Alerta de seguridad informática	8FPH22-00599-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Septiembre de 2022
Última revisión	23 de Septiembre de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del CSIRT de Gobierno. 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 de Gobierno) ha identificado una nueva campaña de phishing vía correo electrónico.

En esta campaña, los delincuentes indican falsamente a la víctima lo siguiente: *"Fallo en la sincronización de los correos pendientes de su buzón. El servidor de correo ha bloqueado 7 mensajes entrantes. A partir del 20 de septiembre de 2022 (UTC), tiene 7 mensajes entrantes pendientes"*.

De abrir el enlace, la persona es dirigida a un sitio falso, semejante a uno de inicio de sesión de correo electrónico, donde se expone al robo de su usuario y contraseña (credenciales).

Observación

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

Indicadores de compromiso

URL redirección:

http://w1.nimh.gov.vn/zrr/fx/?email=(correo)

URL sitio falso:

http://w1.nimh.gov.vn/zrr/fx/?email=(correo)

Asunto	Correo de Salida	SMTP Host
Your mailbox Pending Emails Sync Failure (interior.gob.cl MAIL-SERVER)	chiefaccountant@newportdisplay.com	[45.137.22.123]

Otros antecedentes

Certificado Digital

Fecha Valido	N/A
Fecha Término	N/A
Emitido	N/A

Datos Alojamiento y Dominio

IP	[103.124.92.130]
Número de sistema autónomo (AS) IP	131353
Emitido Etiqueta del sistema autónomo IP	NhanHoa Software company
Registrador IP	APNIC
País IP	VN
Dominio	nimh.gov.vn
Registrador Dominio	taken

Imagen del mensaje

Your mailbox Pending Emails Sync Failure.
Mail-Server Blocked 7 incoming messages .
As of September 20th 2022 (UTC), you have **7** incoming pending messages.

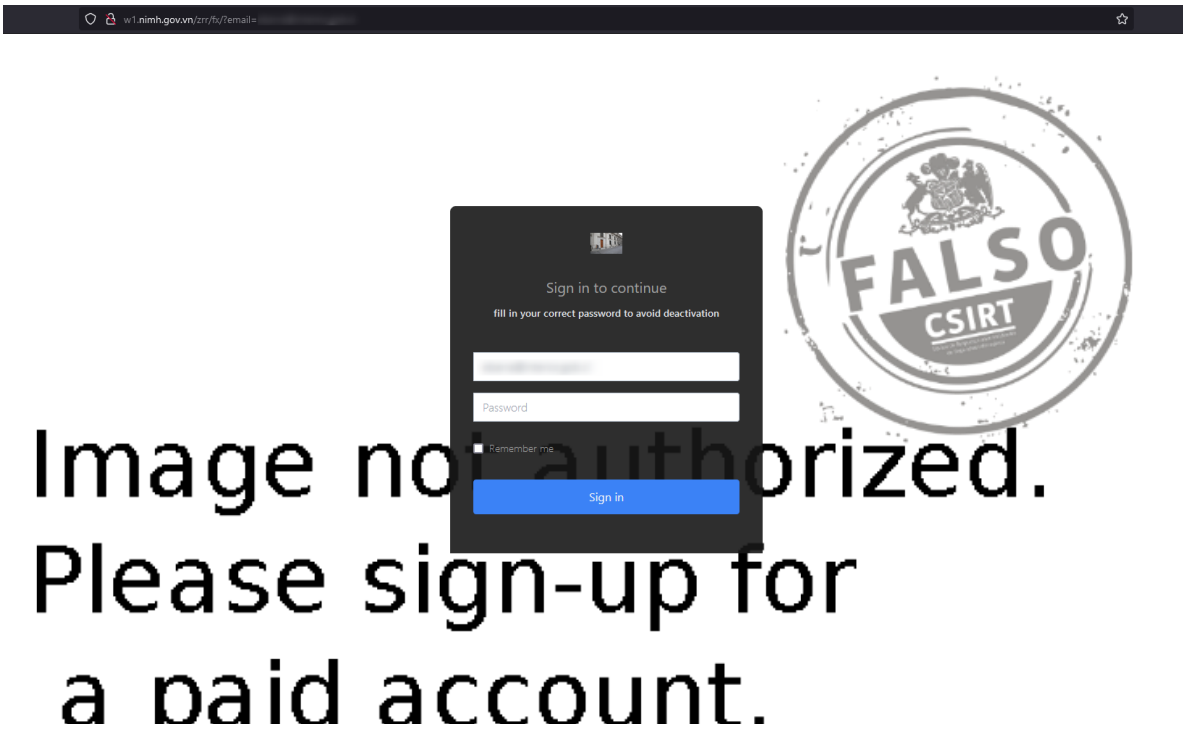
Click to View, Release or Delete pending e-mail messages.
Mail account:

[redacted]

Thanks,
interior.gob.cl Mail System Administrator

This notification was sent to ebarra@interior.gob.cl; Don't want occasional updates about subscription preferences and friendly suggestions?

Imagen del sitio



w1.nimh.gov.vn/zrr/fix/?email=[redacted]

Sign in to continue
fill in your correct password to avoid deactivation

[redacted]
Password
Remember me
Sign in

Image not authorized.
Please sign-up for
a paid account.

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: 2022.09.23 14:17:25 -03'00'