Alerta de seguridad informática	8FPH20-00341-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Diciembre de 2020
Última revisión	15 de Diciembre 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 correo electrónico que supuestamente proviene del Banco Estado.

El atacante busca persuadir a las personas para utilizar un enlace adjunto.

El mensaje del correo indica que el Banco Estado ha actualizado los datos de seguridad y detectó un error en la información de la cuenta.

Al seleccionar el enlace para regularizar y activar la cuenta, la persona es 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:
http://ferreirainvestig.com[.]br/Activacion/cuenta-cdqd/

Urls sitio falso:
https://www.tenews.org[.]ua/cmfchile/pagina/imagenes/comun2008/banca-en-linea-personas.html

Asunto
Su Cuenta está temporalmente suspendida!

Smtp Host:
[186.64.121.153]
[45.236.130.202]

Sender:
apache@terno.com
apache@subterraneo.com

Otros antecedentes

URL Body SHA-256

338a24e2206d3b76f8a9c7364991fbada0908b7432c66a294645e7cc5f937d5d

Certificado Digital

Fecha Válido	:	02-12-2020
Fecha Término	:	02-03-2021
Emitido	:	Let's Encrypt

Datos Alojamiento

IP	:	195.201.34.52
Número de sistema autónomo (AS)	:	24940
Etiqueta del sistema autónomo	:	Hetzner Online GmbH
País	:	DE
Registrador	:	RIPE NCC

Datos del Dominio

Nombre de dominio	:	tenews.org[.]ua
Creado	:	12-09-2016
Expira	:	12-19-2021
Información del registrador	:	Hosting Ukraine LLC
ID IANA	:	
Correo electrónico	:	domain@abuse.tea,
Servidores de nombres	:	ns118.inhostedns.com ns218.inhostedns.ne ns318.inhostedns.org

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.