CSIRTSALUD-AL-20250830-24

TLP: CLEAR

Incidente Id	24
Fecha del reporte	30/08/2025
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 identificado una campaña de phishing sofisticada y dirigida específicamente a funcionarios de diversas entidades del gobierno. Este ataque explota una vulnerabilidad en la forma en que los sistemas de correo corporativo indexan el texto plano, convirtiendo enlaces no clicables en elementos interactivos, lo que facilita el engaño a los usuarios. Los atacantes utilizan URLs dinámicas que varían en cada intento, lo que evade los mecanismos de detección basados en listas negras tradicionales y la clasificación de firewalls perimetrales, permitiendo que los correos maliciosos lleguen a las bandejas de entrada de los usuarios.

Detalles del evento

Durante el análisis de seguridad, se observó que los correos electrónicos maliciosos se originan desde las direcciones comprometidas larias@mincit.gov.co y mberrio@mincit.gov.co. Los asuntos principales utilizados en esta campaña son:

- "Confirmación requerida para evitar que su cuenta sea suspendida de nuestros servicios."
- "Confirmación requerida para evitar la suspensión y vulnerabilidad de su cuenta."

Las URLs de phishing detectadas incluyen variaciones como:

confirmar-cuenta-29a.weebly.com
weebly.com/co
confirmar-cuenta-29m.weebly.com

Al hacer clic en estos enlaces, los usuarios son redirigidos a páginas fraudulentas diseñadas para la captura de credenciales u otra información sensible.

Análisis:

La campaña de phishing se caracteriza por su evasión de los controles de seguridad existentes. Los firewalls perimetrales han clasificado erróneamente los enlaces maliciosos en categorías benignas como "shopping" o "information technology". Esta clasificación incorrecta impide que se disparen las alertas de seguridad y que los enlaces sean bloqueados automáticamente, lo que reduce la efectividad de los controles de seguridad y permite que el ataque progrese.

Además, se ha observado una propagación interna del ataque mediante el reenvío de correos comprometidos entre funcionarios. Este comportamiento incrementa significativamente el riesgo de escalamiento del incidente y la potencial exfiltración de datos sensibles de las organizaciones afectadas.

Impacto potencial:

El impacto potencial de este ataque es grave y multifacético:

- **Compromiso de Credenciales:** La principal amenaza es la captura de credenciales de acceso, lo que podría llevar a la toma de control de cuentas de correo electrónico y otros sistemas internos.

- **Exfiltración de Información Sensible:** Con credenciales comprometidas, los atacantes podrían acceder a información confidencial, datos personales de funcionarios y ciudadanos, y otra propiedad intelectual del gobierno.

- **Pérdida de Confianza:** Un incidente de esta magnitud podría erosionar la confianza pública en la seguridad de los sistemas gubernamentales.

- **Interrupción de Operaciones:** El acceso no autorizado y la manipulación de sistemas podrían causar interrupciones significativas en las operaciones gubernamentales.

- **Propagación de Malware:** Aunque no se ha detectado en este análisis, el compromiso inicial a través de phishing podría ser un vector para la inyección de malware más sofisticado.

Recomendaciones de mitigación:

Para mitigar los riesgos y fortalecer la postura de seguridad ante ataques de este tipo, se emiten las siguientes recomendaciones urgentes:

1. **Bloqueo Explícito de Direcciones Maliciosas:**
    - Implementar el bloqueo explícito e inmediato de las direcciones maliciosas detectadas (ej. confirmar-cuenta-*.weebly.com, weebly.com/co) en los firewalls perimetrales, proxys y sistemas de filtrado DNS corporativos de todas las entidades.
    - Considerar el bloqueo de todo el dominio weebly.com si no es crítico para las operaciones legítimas.

2. **Políticas de Inspección de Contenido en Correo Electrónico:**
    - Configurar políticas de inspección de contenido en el correo electrónico que impidan la conversión automática de texto plano en enlaces clicables, reduciendo así la superficie de ataque para este tipo de vulnerabilidad.
    - Reforzar las políticas de filtrado de adjuntos y enlaces sospechosos.

3. **Detección y Bloqueo Dinámico de URLs Sospechosas:**
    - Habilitar mecanismos de detección y bloqueo dinámico de URLs sospechosas mediante integraciones con feeds de inteligencia de amenazas (TI) que actualicen automáticamente los dominios emergentes asociados a campañas de phishing.

4. **Campaña de Concienciación y Capacitación a Usuarios:**
    - Realizar una campaña de concienciación interna urgente y continua para advertir a los usuarios sobre la aparición de enlaces que aparentan ser legítimos.
    - Recordar las prácticas seguras para la validación de direcciones web (ej. pasar el cursor sobre el enlace sin hacer clic para ver la URL real, verificar la autenticidad del remitente, nunca ingresar credenciales a través de enlaces en correos electrónicos).

5. **Revisión y Refuerzo de Configuraciones de Correo Corporativo:**
    - Revisar y reforzar las configuraciones del sistema de correo corporativo (Microsoft Exchange, Office 365, Google Workspace, etc.) para habilitar u optimizar los filtros de protección contra phishing, adjuntos maliciosos y enlaces sospechosos (ej. ATP/Defender for Office 365, sandbox de URLs).

6. **Implementación de Reglas de Detección en SIEM/EDR:**
    - Implementar reglas de detección específicas en sistemas SIEM (Security Information and Event Management) y EDR (Endpoint Detection and Response) que identifiquen accesos repetidos a dominios de alto riesgo y la propagación de correos con enlaces dinámicos sospechosos.
    - Asegurar que las alertas generadas por estas reglas sean priorizadas y respondidas rápidamente por los equipos de seguridad.

Conclusión:

Este incidente de phishing subraya la necesidad crítica de una defensa en profundidad y una estrategia de seguridad proactiva en todas las entidades gubernamentales. La sofisticación del ataque, que incluye la evasión de controles perimetrales y la explotación de vulnerabilidades en el manejo de correos, demuestra que los cibercriminales están adaptándose constantemente. La rápida implementación de las recomendaciones proporcionadas, combinada con una capacitación constante de los usuarios, es fundamental para mitigar la amenaza actual y fortalecer la resiliencia general de la infraestructura digital del gobierno contra futuros ataques. La colaboración entre las entidades es igualmente crucial para

compartir inteligencia de amenazas y coordinar respuestas efectivas. La seguridad digital es una responsabilidad compartida que requiere vigilancia continua y acción concertada.