Alerta de seguridad informática	8FPH20-00264-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Julio de 2020
Última revisión	07 de Julio 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 de PayPal.

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

El mensaje del correo informa al receptor, que su cuenta fue temporalmente suspendida y para poder utilizarla debe ser activada nuevamente.

Al seleccionar el enlace para suuestamente reactivar la cuenta, la potencial víctima es dirigida a un sitio falso de PayPal, donde se expone al robo de sus credenciales.

Observación

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

Indicadores de compromiso

Urls sitio falso:
hxxps://dearcustmireservice[.]berdary[.]com/file/files

Sender
www-data[@]amzon[.]com

Smtp Host
[173.232.146.83]

Asunto
Confirm Your PayPal Account (Case ID #AL 032G 652 002)

Otros antecedentes

URL Body SHA-256

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Certificado Digital

Fecha Valido	:	05-04-2020
Fecha Termino	:	06-07-2020
Emitido	:	Let's Encrypt Authority X3

Datos Alojamiento

IP	:	88.99.75.142
Número de sistema autónomo (AS)	:	AS 24940
Etiqueta del sistema autónomo	:	Hetzner Online GmbH
País	:	Alemania
Registrador	:	RIPE NCC

Datos del Dominio

Nombre de dominio	:	berdary[.]com
Estado del dominio	:	clientTransferProhibited
Creado	:	18-04-2016
Expira	:	18-04-2021
Información del registrador	:	OpenTLD B.V.
ID IANA	:	1666
Servidores de nombres	:	NS3.AVISHOST.COM NS4.AVISHOST.COM

Imagen del mensaje

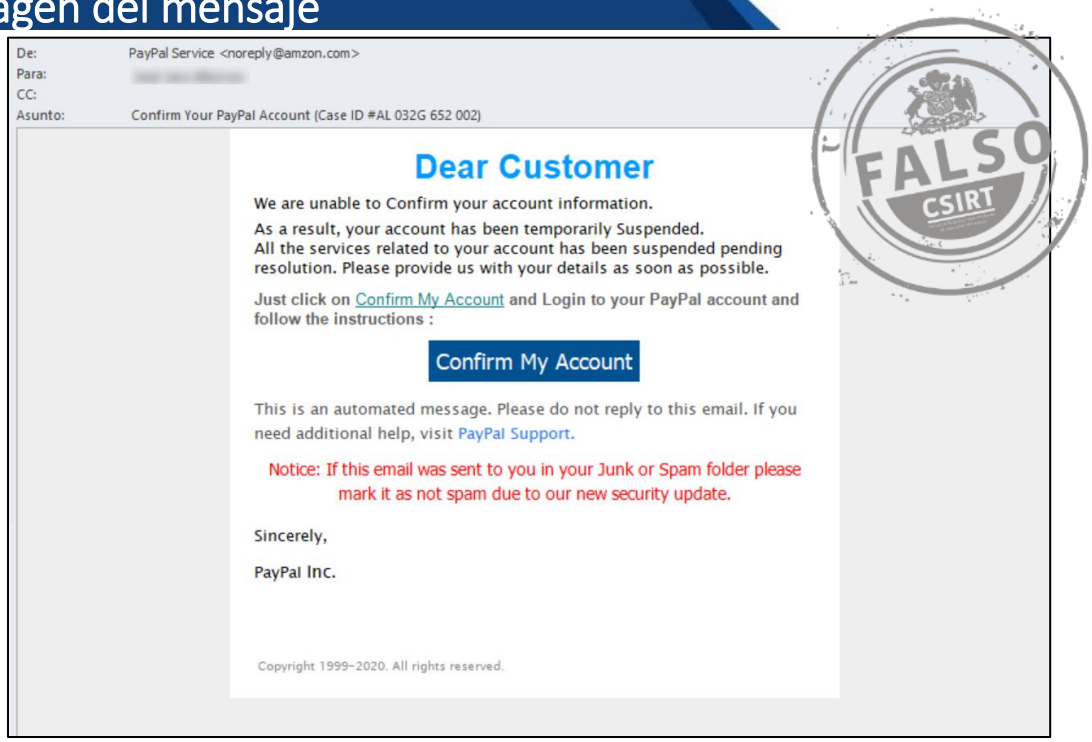
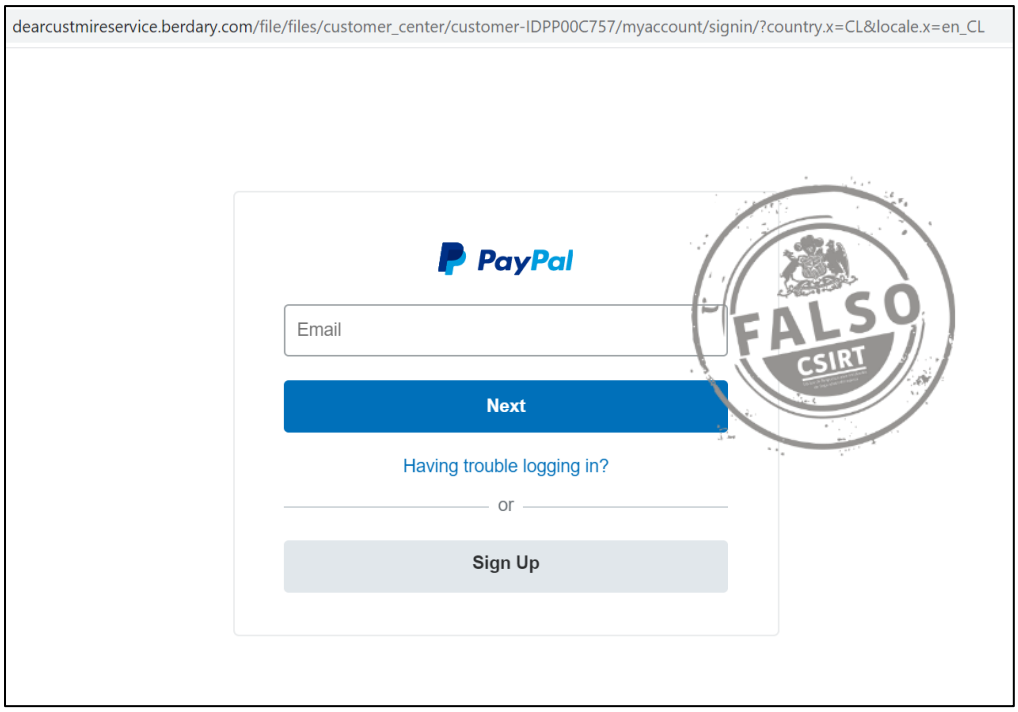


Imagen del sitio



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.