Alerta de seguridad informática	8FPH21-00408-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Junio de 2021
Última revisión	11 de Junio 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 del Gobierno de Chile (CSIRT de Gobierno), advierte sobre una campaña de phishing que está siendo difundida a través de un correo electrónico que se hace pasar como proveniente de la Microsoft Outlook web app.

El atacante busca persuadir a las personas para utilizar un enlace adjunto en el cuerpo del correo. El mensaje del correo indica al usuario que debe migrar al nuevo portal de Microsoft Outlook 2021, que inicie sesión para completar con la actualización, y que deben migrar dentro de las próximas 24 horas para supuestamente evitar demoras en la entrega del correo.

Al seleccionar el enlace para ver más detalles, las personas son dirigidas a un sitio falso, donde se expone al robo de credenciales.

Observación

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

Indicadores de compromiso

URL sitio falso:
https://tyyyyyyy.000webhostapp[.]com/it/admin/

Asunto:
Re: Bienvenido al nuevo Microsoft Outlook para personal / empleado,

SMTP Sender:
tcszmta01.santosbrasil.com.br

SMTP Host
[200.205.26.46]

Otros antecedentes

Certificado Digital

Fecha Valido	:	10-06-2019
Fecha Término	:	10-07-2021
Emitido	:	RapidSSL RSA CA 2018

Datos Alojamiento

IP	:	[145.14.144.213]
Número de sistema autónomo (AS)	:	204915
Etiqueta del sistema autónomo	:	Hostinger International Limited
País	:	NL
Registrador	:	RIPE NCC

Datos del Dominio

Nombre de dominio	:	000webhostapp[.]com
Creado	:	11-05-2016
Expira	:	11-05-2022
Información del registrador	:	Hostinger, UAB
ID IANA	:	1636
Correo electrónico	:	abuse@hostinger.com
Servidores de nombres	:	dns1.000webhost.com dns2.000webhost.com

Imagen del mensaje

viernes 11-06-2021 8:58

ues < @santosbrasil.com.br>

Re: Bienvenido al nuevo Microsoft Outlook para personal / empleado,

Para ues

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

ADVERTENCIA: REMITENTE EXTERNO

El remitente de este correo, es externo al Ministerio del Interior y Seguridad Publica. Si no tiene certeza de su origen, por seguridad, NO abra archivos adjuntos y NO haga click en enlaces (puede verificar el destino de un enlace, pasando el cursor sobre éste). Ante sospechas o dudas, reporte a la mesa de ayuda.

Bienvenido al nuevo Microsoft Outlook para personal / empleado,

Se espera que todo el personal / empleado migre al nuevo portal web de Microsoft Outlook 2021 para habilitar el acceso. Haga clic en Iniciar sesión aquí e inicie sesión para migrar inmediatamente y completar la actualización:

· Accede al nuevo directorio de personal

· Accede a tus nóminas y P60

· Actualiza tu foto de identificación

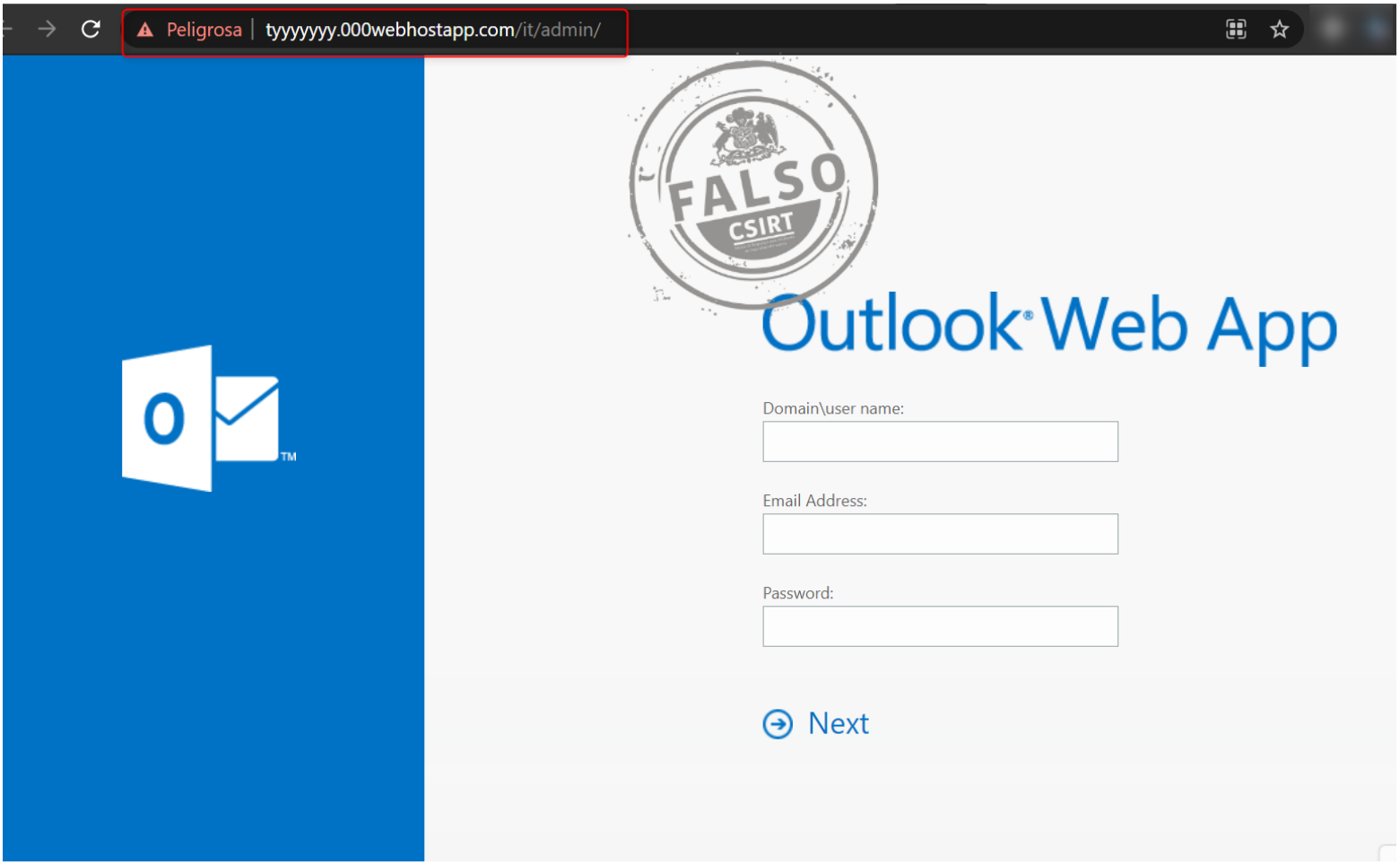
· Flexibilidad de calendario y correo electrónico

· Conecte el número de teléfono móvil al correo electrónico para el correo de voz

Aviso importante: Se espera que todo el personal / empleado migre dentro de las 24 horas para evitar demoras en la entrega del correo.

En nombre de Soporte de TI. Esta es una cuenta de correo electrónico grupal y ha sido monitoreada las 24 horas del día, los 7 días de la semana, por lo tanto, no ignore esta notificación, ya que es muy obligatoria.

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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.06.11 19:15:10 -04'00'