Alerta de seguridad cibernética	8FPH20-00261-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de Julio de 2020
Última revisión	06 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 del servicio de streaming Netflix.

El atacante busca que las personas que reciben el mensaje utilicen el enlace adjunto.

El mensaje informa informa a las personas que lo reciben que su cuenta de Netflix ha caducado y se suspenderá dentro de 24 horas. Advierte que para evitar esto, el usuario debe actualizar su información.

Al seleccionar el enlace de actualizar la cuenta es dirigido a un sitio falso de Netflix, 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://iplanmyself[.]com/ads/assets/HE/FOVAAA/862112d0626a1372383b328ae7924c7f/

Sender
Postmaster[@]marijangudelj[.]com

Smtp Host
[51.15.20.168]

Asunto
✉ Confirma tu forma de pago

Otros antecedentes

URL Body SHA-256

f37cf194fe757525ca8f2929a57b542621845ccb09fa4a45e0aa89edd99773c2

Certificado Digital

Fecha Valido	:	13-05-2020
Fecha Termino	:	12-08-2020
Emitido	:	cPanel, Inc. Certification Authority

Datos Alojamiento

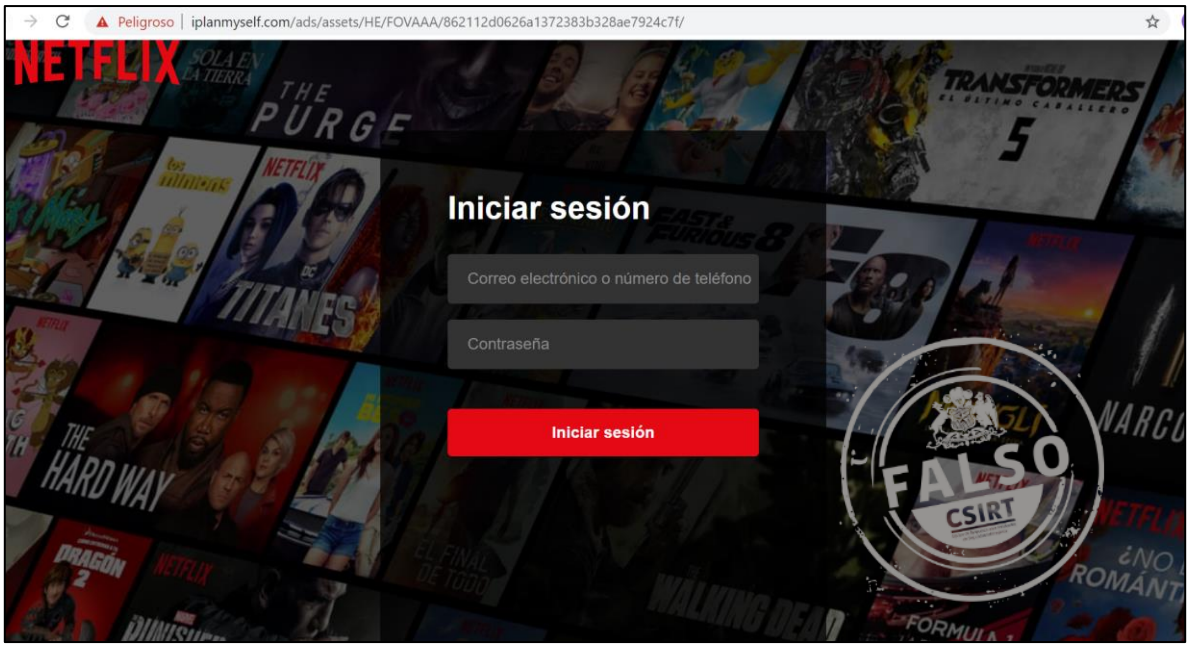
IP	:	166.62.56.228
Número de sistema autónomo (AS)	:	AS 26496
Etiqueta del sistema autónomo	:	GoDaddy.com, LLC
País	:	Estados Unidos
Registrador	:	ARIN

Datos del Dominio

Nombre de dominio	:	iplanmyself[.]com
Estado del dominio	:	clientDeleteProhibited clientRenewProhibited clientTransferProhibited clientUpdateProhibited
Creado	:	05-06-2013
Expira	:	05-06-2021
Información del registrador	:	GoDaddy.com, LLC
ID IANA	:	146
Correo electrónico	:	abuse@godaddy.com
Servidores de nombres	:	NS69.DOMAINCONTROL.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.