Alerta de seguridad cibernética	8FFR20-00797-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Octubre de 2020
Última revisión	13 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 fraude 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 fraude, 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), ha identificado la activación de un portal fraudulento asociado a un dominio que suplanta el sitio web oficial de PayPal, el que podría servir para robar credenciales de usuarios de esa entidad.

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

Indicadores de compromiso

Urls sitio falso

http[:]//da822325-313f-4f85-b334-d9b00a2d64da[.]htmlcomponentservice[.]com/get_draft?id=da8223_943e1deadfc8b224198f3740580b37aa[.]html

Body SHA-256

41fc409b9ee4e8f8339d904322dfa85e2ca3300377203aeb36bf4c68eff627da

Certificado Digital

Fecha Válido	No disponible
Fecha Término	No disponible
Emitido	No disponible

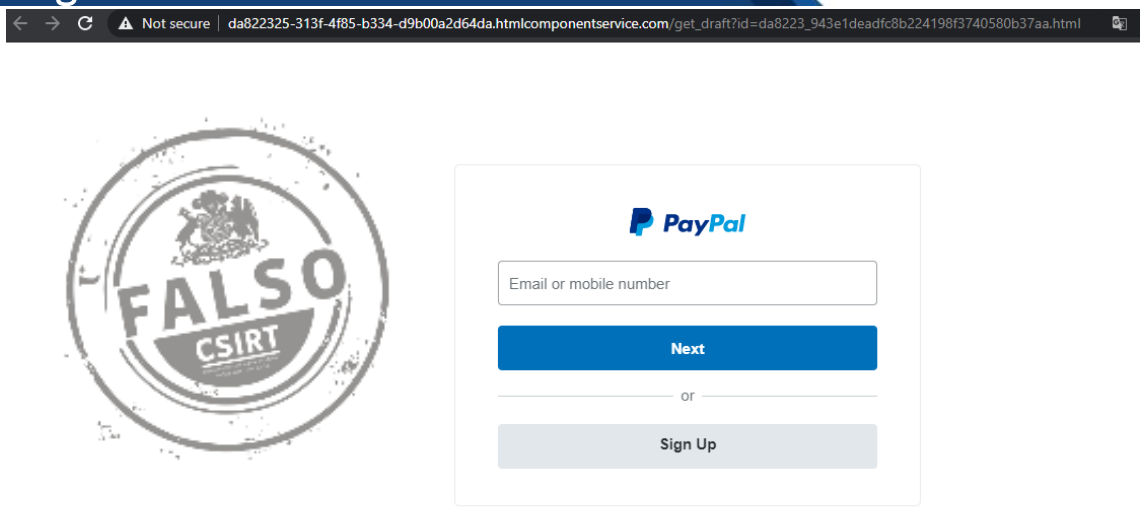
Datos Alojamiento

IP	64[.]233[.]191[.]121
Número de Sistema Autónomo (AS)	15169
Etiqueta del Sistema Autónomo	Google LLC
País	US
Registrador	ARIN

Datos del Dominio

Nombre de Dominio	HtmlComponentService[.]com
Estado del Dominio	ok
Creado	2016-01-09
Expira	2021-01-09
Información del Registrador	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
ID IANA	146
Correo Electrónico	Abuse@godaddy[.]com
Name Server	DNS1.P06.NSONE.NET DNS2.P06.NSONE.NET DNS3.P06.NSONE.NET DNS4.P06.NSONE.NET

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: 2020.10.13 19:48:04 -03'00'