

# CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

**BANK OF AMERICA ADVIERTE A LOS CLIENTES  
SOBRE VIOLACIÓN DE DATOS DESPUÉS DE  
HACHEO A PROVEEDOR**

31 / 01 / 2024

## CONTENIDO

INTRODUCCIÓN .....	3
RESUMEN .....	5
INDICADORES DE COMPROMISO .....	7
NOTICIA COMPLETA .....	7
CONTACTOS DE SOPORTE .....	8

## INTRODUCCIÓN

Bank of America, uno de los principales bancos de Estados Unidos, ha emitido una advertencia a sus clientes sobre una violación de datos que expuso información personal sensible. La brecha ocurrió después de que Infosys McCamish Systems (IMS), uno de los proveedores de servicios de Bank of America, fuera hackeado el año pasado. La exposición incluye datos como nombres, direcciones, números de seguro social y detalles financieros, lo que plantea preocupaciones significativas sobre la seguridad de la información y la protección de los clientes.

## BANK OF AMERICA ADVIERTE A LOS CLIENTES SOBRE VIOLACIÓN DE DATOS DESPUÉS DE HACKEO A PROVEEDOR

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

ID de alerta:	DSOC-CERT_2024_02_13_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	<b>CLEAR</b>
Fecha de publicación:	13/02/2024
Es día cero (0 day):	No

## RESUMEN

Bank of América está advirtiéndolo a los clientes sobre una violación de datos que expuso su información personal después de que Infosys McCamish Systems (IMS), uno de sus proveedores de servicios, fuera hackeado el año pasado.

La información personal identificable (PII) de la cliente expuesta en la brecha de seguridad incluye los nombres de los individuos afectados, direcciones, números de seguro social, fechas de nacimiento e información financiera, incluidos números de cuenta y tarjeta de crédito, según detalles compartidos con el Fiscal General de Texas.

Bank of América sirve aproximadamente a 69 millones de clientes en más de 3,800 centros financieros minoristas y a través de aproximadamente 15,000 cajeros automáticos en los Estados Unidos, sus territorios y más de 35 países.

Si bien Bank of America aún no ha revelado cuántos clientes se vieron afectados por la violación de datos, una carta de notificación de violaciones de IMS presentada al Fiscal General de Maine en nombre de Bank of America reveló que un total de 57,028 personas fueron afectadas directamente.

"Alrededor del 3 de noviembre de 2023, IMS se vio afectada por un evento de ciberseguridad cuando un tercero no autorizado accedió a los sistemas de IMS, lo que resultó en la no disponibilidad de ciertas aplicaciones de IMS", dice la notificación de violación de datos.

"El 24 de noviembre de 2023, IMS informó a Bank of America que los datos relacionados con los planes de compensación diferida atendidos por Bank of America podrían haber sido comprometidos. Los sistemas de Bank of America no fueron comprometidos."

"Es poco probable que podamos determinar con certeza qué información personal se accedió como resultado de este incidente en IMS." era una continuación de la intrusión, posiblemente ejecutada por el mismo individuo o un colaborador dentro del grupo.

Ambos servidores de archivos recibieron el mismo tratamiento de desactivación de Windows Defender que el host original. Se estableció una conexión RDP con un servidor de respaldo y se ejecutaron los mismos comandos de desactivación. Luego, los atacantes prepararon un binario de ransomware en cada uno de los hosts a los que tenían acceso. Finalmente, lanzaron el ransomware Trigona en cada host a través de sus sesiones RDP.

Tras aproximadamente dos horas y 49 minutos desde el acceso inicial, el ransomware Trigona se ejecutó. Este ransomware no solo afectó al host donde se ejecutó inicialmente, sino que se propagó a todos los hosts accesibles a través del protocolo Server Message Block (SMB). El resultado: doble impacto de extorsión, con la exfiltración de datos sensibles y la cifrado de sistemas.

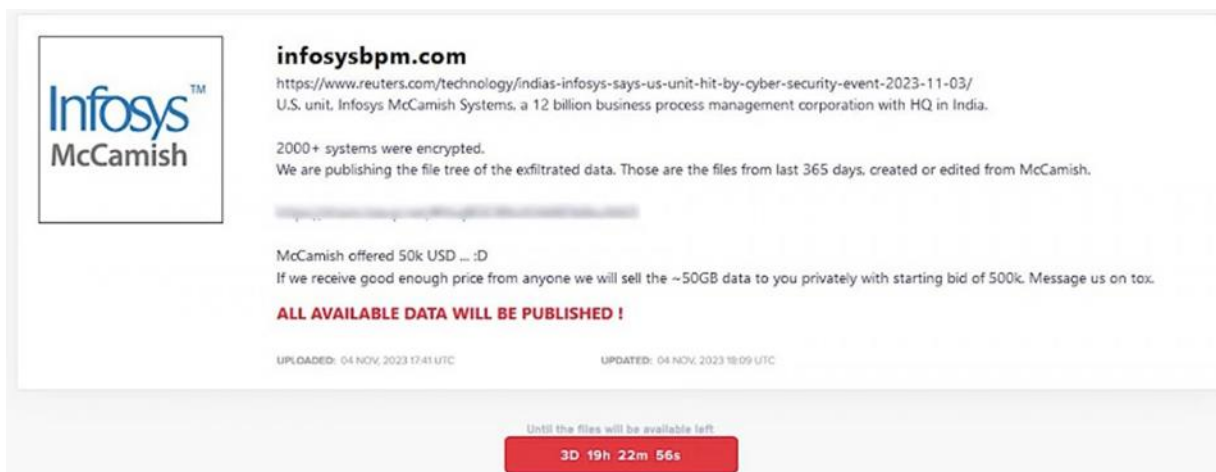
La violación de seguridad de noviembre llevó a una "no disponibilidad de ciertas aplicaciones y sistemas en IMS", como se explicó cuando se divulgó el incidente por primera vez en una presentación ante la Comisión de Bolsa y Valores de los Estados Unidos.

El 4 de noviembre, la banda de ransomware LockBit reclamó la responsabilidad del ataque a IMS, diciendo que sus operadores cifraron más de 2,000 sistemas durante la violación.

La operación de ransomware como servicio (RaaS) LockBit salió a la luz en septiembre de 2019 y desde entonces ha apuntado a muchas organizaciones de alto perfil, incluyendo Royal Mail del Reino Unido, el gigante automotriz Continental, la Ciudad de Oakland y el Servicio de Impuestos Internos de Italia.

En junio, las autoridades de ciberseguridad en los Estados Unidos y socios en todo el mundo publicaron un aviso conjunto que estima que la banda LockBit ha extorsionado al menos \$91 millones de organizaciones estadounidenses tras aproximadamente 1,700 ataques desde 2020.

Infosys, la empresa matriz de IMS, es una gigante multinacional de consultoría y servicios de TI con más de 300,000 empleados y clientes en más de 56 países.



The screenshot shows a ransomware note on a website. On the left is the 'Infosys McCamish' logo. The main text is as follows:

**infosysbpm.com**  
<https://www.reuters.com/technology/indias-infosys-says-us-unit-hit-by-cyber-security-event-2023-11-03/>  
U.S. unit, Infosys McCamish Systems, a 12 billion business process management corporation with HQ in India.

2000+ systems were encrypted.  
We are publishing the file tree of the exfiltrated data. Those are the files from last 365 days, created or edited from McCamish.

McCamish offered 50k USD ... :D  
If we receive good enough price from anyone we will sell the ~50GB data to you privately with starting bid of 500k. Message us on tox.

**ALL AVAILABLE DATA WILL BE PUBLISHED !**

UPLOADED: 04 NOV, 2023 17:41 UTC      UPDATED: 04 NOV, 2023 18:09 UTC

Until the files will be available left  
**3D 19h 22m 56s**

La información de la cuenta financiera de los clientes de Bank of America, tarjeta de crédito, seguro social y/o otros números de identificación únicos emitidos por el gobierno manejados por la firma de contabilidad líder Ernst & Young también se expusieron después de que la plataforma MOVEit Transfer del proveedor de servicios fuera hackeada en mayo de 2023 por la banda criminal cibernética Cl0p.

## INDICADORES DE COMPROMISO

[https://github.com/develgroup/SOC\\_IOCs/tree/main/20220506\\_01\\_LockBit](https://github.com/develgroup/SOC_IOCs/tree/main/20220506_01_LockBit)

## NOTICIA COMPLETA

<https://devel.group/blog/bank-of-america-advierte-a-los-clientes-sobre-violacion-de-datos-despues-de-hackeo-a-proveedor/>



## CONTACTOS DE SOPORTE



Correo electrónico: [cert@develsecurity.com](mailto: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>