

Incidente de Ciberseguridad

Fecha: 14/02/2024

Problemática: Corredor de Seguros S.A. de Guatemala sufrió incidente de seguridad

Correlativo: AC-0008

Institución / Sector: Privado

SITUACIÓN

El actor de amenazas «qilin ransomware», publicó evidencia de ciberataque a la empresa «Corredor de Seguros S. A. Guatemala», con lo cual podría realizar ciberextorsión para recuperar datos e información sensible de usuarios. Dicha empresa mantiene operaciones desde 1969 en Guatemala.

RIESGOS

- Cifrado y pérdida de información
- Afectación en la disponibilidad, integridad y confidencialidad de los sistemas
- Ciberextorsión
- Exfiltración de datos

RECOMENDACIONES A LOS USUARIOS

- Actualizar regularmente los sistemas y programas informáticos
- Realizar copias de seguridad de archivos y datos, en áreas geográficas distintas
- Implementar, monitorear y soluciones de ciberseguridad
- Verificar antes de abrir enlaces y archivos recibidos a través de correo electrónico u otro medio de mensajería instantánea

Nivel de priorización

Prioridad
Urgente / No Urgente
Urgente

Actualización
Seguimiento/Preventiva/Resiliente
Resiliente

Matriz de evaluación

Riesgo
Alto/Medio/Bajo
Alto

Nivel de Afectación

Integridad	Disponibilidad	Confidencialidad
Alto	Medio	Alto

ANEXO

Víctima: seguros

ID: 13286 detectado el 14-02-2024 10:33:52 por el grupo **qilin**

Descripción: No le queda mucho tiempo, la empresa decide ignorarnos, lo que significa que los datos estarán abiertos y disponibles para su descarga pública y gratuita.

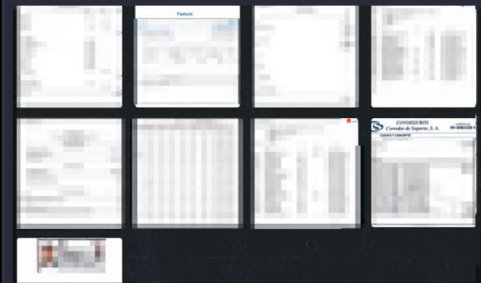
Hash de seguimiento: 6454c1e69cfaf841b687d781b476b6b0970187744acd3978d4e954101e5803b

Víctima ubicada en: Guatemala

Sitio web: consegueros.com.gt

Sector laboral:

[Pantalla] ^



REFERENCIAS

Fuente: RANSOMFEED https://ransomfeed.it/index.php?page=post_details&id_post=13286
Canal de extorsión «qilin» [http://kbsqoivihgdmwczmxkbovk7ss2dcynitwhhfu5yw725dboqo5kthfaad\[.\]onion](http://kbsqoivihgdmwczmxkbovk7ss2dcynitwhhfu5yw725dboqo5kthfaad[.]onion)
Sitio oficial Corredor de seguros S.A. <https://www.consegueros.com.gt/>