DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°192**	**Fecha: 16-08-2023**
		Página: 7 de 16

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nueva campaña de correo electrónico de Phishing suplanta a entidades públicas del Estado		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

El Equipo de Trabajo de Seguridad Digital de la DINI, ha detectado una nueva campaña de correo electrónico de Phishing que suplanta al Ministerio de Economía y Finanzas (MEF) y Ministerio de Transporte y Comunicaciones (MTC). El actor de amenazas utiliza como señuelo una presunta validación de correo electrónico por un cambio de versión en los servidores de correo de la entidad. El objetivo principal es obtener las credenciales de acceso a las cuentas de correo de la entidad y la exfiltración de información confidencial.

2. DETALLES:

El vector inicial de esta campaña, es el envío de correo electrónico de Phishing, que suplanta a dos entidades públicas como el MEF y el MTC. Los correos utilizados en esta campaña provienen de dos posibles cuentas de correos que podrían haber sido suplantados: avalencia@mef[.]gob[.]pe y ccasapaico@mtc[.]gob[.]pe.

El actor de amenazas emplea como señuelo, una supuesta validación de correo electrónico por un cambio de versión en los servidores de correo de la entidad, de no hacerlo la cuenta se bloqueará dentro las 24 horas. Para ello, inducen a la víctima para que haga clic en el enlace "**PORTAL DE VALIDACIÓN DE CORREO ELECTRÓNICO"** e inicie sesión.

De: Va[redacted]valencia@mef.gob.pe>
Enviado: miércoles, 16 de agosto de 2023 08:17
Asunto: Estimado usuario de correo electrónico,

Estimado usuario de correo electrónico,

Estamos mejorando nuestros servicios de correo electrónico y seguridad, y por esto dentro de las próximas 24 horas cerraremos todas las cuentas de correo electrónico bajo el servicio de la versión anterior del servidor. Su cuenta de correo electrónico actualmente está utilizando los servicios de la versión anterior del servidor, debe validar su correo electrónico para migrar automáticamente a la última versión del servidor de nuestros servicios para evitar que su cuenta de correo electrónico se desactive dentro de las próximas 24 horas.

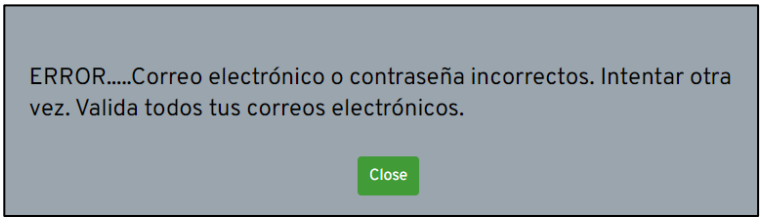
Haga clic en **PORTAL DE VALIDACIÓN DE CORREO ELECTRÓNICO** e inicie sesión en su correo electrónico a través del sitio web de validación emergente para migrar automáticamente a los servicios de la última versión del servidor de correo electrónico para evitar la desactivación de su correo electrónico.

ADMINISTRADOR DE AYUDA.

Seguridad del servicio de correo electrónico.
2023 Todos los derechos reservados.

Si la víctima hace clic en el enlace, será redirigido al sitio web (hxxps://fom.li/f/4g4O3LSYbQ) del atacante, en el cual se le pedirá que ingrese sus credenciales de correo.

Luego de ingresar las credenciales y proceder a la validación, se le mostrará una ventana en la que se le indica, que el correo electrónico o la contraseña ingresada son incorrectas.



Sin embargo, en este punto, el actor de amenazas ya podría obtener las credenciales de inicio de sesión de su víctima.


```
{
    "type": "short",
    "question": "Correo electrónico:",
    "correctAns": "prueba@peru.com",
    "id": "rOYJnX4zhO"
},
{
    "type": "short",
    "question": "Contraseña:",
    "correctAns": "sapoxxxxxxxxxxxxx",
    "
}
```


3. RECOMENDACIONES:

- Maximizar las actividades y medidas de ciberseguridad contempladas en sus directivas internas sobre incidentes de seguridad informática, con el fin de prevenir algún incidente de seguridad que podría afectar los activos críticos digitales de su entidad.
- Evitar abrir archivos adjuntos y hacer clic en enlaces de correos electrónicos no solicitados y poco confiables.
- Evitar ingresar información confidencial en sitios web no seguros (http).
- Contar con una solución de seguridad y mantener permanentemente actualizado el software y aplicaciones.
- Nunca utilizar la cuenta de correo electrónico institucional para el registro en ofertas o promociones por Internet.
- Detectar errores gramaticales en el mensaje. Y, si se trata de un asunto urgente o acerca de una promoción muy atractiva, es muy probable que se trate de un fraude, comunicar al encargado de TI.
- Considerar implementar la autenticación de dos factores para el acceso al correo electrónico corporativo y otros servicios orientados a Internet (incluidos RDP, puertas de enlace VPN-SSL, etc.) que un atacante podría usar para obtener acceso a la infraestructura interna de su entidad y datos críticos para el negocio.
- Asegurar de que todos los puntos finales, tanto en redes de TI como de TO, estén protegidos con una solución de seguridad reciente para puntos finales que esté configurada correctamente y se mantenga actualizada siempre.
- Capacitar permanentemente al personal sobre el manejo adecuado de sus correos electrónicos entrantes de manera segura y para proteger sus sistemas contra el malware que pueden contener los archivos adjuntos de correo electrónico.
- Revisar regularmente las carpetas de correo no deseado y luego vaciarlas.
- Supervisar la exposición de las cuentas de su organización en la web.
- Considerar el uso de soluciones de espacio aislado diseñadas para probar automáticamente los archivos adjuntos en el tráfico de correo electrónico entrante; asegúrese de que su solución de Sandbox esté configurada para no omitir correos electrónicos de fuentes "confiables", incluidas las organizaciones asociadas y de contacto. Nadie está 100% protegido de un compromiso.

Fuente de Información:	Equipo de Trabajo de Seguridad Digital