Alerta de seguridad cibernética	8FPH20-00183-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de Abril de 2020
Última revisión	17 de Abril 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 proviene de una organización supuestamente denominada Departamento de la Oferta Mundial de Promociones de Lotería la que actúa junto a una popular Lotería de EEUU.

El mensaje busca generar una respuesta de quien lo recibe a una casilla enmascarada entregada por el remitente.

El mensaje del correo informa a la víctima que fue ganador de la lotería realizada el pasado 28 de marzo y distribuye premios para familias e individuos afectados para sobrevivir a la pandemia de Covid-19. Para cobrar el premio de 500 mil dólares americanos, el receptor debe responder el correo indicando los números ganadores. La cantidad de dinero expresada en palabras tiene un error, pues el monto escrito es “cincocientos mil”, lo que podría suponer el uso de un traductor en la elaboración del mensaje. La narrativa es a veces extraña y reiterativa, por ejemplo, al mencionar la fecha en que fue realizado el sorteo, indicada al principio y final de un breve párrafo.

El correo se recibe desde la casilla jewellann.harry[@]caricom[.]org, pero al enviar la respuesta, ésta es enviada al correo “bwann1977[@]gmail[.]com”.

OBSERVACIÓN

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

INDICADORES DE COMPROMISO

Email fraudulento:
bwann1977[@]gmail[.]com

Smtp Host
[83.222.24.66]
[83.222.12.21]

Sender
jewellann.harry[@]caricom[.]org

Asunto
NOTIFICACIÓN DE ADJUDICACIÓN; NOTICIA FINAL

IMAGEN DEL MENSAJE

RE / NOTIFICACIÓN DE ADJUDICACIÓN; NOTICIA FINAL

Betty Nwann <jewellann.harry@caricom.org>

PROMOCIÓN MUNDIAL DE LOTERÍA EN CONJUNCIÓN CON POWERBALL LOTTERY BS ESTADO UNIDO, ESTADOS UNIDOS.
DE: EL DEPARTAMENTO DE LA OFERTA MUNDIAL DE PROMOCIONES DE LOTERÍA POR CORREO ELECTRÓNICO,
REF: OYL / 26510460037/02
NÚMERO GANADOR: 02, 37, 39, 48, 48, 05
FECHA DE GANANCIA: 08 de abril de 2020

ATENCIÓN: Usuario de correo electrónico

RE / NOTIFICACIÓN DE ADJUDICACIÓN; NOTICIA FINAL

Nos complace informarle sobre el anuncio hoy, 28 de marzo de 2020, de los ganadores de nuestra lotería de promoción por correo electrónico a través de: WORLD PROMO LOTTERY INTERNATIONAL EN CONJUNCIÓN CON LOS PROGRAMAS DE LOTERÍA DE POWERBALL que se realizó el 28 de marzo de 2020.
Su dirección de correo electrónico se adjunta a El número de boleto 023-0148-790-459, con el número de serie 5073-11, sacó los números de la suerte 02, 37, 39, 48, 48, 05 y, en consecuencia, ganó la lotería en la tercera categoría.

Este programa de lotería es para ayudar a familias e individuos a sobrevivir a la epidemia en curso de COVID 19 (Corona Virus Pandemic).
Por lo tanto, se le ha aprobado un pago global de US $ 500.000.00 (cincocientos mil dólares estadounidenses) en efectivo acreditado para presentar la REF. OYL / 25041238013/02. Esto proviene del premio total de US $ 80,400,000.00 compartido entre los diecisiete ganadores internacionales en esta categoría. Todos los participantes fueron seleccionados a través de un sistema de votación por computadora elaborado con 25,000 nombres de Australia, Nueva Zelanda, América, Europa, América del Norte, África y Asia como parte del Programa de Promociones Internacionales, que se realiza anualmente.

Para obtener más detalles sobre el procesamiento y el envío de su premio en dinero, contácteme.

Recuerde que todo el dinero del premio debe ser reclamado antes del 8 de abril de 2020. Después de esta fecha, todos los fondos no reclamados serán etiquetados como no reclamados.

NOTA: Para evitar demoras y complicaciones innecesarias, recuerde citar su referencia y números ganadores en cada una de sus correspondencias con su agente. Además, si se produce algún cambio en su dirección, informe a su agente de reclamos lo antes posible.

Felicitaciones nuevamente de todo nuestro personal y gracias por ser parte de nuestro programa de promociones.

Sinceramente,

Sra. Betty Nwann

PARA LA PROMOCIÓN DE LA LOTERÍA MUNDIAL:
EL DEPARTAMENTO DE LA OFERTA MUNDIAL DE PROMOCIONES DE LOTERÍA POR CORREO ELECTRÓNICO,

nótese bien Cualquier violación de la confidencialidad por parte de los ganadores.
resultará en la descalificación.

¡¡¡FELICITACIONES DE NUEVO !!!!

****

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: 2020.04.17 19:32:39 -04'00'