Revisa las nuevas amenazas y consejos que presentamos a continuación.

⚠️ Nuevas Amenazas Detectadas

Tarjeta Bip! - Campaña Fraudulenta

Se trata de una página web falsa que se hace pasar por
la Tarjeta Bip! para robar datos de usuarios, utilizando ilegalmente sus logos e imagen.

Lo anterior constituye una falsificación de marca que podría afectar a usuarios, clientes y a la entidad aludida.

Detalles de la alerta

Código
ACF25-00085
Tipo de Alerta
Campaña Fraudulenta
Entidad o aplicación afectada
Tarjeta Bip!
TLP
TLP:CLEAR
Fecha de publicación
25 de agosto de 2025 a las 15:57
Fecha de última actualización
25 de agosto de 2025 a las 15:57

Actualización de cuenta bip! – Ajuste pendiente

ED equipo de bip! <mby47i93ds.274736@gmail.com>
Para [redacted]

Responder | Responder a todos | Reenviar | ...
dom 24-08-2025 18:39

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Estimado/a usuario/a,

Adjuntamos a este correo una factura correspondiente a un pequeño ajuste pendiente en su cuenta bip! por un monto de **$950 CLP**.

Factura en PDF

Le agradecemos su atención. Si ya ha realizado el pago, puede ignorar este mensaje.

Atentamente,
El equipo de bip!

1-click unsubscribe

bip! Servicios de Transporte
Av. Alameda 1234, Santiago, Chile
Tel: +56 2 1234 5678 | contacto@tarjetabip.cl

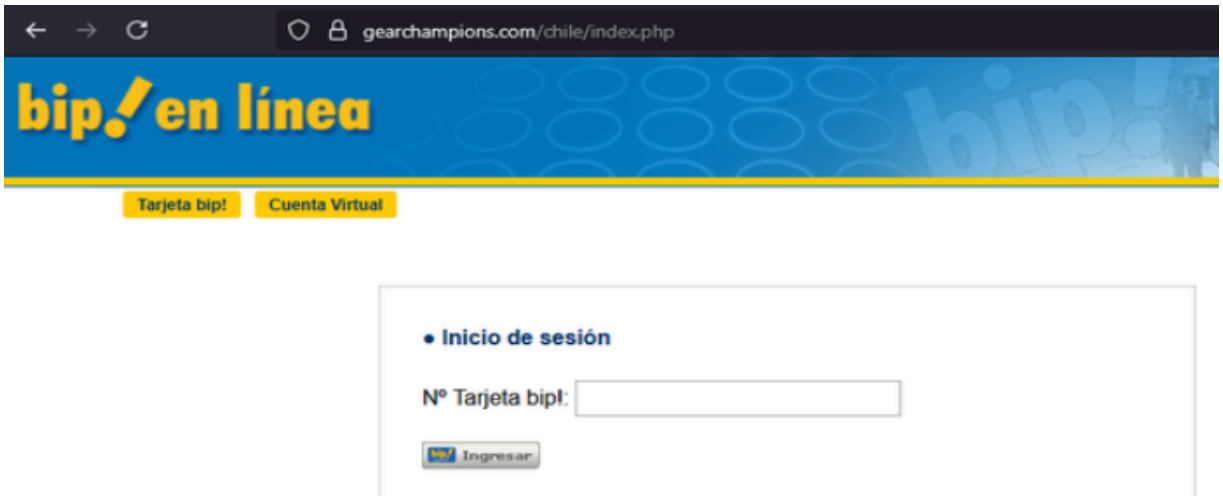
Factura de Ajuste de Cuenta

Fecha	21 de Agosto de 2025
Número de Factura	INV-20250821-001
Cliente	Usuario de tarjeta bip!
Monto Pendiente	$950 CLP
Estado	Pendiente de Pago

Gracias por utilizar nuestros servicios. Le recordamos que puede pagar este ajuste en nuestro portal oficial. Si ya ha realizado el pago, no se requiere ninguna acción adicional.

Hacer Pago Ahora

— bip! Servicios de Transporte



ANALISIS FORENSE

Valor	Comentario
Actualizacióndecuentabip!–Ajustependiente	Asunto Email
https://gearchampions.com/chile/index.php	URL sitio falso
https://go.contactpigeon.com/redir/138626367/78218079/	URL redirección
https://mailsrvecom-images.s3.amazonaws.com/private/7Xk32MXn/file1_1756072760%20%281%29.pdf	Falso documento
<mby47i93ds.274736@gmail.com	Correo de salida

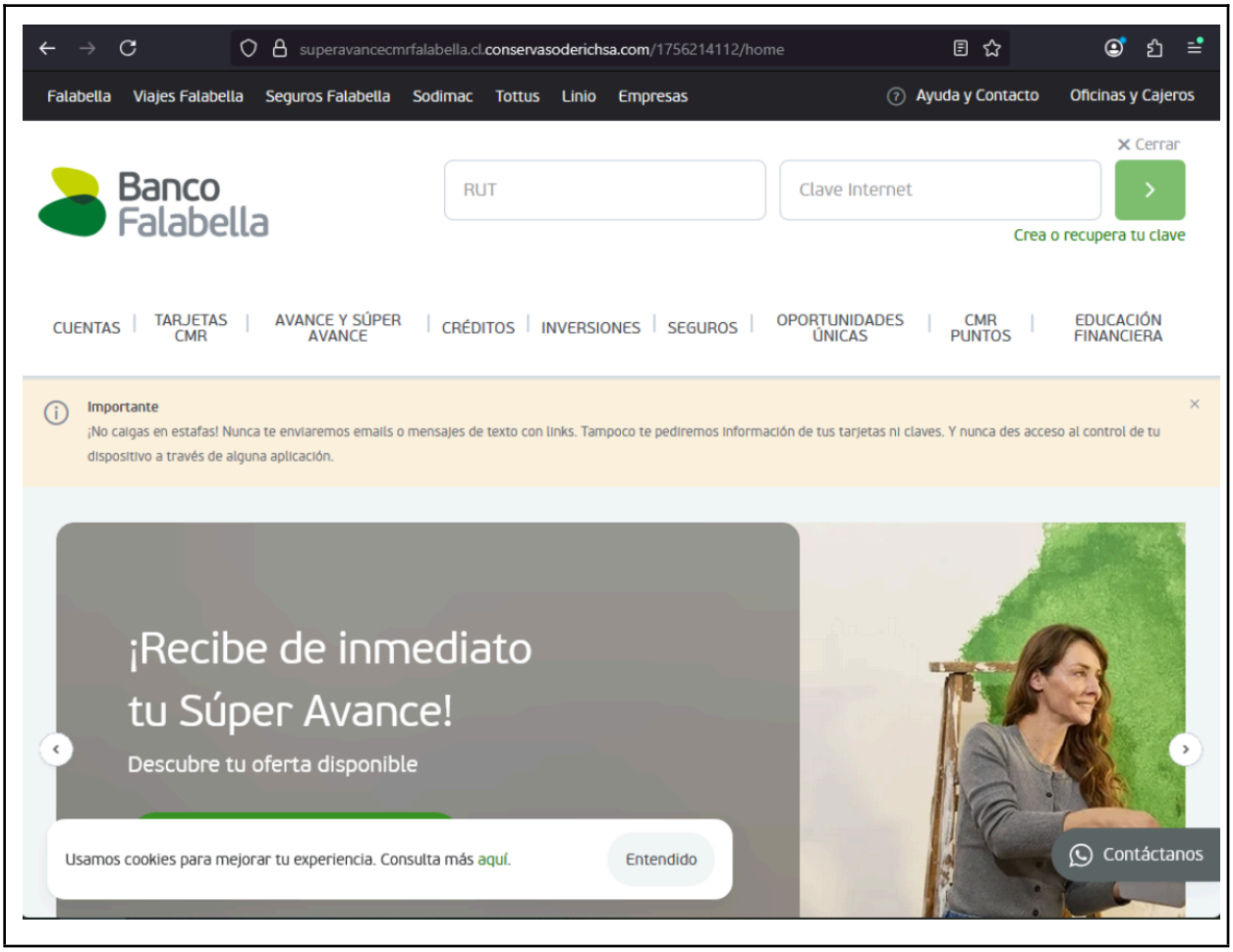
Banco Falabella - Campaña Fraudulenta

Se trata de una página web falsa que se hace pasar por Banco Falabella para robar datos de usuarios, utilizando ilegalmente los logos e imagen corporativa de dicha empresa.

Lo anterior constituye una falsificación de marca que podría afectar a usuarios, clientes y a la entidad aludida.

Detalles de la alerta

Código
ACF25-00086
Tipo de Alerta
Campaña Fraudulenta
Entidad o aplicación afectada
Banco Falabella
TLP
TLP:CLEAR
Fecha de publicación
26 de agosto de 2025 a las 12:18
Fecha de última actualización
26 de agosto de 2025 a las 12:18



ANALISIS FORENSE

Valor	Comentario
https://soscitizens.be/activacion/cuenta-test/	URL redirección
https://superavancecmrfalabella.cl.conservasoderichsa.com/1756214112/home	URL sitio falso

Lego - Campaña Fraudulenta

Se trata de una página web falsa que se hace pasar por Lego para robar datos de usuarios, utilizando ilegalmente los logos e imagen corporativa de dicha empresa.

Lo anterior constituye una falsificación de marca que podría afectar a usuarios, clientes y a la entidad aludida.

Detalles de la alerta

Código
ACF25-00086
Tipo de Alerta
Campaña Fraudulenta
Entidad o aplicación afectada
Banco Falabella
TLP
TLP:CLEAR
Fecha de publicación
26 de agosto de 2025 a las 12:18
Fecha de última actualización
26 de agosto de 2025 a las 12:18

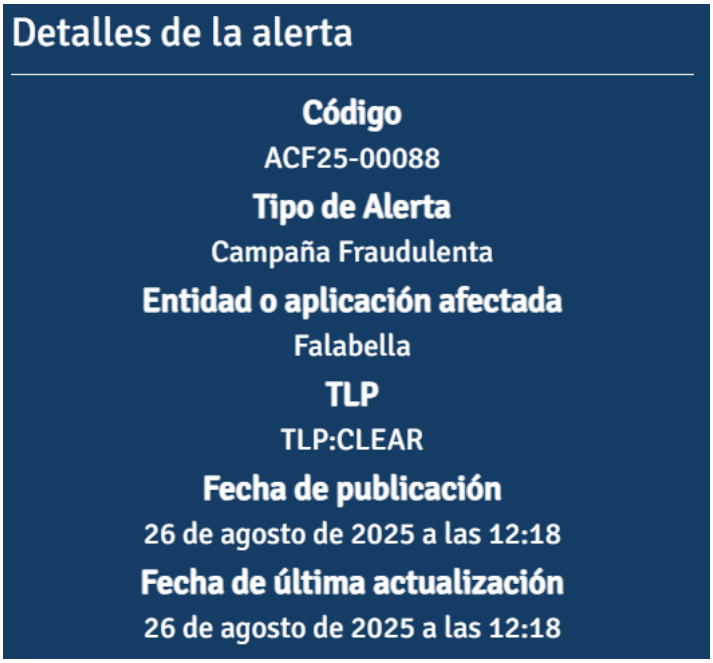
ANALISIS FORENSE

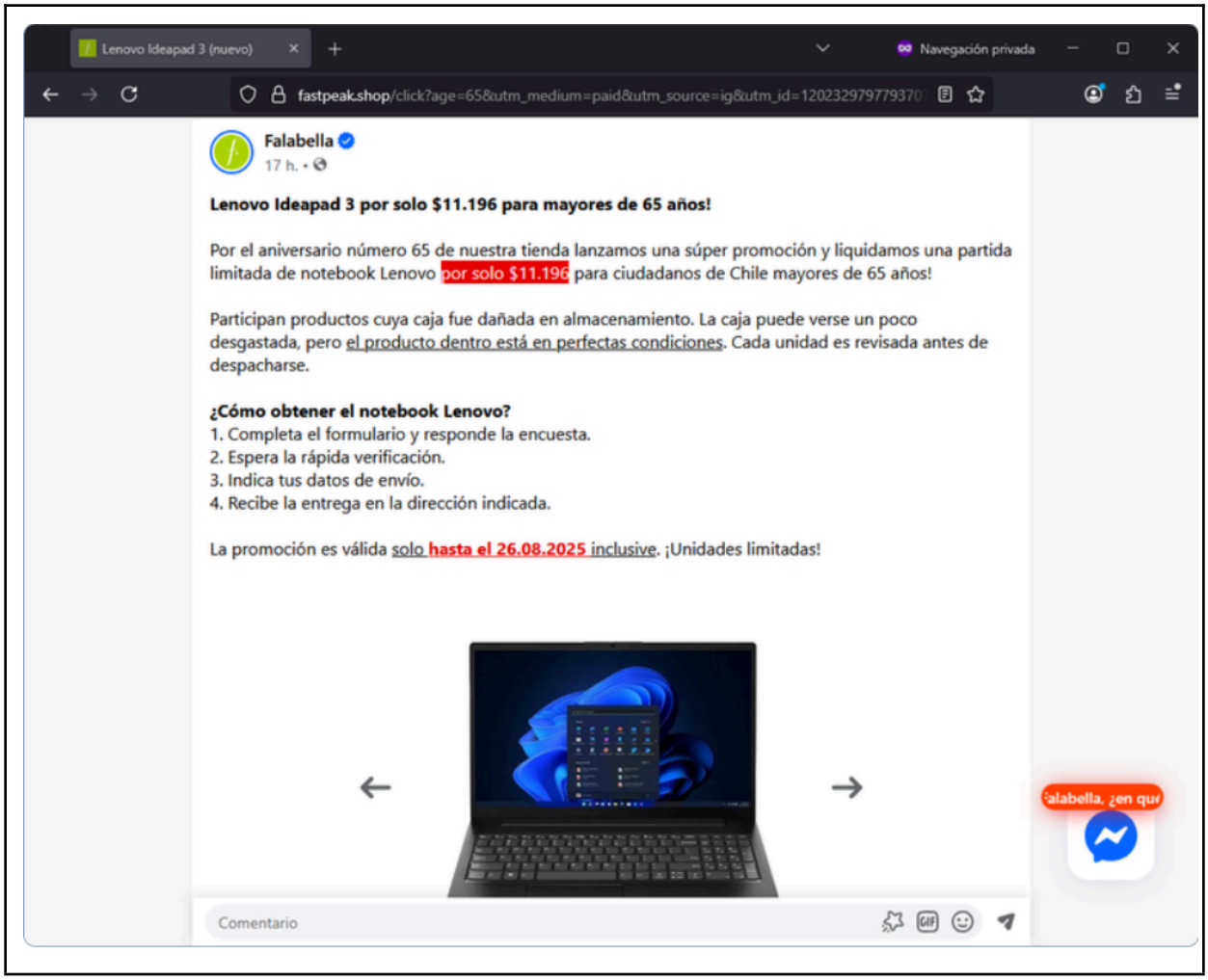
Valor	Comentario
https://sellafi.online/	URL sitio falso

Falabella - Campaña Fraudulenta

Se trata de una página web falsa que se hace pasar por Falabella para robar datos de usuarios, utilizando ilegalmente los logos e imagen corporativa de dicha empresa.

Lo anterior constituye una falsificación de marca que podría afectar a usuarios, clientes y a la entidad aludida.





ANALISIS FORENSE

Valor	Comentario
https://fastpeak.shop/	URL sitio falso

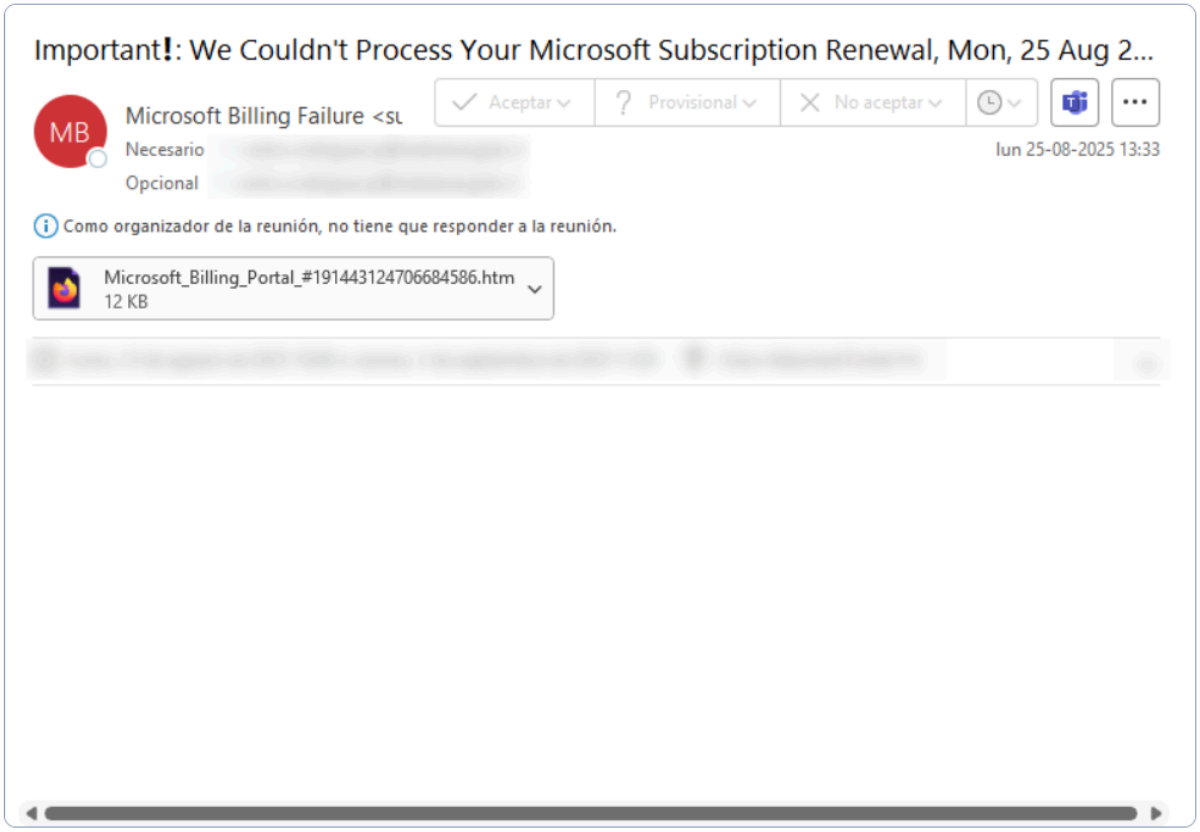
Microsoft - Campaña Fraudulenta

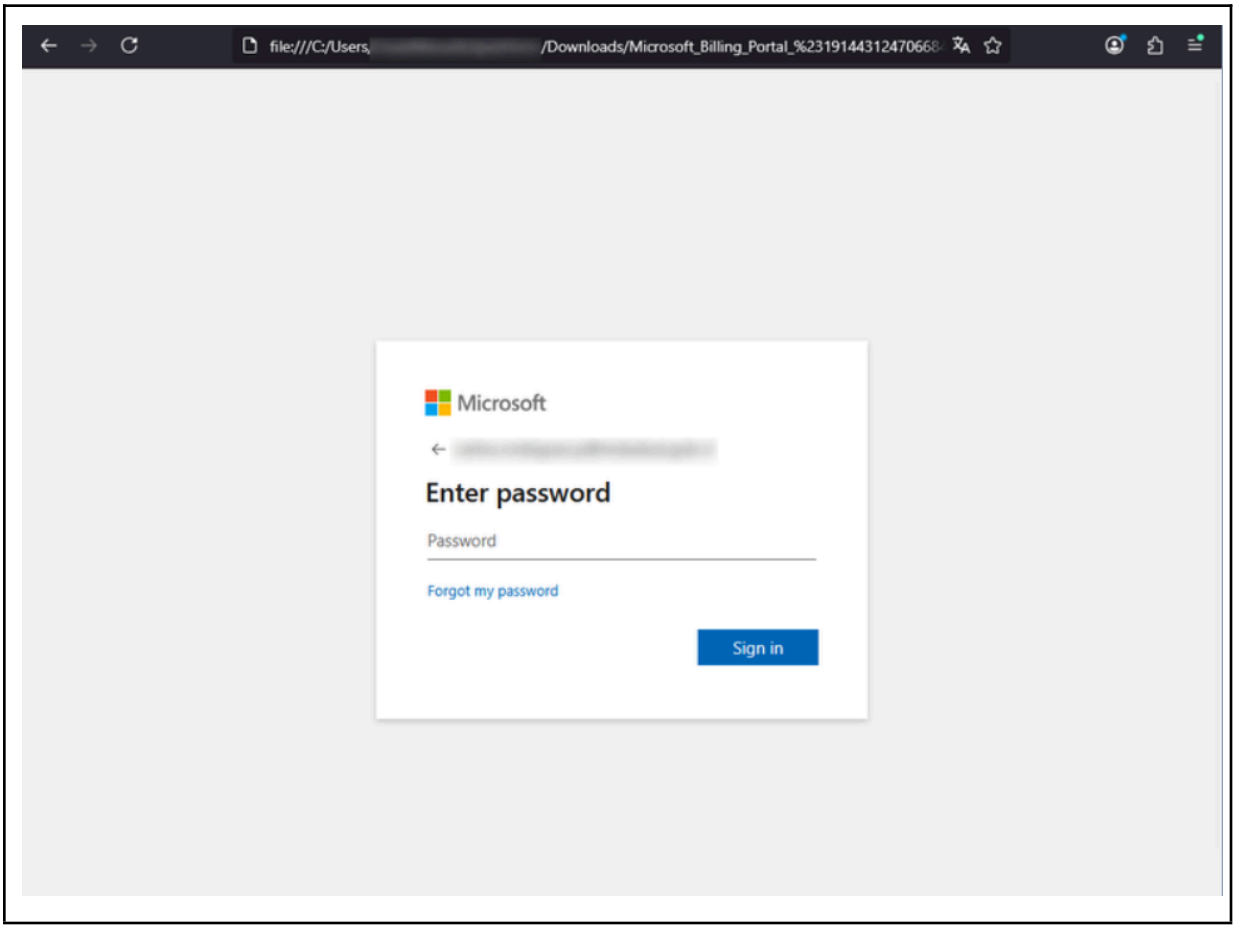
Se trata de una página web falsa que se hace pasar por Microsoft para robar datos de usuarios, utilizando ilegalmente los logos e imagen corporativa de dicha empresa.

Lo anterior constituye una falsificación de marca que podría afectar a usuarios, clientes y a la entidad aludida.

Detalles de la alerta

Código
ACF25-00089
Tipo de Alerta
Campaña Fraudulenta
Entidad o aplicación afectada
Microsoft
TLP
TLP:CLEAR
Fecha de publicación
26 de agosto de 2025 a las 12:17
Fecha de última actualización
26 de agosto de 2025 a las 12:17





ANALISIS FORENSE

Valor	Comentario
https://nhpfggop.emeluxewigs.co.za:8443/impact?cid8R7KWD8G={Correoelectronico}	URL sitio falso
Important ❗:WeCouldn'tProcessYourMicrosoftSubscriptionRenewal,Mon,25Aug202510:33:19-0700	Asunto Email
mmoraoseguera@support.captainhomes.ca	Correo de salida

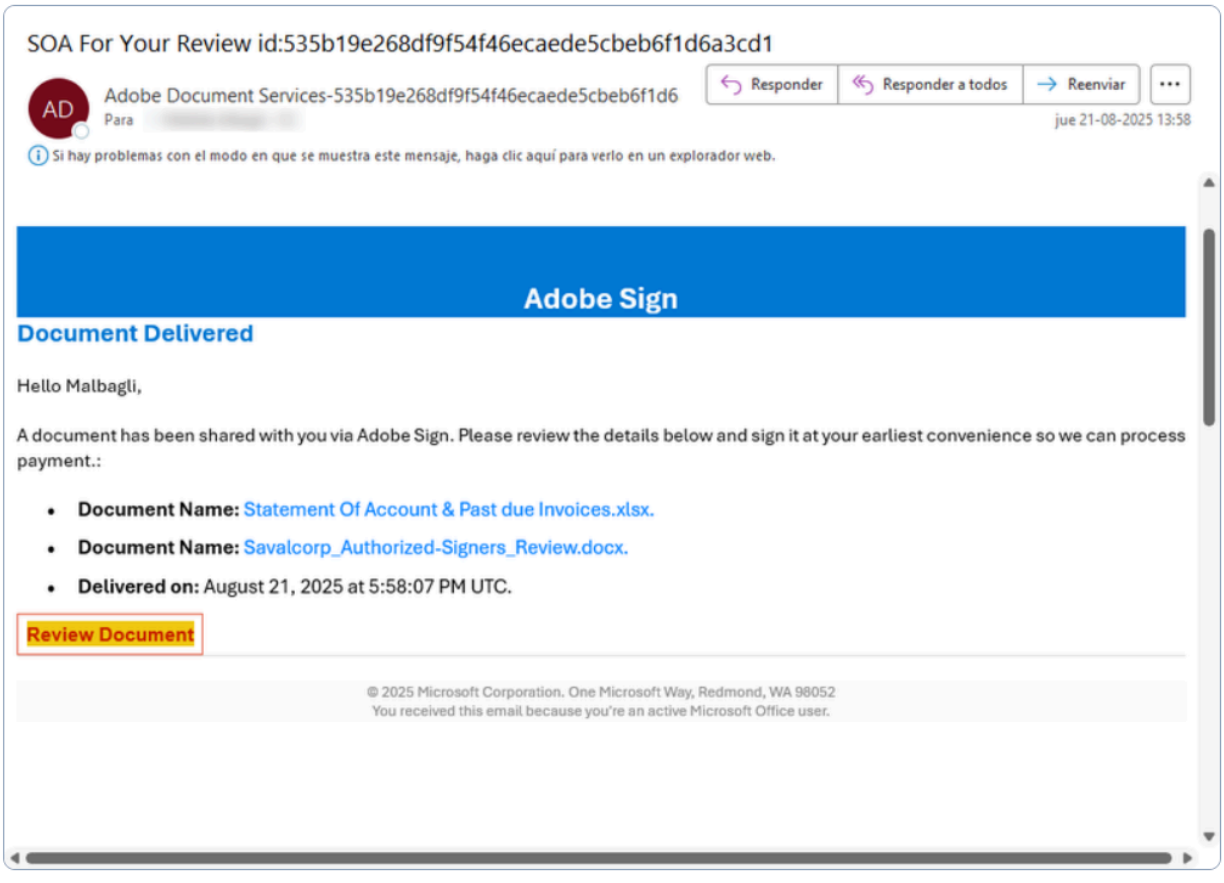
Microsoft - Campaña Fraudulenta

Se trata de una página web falsa que se hace pasar por Microsoft para robar datos de usuarios, utilizando ilegalmente los logos e imagen corporativa de dicha empresa.

Lo anterior constituye una falsificación de marca que podría afectar a usuarios, clientes y a la entidad aludida.

Detalles de la alerta

Código
ACF25-00090
Tipo de Alerta
Campaña Fraudulenta
Entidad o aplicación afectada
Microsoft
TLP
TLP:CLEAR
Fecha de publicación
29 de agosto de 2025 a las 08:38
Fecha de última actualización
29 de agosto de 2025 a las 08:38



ANALISIS FORENSE

Valor	Comentario
eronsman@palmwineboys.com	Correo de salida
https://agrutrou.stebugea.sa.com/jc@M2CG3c4rLB/${Correoelectrónico}	URL redirección
https://agrutrou.stebugea.sa.com/k5af3grrsq11?id=80cec29857dfbbd98-972bd2c1e64246-12cd2980ec9b8-0c1cf6bd471-67773fdcb8-4e563c6a04-3dab0c74d389b-068da64ec15b09c88aaca4	URL sitio falso
https://t.yesware.com/tt/2502560518384679c184679604337623c9594452/a98278710594448804543c809c846794/9488045f35e5944e594404aa60433762/abralliance.com/{Correoelectronico}	URL redirección

SOAForYourReviewid:535b19e268df9f54f46ecaede5cbeb6f1d6a3cd1	Asunto email

Consejos

Semanal	Permanente
No prestes tu celular desbloqueado. Muchas apps quedan abiertas y alguien puede enviarse información sensible en segundos.	1. Gestiona tus claves 2. Presta atención a las direcciones 3. Presta atención a las redes wifi 4. Instala las actualizaciones de seguridad de tu computador/teléfono 5. Respalda tu información