Alerta de seguridad cibernética	8FPH20-00230-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Mayo de 2020
Última revisión	25 de Mayo 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, ha identificado una campaña de phishing a través de un email que intenta suplantar al administrador de la cuenta de correo del usuario.

El atacante intenta persuadir a la víctima para utilizar un enlace en el cuerpo del correo.

El mensaje indica una supuesta retención de los correos entrantes de la casilla del usuario producto de actualizaciones que se están realizando para mantener segura la cuenta, pero solicita que el usuario restaure la cuenta para recibir los correos entrantes.

Para realizar la supuesta actualización, la persona debe ingresar a un enlace. Al seleccionarlo, la víctima es dirigida a un sitio falso del correo corporativo dónde se expone a la pérdida de sus credenciales de la cuenta de correo.

El correo no indica el nombre de la entidad administradora, tiene deficiencias en su redacción y puntuación.

Observación

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

Indicadores de compromiso

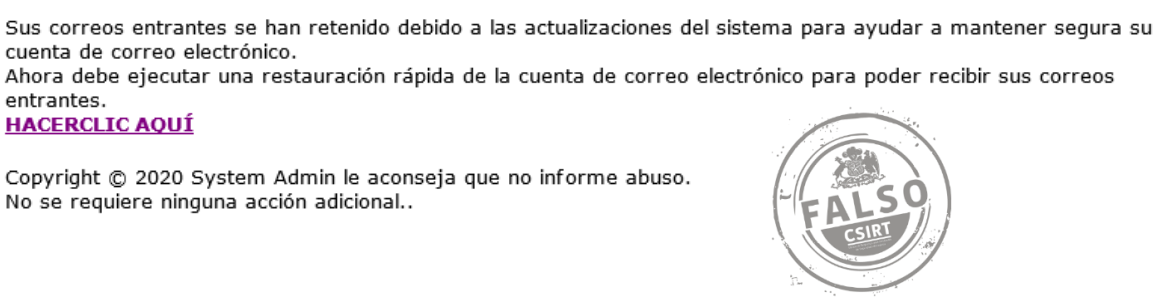
Urls sitio falso:
hxxps://kwiksurveys[.]com/s/QKTYAyRJ#/0

Smtp Host
[212.5.159.59]

Sender
dppbulgarka@iag.bg

Asunto
ÚLTIMA ADVERTENCIA

Imagen del mensaje


Sus correos entrantes se han retenido debido a las actualizaciones del sistema para ayudar a mantener segura su cuenta de correo electrónico.
Ahora debe ejecutar una restauración rápida de la cuenta de correo electrónico para poder recibir sus correos entrantes.
HACERCLIC AQUÍ

Copyright © 2020 System Admin le aconseja que no informe abuso.
No se requiere ninguna acción adicional..

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 q ue se ingresen sean los oficiales.