial priorizar las actualizaciones para aplicaciones externas y servicios de acceso remoto.
4. Realizar contacto inmediato con el Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD), a través del correo incidentes@csirt.gob.do, para reportar cualquier acción sospechosa o posible incidente de ciberseguridad antes de realizar una acción.
5. Realizar campañas de concientización periódica a todos los usuarios de la institución.