Alerta de seguridad informática	8FPH21-00366-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2021
Última revisión	04 de Febrero 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), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico que supuestamente proviene de Netflix.

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

El mensaje indica al usuario sobre la actualización de sus datos de la cuenta y sugiere la realización del proceso de verificación pues de lo contrario, advierte el mensaje, su servicio de Netflix por quedará temporalmente suspendida.

Al seleccionar el enlace para ver más detalles, las personas son dirigida 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:
hxxps://datingoneviral[.]com/.well-known/FAMOUSHOUSE/

Urls sitio falso:
hxxps://datingoneviral[.]com/.well-known/FAMOUSHOUSE/d23a5a94aa2bfc2592bbf5cf896ff54c/

Smtp Host
[112.78.125.36]

Asunto
Actualizar sus informaciones

Otros antecedentes

URL Body SHA-256

f37cf194fe757525ca8f2929a57b542621845ccb09fa4a45e0aa89edd99773c2

Certificado Digital

Fecha Válido	:	15-12-2020
Fecha Término	:	16-03-2021
Emitido	:	cPanel, Inc. Certification Authority

Datos Alojamiento

IP	:	[69.12.92.254]
Número de sistema autónomo (AS)	:	8100
Etiqueta del sistema autónomo	:	QuadraNet Enterprises LLC
País	:	US
Registrador	:	ARIN

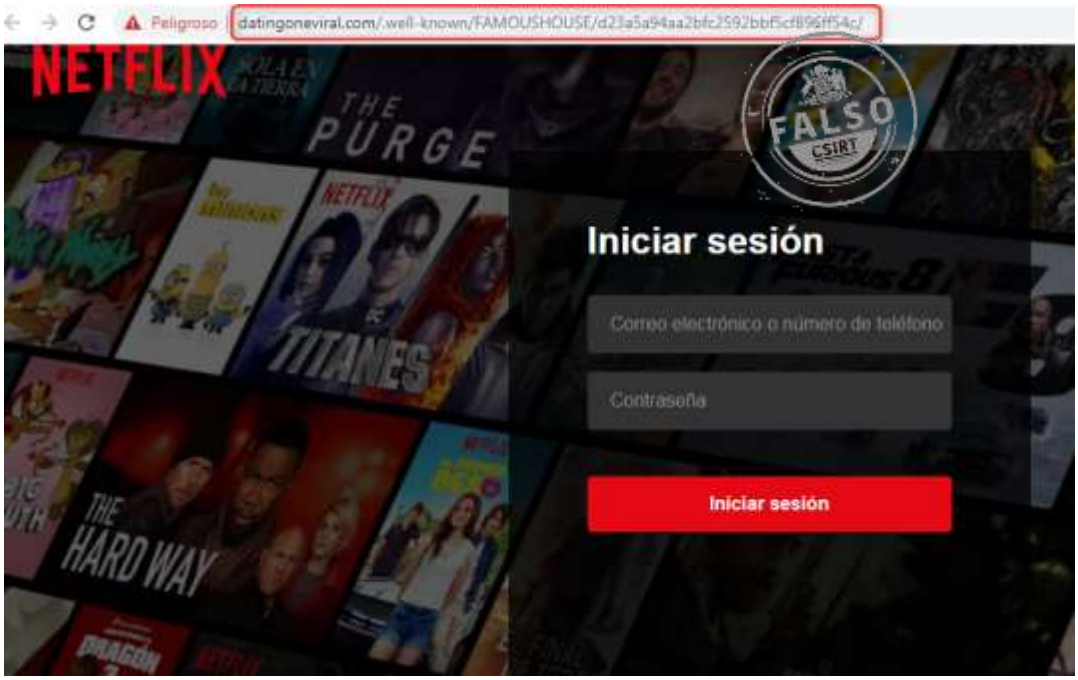
Datos del Dominio

Nombre de dominio	:	datingoneviral[.]com
Creado	:	2020-12-13
Expira	:	2021-12-13
Información del registrador	:	GoDaddy.com, LLC
ID IANA	:	146
Correo electrónico	:	abuse @fodaddy.com
Servidores de nombres	:	NS37.DOMAINCONTROL.COM NS38.DOMAINCONTROL.COM

Imagen del mensaje

Para: Usted

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.