| | |
|---|---|
| Alerta de seguridad informática | 8FPH21-00432-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 06 de septiembre de 2021 |
| Última revisión | 06 de septiembre de 2021 |

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico que se hace pasar como proviene del Banco Ripley.

Con estos emails, el atacante busca persuadir a las personas para utilizar un enlace adjunto en el cuerpo del correo. Para ello, el mensaje del correo indica falsamente que su cuenta ha sido suspendida temporalmente y que por su seguridad acceda inmediatamente a la siguiente actualización de cuenta. Si las personas hacen clic en el enlace, son dirigidas a un sitio falso, donde se exponen al robo de datos confidenciales.

## Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

## Indicadores de compromiso

URL redirección:
http://rimtrome[.]com/activacion/cuenta-sqcz/

URL sitio falso:
https://forum.kmsinversiones[.]com/login

Asunto:
✓ Aviso Importante: Alerta Maxima de Seguridad

Correo electrónico
apache@marrowfive2.net

SMTP Host
[45.7.230.115]

# Otros antecedentes

## Certificado Digital

| | | |
|---|---|---|
| Fecha Valido | : | 31-08-2021 |
| Fecha Término | : | 29-11-2021 |
| Emitido | : | R3 |

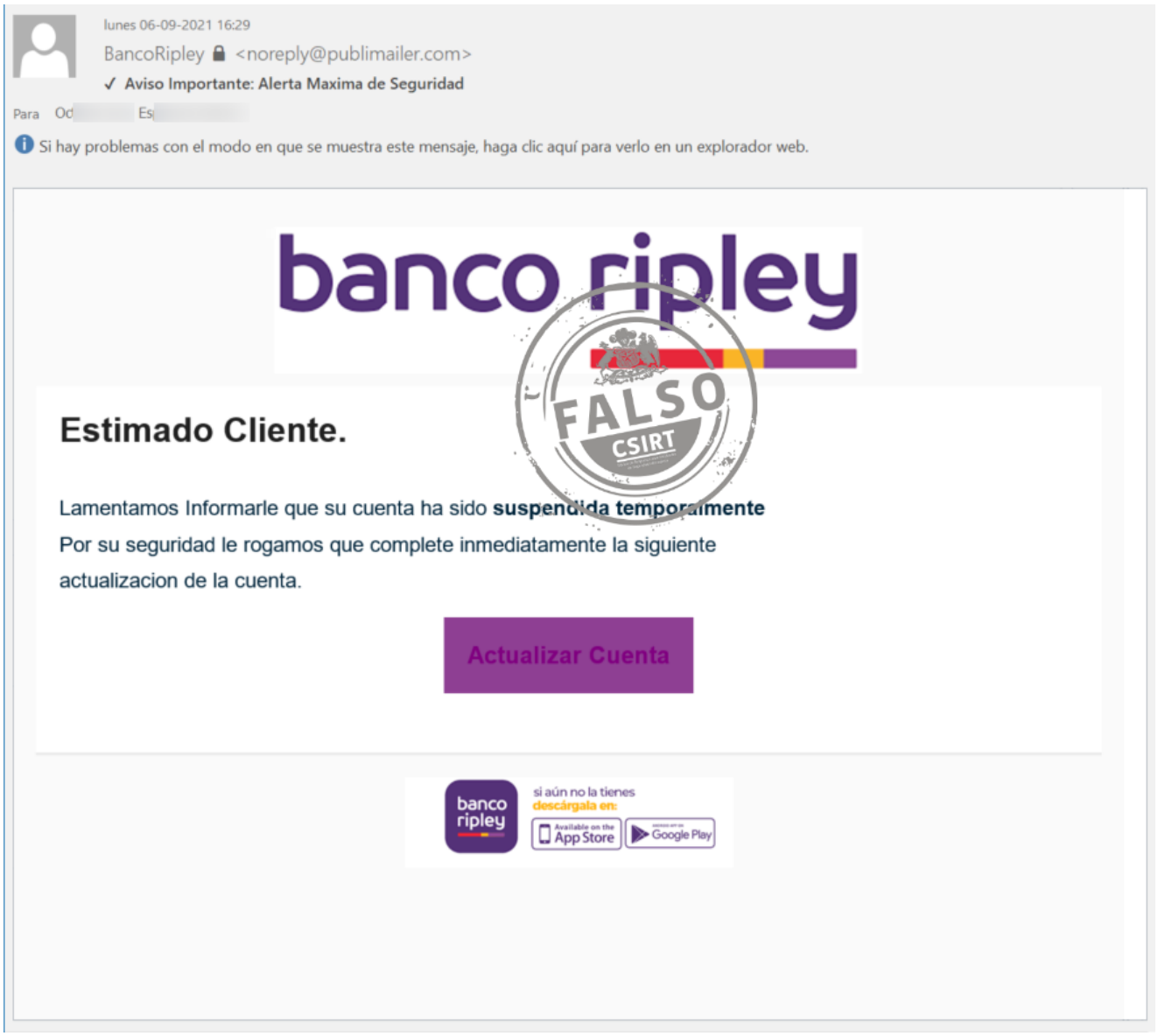
## Datos Alojamiento

| | | |
|---|---|---|
| IP | : | [192.141.51.210] |
| Número de sistema autónomo (AS) | : | 262256 |
| Etiqueta del sistema autónomo | : | Servicios Informaticos Hostname Ltda |
| País | : | CL |
| Registrador | : | LACNIC |

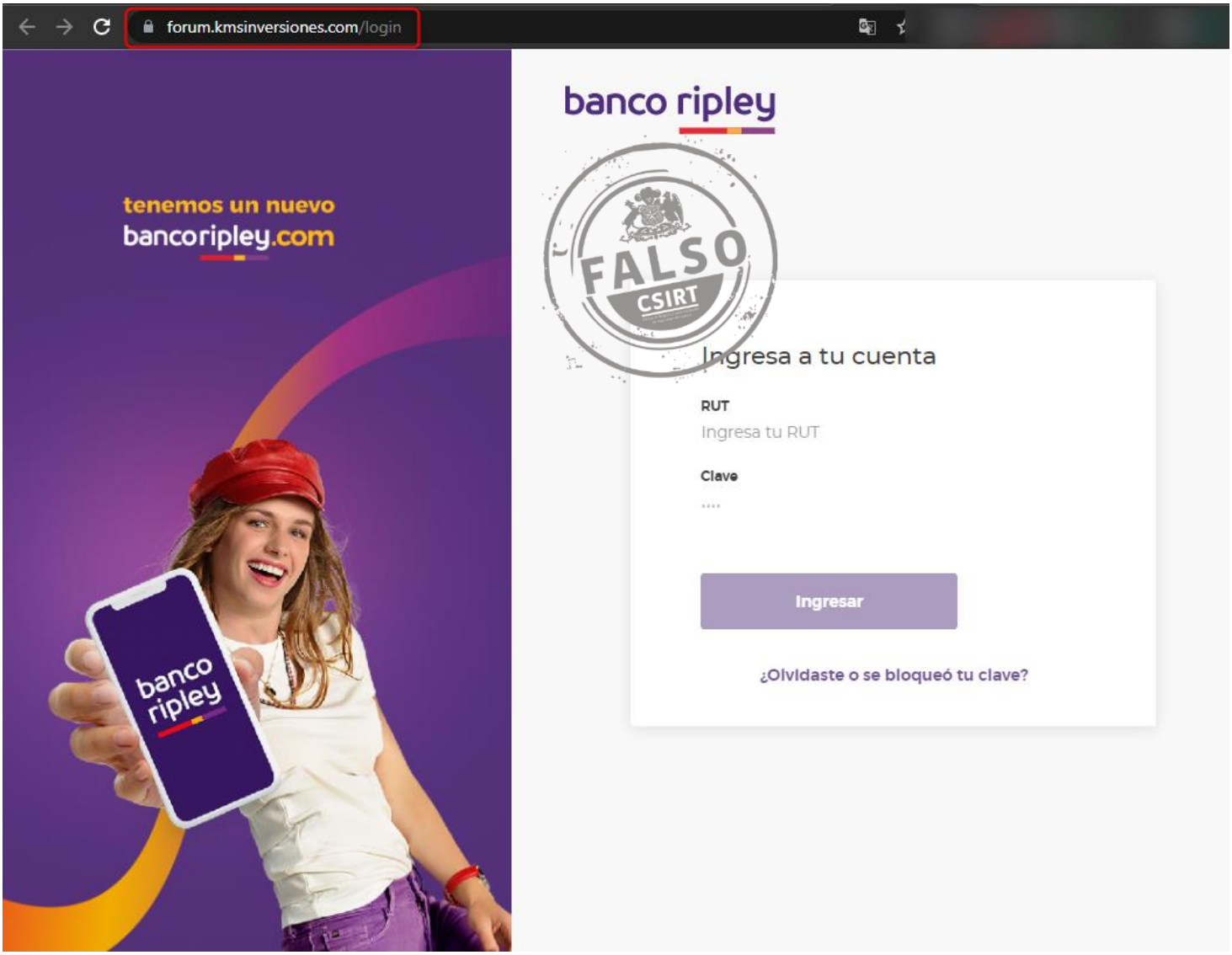
## Datos del Dominio

| | | |
|---|---|---|
| Nombre de dominio | : | kmsinversiones[.]com |
| Creado | : | 06-06-2021 |
| Expira | : | 06-06-2022 |
| Información del registrador | : | ENOM, INC. eNom, LLC |
| ID IANA | : | 48 |
| Correo electrónico | : | abuse@enom.com |
| Servidores de nombres | : | dns1.dnscl.net<br>dns2.dnscl.net |

# Imagen del mensaje



## Imagen del sitio



## Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.09.07 12:10:42 -03'00'