| | |
|---|---|
| Alerta de seguridad informática | 8FPH20-00318-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Phishing |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 19 de Octubre de 2020 |
| Última revisión | 19 de Octubre de 2020 |

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), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico que supuestamente proviene del Banco Estado.

El atacante busca persuadir a las personas para utilizar un enlace adjunto en el cuerpo del correo.

El mensaje del correo indica que por motivo de seguridad fue bloqueada su cuenta y que es necesario ingresar a su cuenta. Al seleccionar el enlace para ver más detalles es dirigido a un sitio falso, donde se expone al robo de sus credenciales.

## Observación

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

## Indicadores de compromiso

**Urls Redirección:**
http[:]//cetpline[.]com/Activacion/cuenta-dghq/

**Urls sitio falso:**
https[:]//valpanet[.]com/pichanaki/pagina/imagenes/comun2008/banca-en-linea-personas.html

**Smtp Host**
[45.7.230.89]

**Sender:**
apache@machine.net

**Asunto**
Fw: NOTIFICACION: CUENTA SUSPENDIDO

# Otros antecedentes

## URL Body SHA-256

338a24e2206d3b76f8a9c7364991fbada0908b7432c66a294645e7cc5f937d5d

## Certificado Digital

| | | |
|---|---|---|
| Fecha Valido | : | 23/07/2020 |
| Fecha Término | : | 27/07/2021 |
| Emitido | : | cPanel, Inc. Certification Authority |

## Datos Alojamiento

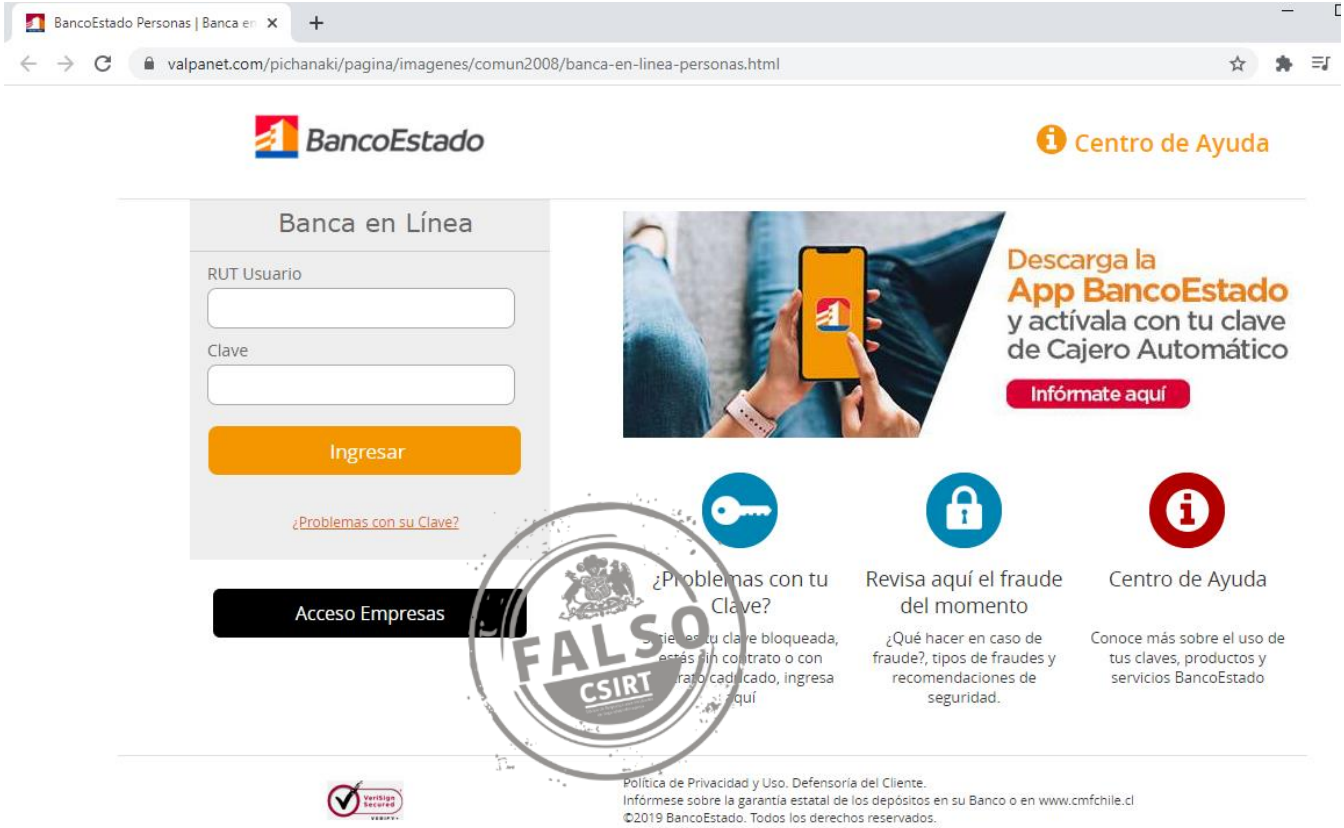
| | | |
|---|---|---|
| IP | : | 186.64.117.245 |
| Número de sistema autónomo (AS) | : | 52368 |
| Etiqueta del sistema autónomo | : | ZAM LTDA. |
| País | : | CL |
| Registrador | : | LACNIC |

## Datos del Dominio

| | | |
|---|---|---|
| Nombre de dominio | : | valpanet[.]com |
| Creado | : | 2014-07-12 |
| Expira | : | 2021-07-12 |
| Información del registrador | : | PDR Ltd. d/b/a PublicDomainRegistry.com |
| ID IANA | : | 303 |
| Correo electrónico | : | No aplica |
| Servidores de nombres | : | ns1.sitiodns.net<br>ns2.sitiodns.net<br>ns3.sitiodns.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: 2020.10.19 19:57:38 -03'00'