Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

# EL GRUPO DE RANSOMWARE LOCKBIT HA DISTRIBUIDO 1.5TB DE DATOS DEL BANCO SYARIAH INDONESIA (BSI)

*16 / mayo /2023*

# CONTENIDO

# INTRODUCCIÓN

El grupo de ransomware LockBit 3.0 quien habría cifrado y robado la información del Banco Syariah Indonesia (BSI) el 8 de mayo del 2023 ha decidido que el plazo a caducado y ha distribuido toda la información que habría recolectado de esta institución. El grupo indicaría que toda la información seria distribuida en la dark web, luego de que no se realizaran las peticiones en la nota de rescate que estos enviaran al grupo BSI, posterior a la violación de sus datos.

Así mismo el grupo provee “recomendaciones” a todos los clientes, cooperadores y miembros del BSI. Estas recomendaciones incluirían el cese al uso de los servicios de BSI así como acciones legales contra este, por parte de los clientes alegando la violación a la privacidad de la información.

## LOCKBIT RANSOMWARE

A continuación, se encuentra en cuadro de identificación de la amenaza.

| | |
|---|---|
| **ID de alerta:** | DSOC-CERT_2023_05_16_1 |
| **Clasificación de alerta:** | Noticia |
| **Tipo de Impacto:** | Alta |
| **TLP (Clasificación de información):** | **CLEAR** |
| **Fecha de publicación:** | 16/05/2023 |
| **Es día cero (0 day):** | No |

# EL ATAQUE

El grupo de ransomware LockBit 3.0, quien afirmara haber atacado el sistema informático de Bank Syariah Indonesia también conocida como BSI ha difundido esta mañana los datos cifrados de clientes y empleados, a través de la Dark Web. LockBit afirmó haber robado 15 millones de datos de clientes, información de empleados y alrededor de 1.5 TB de datos internos.

La cuenta de Twitter @darktracer_int ha publicado este 16 de mayo pruebas de los datos de BSI, así como la nota de apelación de LockBit contra este último. Según la cuenta “El periodo de negociación ha terminado, y el grupo ransomware Lockbit finalmente publicó todos los datos robados del Banco Syariah Indonesia en la dark web”.

El grupo de ransomware habría atacado a BSI el 8 de mayo del 2023, quienes como resultado habrían parado todas sus operaciones. Estos hacían saber a través de un comunicado que “El gerente del banco no pudo pensar en algo mejor que mentir descaradamente a sus clientes y colaboradores haciéndoles creer que el banco estaba atravesando una serie de trabajos técnicos”.


Imagen 1. Tweet desde la cuenta de @DarkTracer.

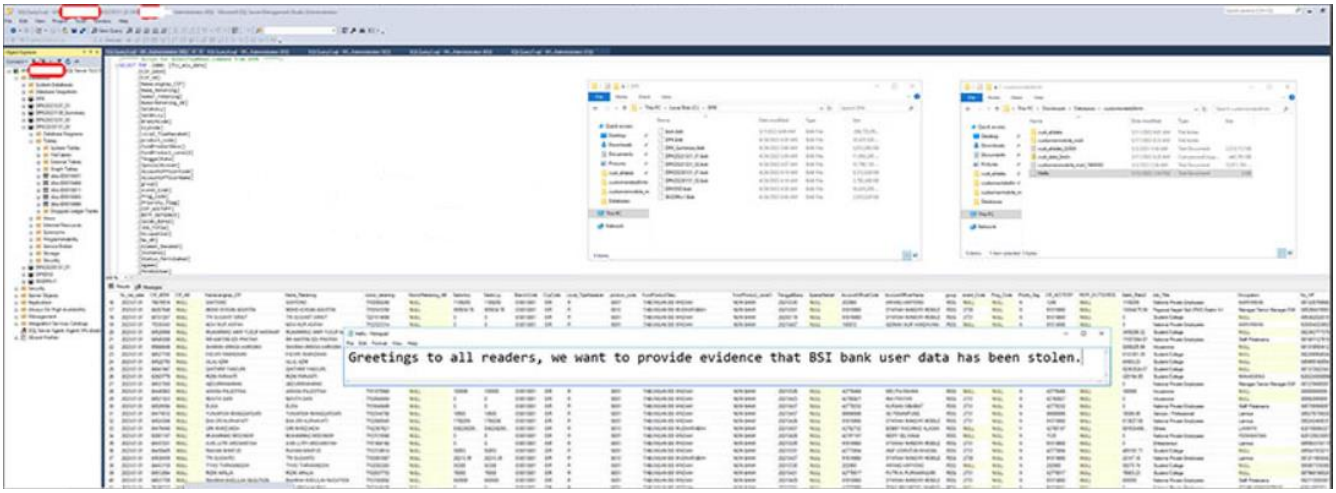


Imagen 2. Evidencia de información comprometida, compartida por LockBit.

## LA NOTA DE RESCATE

En la misiva, LockBit indicaba el hurto y cifrado de información, la cual rondaba los 1.5 TB, entre la información hurtada presumida por el grupo se encontraba:

- 9 bases de datos las cuales contenían la información de más de 15 millones de clientes y empleados, estos incluían: números de teléfono, direcciones, nombres, importes de cuentas, números de tarjetas, transacciones, entre otros.
- Documentos financieros.
- Documentos legales.
- Acuerdos de Confidencialidad (NDA).
- Contraseñas para todos los servicios internos y externos del banco.

En la carta, se le daba a BSI un periodo de 72 horas, para una respuesta, alegando que "si el banco valoraba su reputación, como a sus clientes y colaboradores" procederían a contactarlos antes del tiempo provisto.

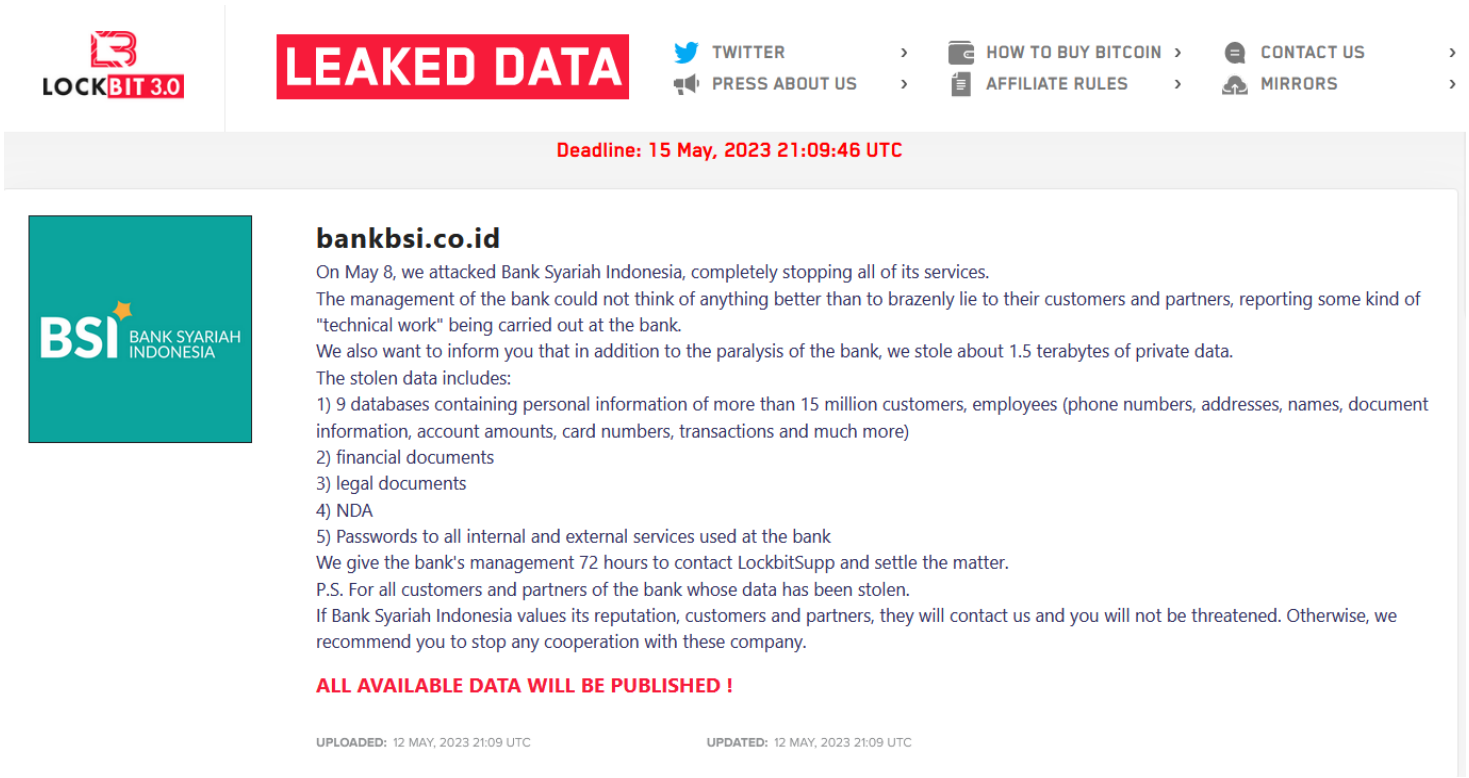


Imagen 3. Nota de exigencias de LockBit 3.0.

## FILTRACIÓN

Los afiliados de LockBit 3.0 usan Stealbit, una herramienta de exfiltración personalizada utilizada anteriormente con LockBit 2.0 [TA0010]; rclone, un administrador de almacenamiento en la nube de línea de comandos de código abierto [T1567.002]; y servicios de intercambio de archivos disponibles públicamente, como MEGA [T1567.002 ], para filtrar archivos de datos confidenciales de la empresa antes del cifrado. Si bien rclone y muchos servicios de intercambio de archivos disponibles públicamente se utilizan principalmente para fines legítimos, también pueden ser utilizados por actores de amenazas para ayudar a comprometer el sistema, explorar la red o la exfiltración de datos. Los afiliados de LockBit 3.0 a menudo utilizan otros servicios de intercambio de archivos disponibles públicamente para filtrar datos también [T1567].

| Sitios de File Sharing |
|---|
| https://www.premiumize[.] .com |
| **https://anonfiles[.] .com** |
| **https://www.sendspace[.] .com** |
| **https://fex[.] red** |
| **https://transfer[.] .sh** |
| **https://send.exploit[.] en** |

## LA DISTRIBUCIÓN

LockBit habría emitido declaraciones junto con la filtración de los datos. En la declaración de LockBit se hace notar la "recomendación a todos los clientes que están sufriendo la irresponsabilidad e incompetencia de esta gente". Siendo uno de los más importantes, el llamamiento a los clientes de BSI para que deje de usar los servicios de este. En palabras del grupo "Esta gente no sabe cómo proteger su dinero e información personal, de los delincuentes" llamando al grupo BSI "ladronzuelos" quienes "ni siquiera pudieron levantar su sitio en toda una semana, y solo pudieron mentirle en la cara a sus clientes, borrar comentarios en Twitter y que hacer crecer la barriga".

Entre otras demandas del grupo se encuentra qué:

- Los clientes dejen de utilizar los servicios de BSI e inclusive decirlo a familiares y amigos que dejen de usarlo.
- Que los clientes pidan una compensación a BSI por los problemas causados, apuntando corte y acciones legales contra BSI, alegando la violación de la privacidad de la información.

Los atacantes hacían notar que no divulgarían las vulnerabilidades en los sistemas de BSI y personal afectado, de manera que el grupo se "quedaría con una pequeña parte de los datos más interesantes para su posterior explotación".

# Index of /BANK_BSI/

| | |
|---|---|
| ../ | |
| 1. RCEO/ | 08-May-2023 11:25 |
| 1.a. Sekretaris/ | 08-May-2023 11:25 |
| 2. Retail Banking/ | 08-May-2023 11:25 |
| 2019_03/ | 08-May-2023 11:25 |
| 20230307T175250_SAE_DATA_BACKUP/ | 08-May-2023 11:25 |
| 3. Wholesale Banking/ | 08-May-2023 11:33 |
| 4. Financing Risk & Recovery/ | 08-May-2023 11:34 |
| 5. Financing Operation/ | 08-May-2023 11:34 |
| 6. Operational/ | 08-May-2023 11:37 |
| 7. Business Control/ | 08-May-2023 11:41 |
| 8. Funding & Transaction/ | 08-May-2023 11:41 |
| Berkas Rumah Dinas BSI/ | 08-May-2023 11:41 |
| Billy SME/ | 08-May-2023 11:55 |
| Dahlan/ | 08-May-2023 11:56 |
| Databases/ | 15-May-2023 20:50 |
| Dokumen Syarat Akad_19 Apr 2022/ | 08-May-2023 12:02 |
| Dokumentasi Area Bjm/ | 08-May-2023 12:02 |
| Dokumentasi Lama/ | 08-May-2023 12:02 |
| FILM/ | 08-May-2023 12:02 |
| Fahmi CBO/ | 08-May-2023 12:02 |
| ID CARD TAD BSM/ | 08-May-2023 12:03 |
| Marketing/ | 08-May-2023 12:03 |
| PERPANJANGAN SEWA ATM PELITA INSANI/ | 08-May-2023 12:03 |
| MEDALLION.zip | 08-May-2023 12:03 |

Imagen 4. Índice de los datos hurtados a BSI.

BSI BANK SYARIAH INDONESIA

**bankbsi.co.id**

Our recommendations to all customers who suffered from the irresponsibility and incompetence of these people:

1. Most importantly, stop using BSI. These people do not know how to protect your money and personal information from criminals. They couldn't even get their site up in a week. The best these little crooks can do is lie to their clients' faces, delete comments on Twitter and grow a belly.

2. Ask your family and friends to stop using BSI. This is an equally important point because our warning about this bank's irresponsibility will not reach all BSI customers.

3. BSI should compensate you for the trouble you have caused. If you find even a line about yourself (you will find it) - go to court, make class action lawsuits against BSI. They violated data privacy laws by leaking information and making you wait and worry while the "technical work" was going on, when they could have paid us and it would have worked the same day.

We did not disclose the vulnerability in BSI systems and the compromised bank staff, so we kept a small part of the most interesting data for ourselves for post-exploitation. See you soon.

BSI DATA:

[redacted]

P.S. About the correspondence attached to this post.
It's pretty stupid to think that in the time we spent on the BSI corporate network before we attack (about 2 months) we wouldn't have been able to find and steal everything we needed.

**ALL AVAILABLE DATA PUBLISHED !**

UPLOADED: 15 MAY, 2023 20:29 UTC UPDATED: 15 MAY, 2023 20:29 UTC

Imagen 5. Nota de LockBit tras la distribución de la información.

## RECOMENDACIONES

- Implemente un plan de recuperación que mantenga y conserve múltiples copias de datos confidenciales o de propiedad y servidores en una ubicación segura, segmentada y separada físicamente (es decir, disco duro, dispositivo de almacenamiento o la nube).
- Implemente la segmentación de la red y mantenga copias de seguridad fuera de línea de los datos para garantizar una interrupción limitada de la organización.
- Implemente contraseñas seguras, mas largas y con variación de caracteres.
- Mantenga actualizado todos los sistemas operativos, y software.
- Habilite la autenticación multifactorial, incluyendo medidas biométricas o los autenticadores de claves de dispositivos USB físicos en todos sus sistemas.
- Audite las cuentas de usuarios con privilegios administrativos y configure los controles de acceso, con el principio de privilegios mínimos.
- Desactive los puertos no utilizados.
- Vuelva a evaluar y simplificar los permisos de las cuentas de usuario, prestando especial atención a permisos asignados a usuarios endpoints y cuentas TI con permisos de administrador.
- Asegúrese de que todos los datos de copia de seguridad estén encriptados, sean inmutables.
- Borras las cuentas de usuarios desactualizados y/o no utilizadas, una revisión de los sistemas debería incluir la eliminación de estos puntos débiles.
- Examine el tráfico de red entrante y saliente, en busca de actividad sospechosa dentro de su red.
- Asegúrese de que todas las configuraciones del sistema sigan todos los procedimientos de seguridad. Los procedimientos operativos estándar se deben evaluar de manera periódica y así poder mantenerlos actualizados contra las amenazas emergentes.

## INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20230320_02_LockBitRansomware3.0

# CONTACTOS DE SOPORTE


**Correo electrónico:** cert@develsecurity.com

**Teléfonos directos:**

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

**Sitio Web:** https://www.devel.group/reporta-un-incidente