Alerta de seguridad informática	8FPH21-00415-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	01 de Julio de 2021
Última revisión	01 de Julio 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 se está difundiendo a través de correo electrónico, los que se hacen pasar como provenientes del equipo de administración de la institución a la cual llegan.

El atacante busca persuadir a las víctimas de utilizar un enlace adjunto en el cuerpo del correo. Para ello, el mensaje del correo indica al usuario que “Se espera que todo el personal migre al nuevo portal web de Microsoft Outlook de 2021 y se espera que todo el personal migre en un plazo de 24 horas para evitar retrasos en la entrega del correo”.

Al seleccionar el enlace para ver más detalles, el usuario es dirigido a un sitio falso donde se exponen al robo de sus credenciales.

Observación

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

Indicadores de compromiso

URL sitio falso:
http://webmail-000000.moonfruit[.]com/

Asunto:
migrar al nuevo Microsoft Outlook 2021

SMTP Sender:
taslima.islam@insidehighered[.]com

SMTP Host
[40.107.101.76]

Otros antecedentes

Certificado Digital

Fecha Valido	:	NO APLICA
Fecha Término	:	NO APLICA
Emitido	:	NO APLICA

Datos Alojamiento

IP	:	[34.255.56.68]
Número de sistema autónomo (AS)	:	16509
Etiqueta del sistema autónomo	:	AMAZON-02
País	:	IE
Registrador	:	RIPE NCC

Datos del Dominio

Nombre de dominio	:	moonfruit[.]com
Creado	:	10-09-1999
Expira	:	10-09-2021
Información del registrador	:	GANDI SAS Gandi SAS
ID IANA	:	81
Correo electrónico	:	abuse@support.gandi.net
Servidores de nombres	:	ns-1176.awsdns-19.org ns-1819.awsdns-35.co.uk ns-78.awsdns-09.com ns-897.awsdns-48.net

Imagen del mensaje

Taslima Islam <taslima.islam@insidehighered.com>

migrar al nuevo Microsoft Outlook 2021

Para [redacted]@uc.cl

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.

FALSO CSIRT

Para: Todo el personal,

Se espera que todo el personal migre al nuevo portal web de Microsoft Outlook de 2021 para acceder a lo siguiente. Haga clic aquí para migrar:

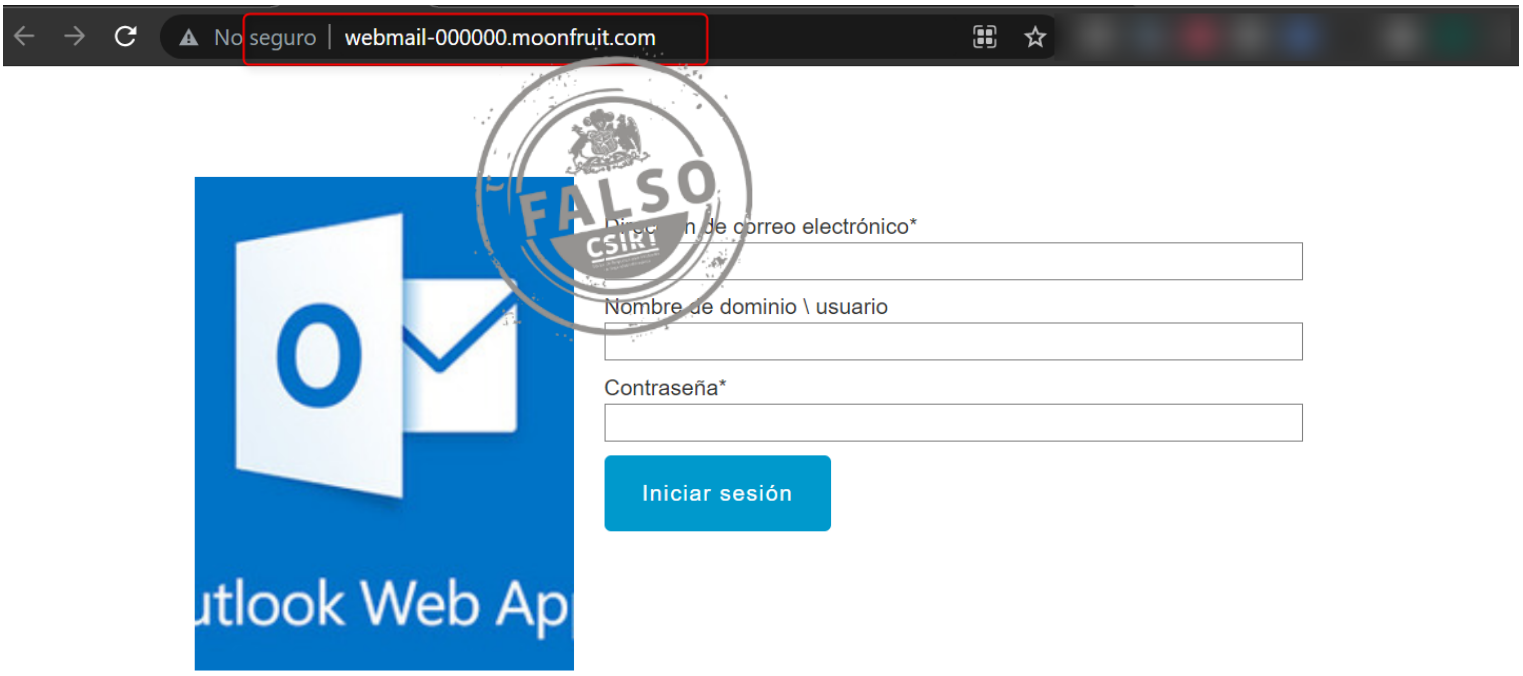
· Accede al nuevo directorio de personal
· Accede a tus nóminas y P60
· Actualiza tu foto de identificación
· Flexibilidad de correo electrónico y calendario
· Conecte el número de teléfono móvil al correo electrónico para el correo de voz

Aviso importante: se espera que todo el personal migre en un plazo de 24 horas para evitar retrasos 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, porque es muy obligatoria.

Atentamente.
Equipo de administración.

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: 2021.07.01 15:40:19 -04'00'