CSIRTSALUD-AL-20250829-23

TLP: CLEAR

Incidente Id	23
Fecha del reporte	29/08/2025
Entidad	Todas las entidades del ecosistema digital
Título	Campaña de Phishing dirigida a múltiples entidades del gobierno de Colombia
Herramienta de detección	FortiSIEM
Activo involucrado	Correo electrónico
Tipo de incidente	Phishing
Nivel de riesgo	Crítico

Descripción:

Se ha detectado una campaña de phishing masiva dirigida a múltiples entidades gubernamentales en Colombia. La campaña consiste en correos electrónicos fraudulentos con asuntos que intentan persuadir a los usuarios para que confirmen su cuenta y así evitar su suspensión.

Detalles del evento

Los correos electrónicos se originan desde las direcciones larias@mincit.gov.co y mberrio@mincit.gov.co. Se han identificado dos asuntos principales en estos correos:

- **"Confirmación requerida para evitar que su cuenta sea suspendida de nuestros servicios."**

- **"Confirmación requerida para evitar la suspensión y vulnerabilidad de su cuenta"**

Se han encontrado resultados coincidentes en varias organizaciones. La herramienta de monitoreo FortiSIEM detectó un total de 23 eventos coincidentes en Minsalud, 4 en Supersalud, 4 en Invima, 2 en FPS y 1 en INS.

Análisis:

La campaña utiliza ingeniería social para crear un sentido de urgencia, instando a los destinatarios a tomar medidas inmediatas ("**Confirmación requerida para evitar que su cuenta sea suspendida**"). A pesar de provenir de dominios legítimos del gobierno colombiano, el contenido y la intención de los correos son maliciosos. Este tipo de ataque busca engañar a los usuarios para que revelen credenciales u otra información sensible.

Impacto potencial:

Si los usuarios caen en el engaño, podría resultar en la vulnerabilidad de sus cuentas, lo que podría llevar a un acceso no autorizado a los sistemas y datos de las entidades del gobierno. Esto puede resultar en la filtración de información sensible y comprometer la seguridad de la infraestructura digital del Estado.

Recomendaciones de mitigación:

- **Configurar filtros:** Configurar filtros de contenido que pongan en cuarentena o marquen como sospechosos los mensajes que contengan los asuntos identificados.
- **Escaneo de adjuntos y URLs**: Asegurarse de que el sistema de seguridad de correo electrónico, como FortiSIEM, escanee todos los archivos adjuntos y enlaces web en busca de malware o sitios de phishing conocidos.
- **Capacitación de usuarios**: Iniciar una campaña de concientización urgente para educar al personal de todas las entidades sobre los riesgos del phishing. Incluir sesiones de capacitación sobre cómo identificar correos sospechosos y la importancia de no hacer clic en enlaces o descargar archivos de remitentes desconocidos.
- **Verificación de cuentas**: Informar a los empleados que las solicitudes de "confirmación de cuenta" o "suspensión de servicio" nunca se realizarán a través de correos electrónicos no solicitados. Instruir a los usuarios para que verifiquen cualquier solicitud similar directamente a través de canales oficiales.
- **Autenticación multifactor (MFA)**: Promover la implementación obligatoria de la autenticación multifactor en todas las cuentas de usuario. Esto añade una capa de

seguridad crítica que puede frustrar los intentos de acceso no autorizado, incluso si un atacante obtiene las credenciales de un usuario a través del phishing.

- **Actualización de políticas de seguridad:** Revisar y actualizar las políticas de seguridad para reflejar este tipo de amenazas, asegurando que se apliquen las medidas de protección adecuadas en toda la infraestructura de red.

- **Análisis forense**: Realizar un análisis forense detallado en los sistemas de los usuarios que hayan sido objetivo de estos correos para determinar si alguna cuenta fue comprometida y tomar medidas para mitigar cualquier daño.

Conclusión:

El incidente es una campaña de phishing de alto riesgo que requiere una acción inmediata para mitigar el potencial impacto. La propagación de estos correos a múltiples entidades demuestra la necesidad de una respuesta coordinada para proteger los activos digitales del gobierno.