Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CAMPAÑA DE PHISHING AVANZADA UTILIZA GOOGLE SITES Y FIRMAS DKIM PARA ROBAR CREDENCIALES

23/ 04 / 2025

CONTENIDO

INTRODUCCIÓN

En el mundo de la ciberseguridad, los atacantes no descansan, y la reciente campaña de phishing que utiliza la infraestructura de Google lo demuestra con claridad. Se trata de un ataque altamente sofisticado que emplea una técnica conocida como DKIM Replay, la cual permite a los delincuentes reenviar correos legítimos generados por Google sin alterar su firma digital. Esta táctica, combinada con el uso de Google Sites para alojar páginas falsas que imitan el entorno de inicio de sesión de Google, ha dado lugar a una operación engañosa extremadamente convincente. Los mensajes llegan a las víctimas sin alertas de seguridad visibles, superando con éxito los filtros tradicionales de autenticación como SPF, DKIM y DMARC. El objetivo final es robar credenciales de acceso mediante ingeniería social y suplantación visual. Este incidente expone cómo los atacantes explotan servicios legítimos para aumentar la efectividad de sus campañas y burlar los controles de seguridad. Ante este panorama, es crucial que las organizaciones refuercen sus mecanismos de protección y capaciten a sus usuarios para identificar estos nuevos vectores de amenaza. La adopción de autenticación multifactor y la verificación constante de URLs son prácticas esenciales en la defensa contra este tipo de ataques.

CAMPAÑA DE PHISHING AVANZADA UTILIZA GOOGLE SITES Y FIRMAS DKIM PARA ROBAR CREDENCIALES

A continuación, se encuentra en cuadro de identificación de la amenaza.

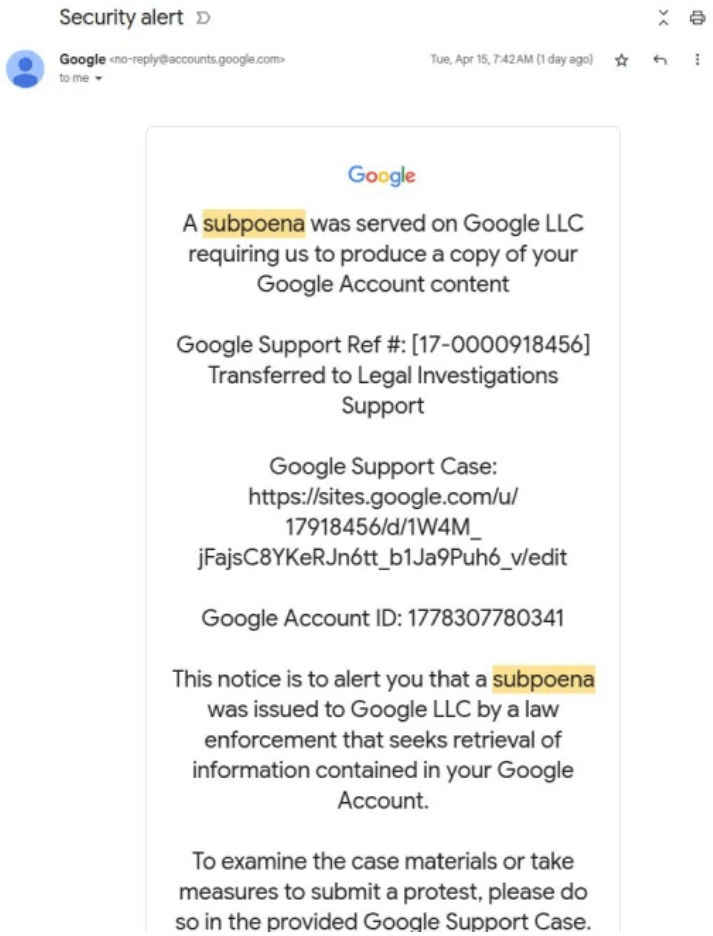
ID de alerta:	DSOC-CERT_2025_04_23_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	23/04/2025
Es día cero (0 day):	No

RESUMEN

Una nueva y sofisticada campaña de phishing ha sido detectada recientemente, utilizando técnicas avanzadas que permiten a los atacantes enviar correos electrónicos aparentemente legítimos desde direcciones vinculadas a Google, engañando incluso a los filtros de seguridad más robustos.
Los ciberdelincuentes han logrado explotar Google Sites —una herramienta antigua de creación de páginas web— y mecanismos de firma de correos DKIM (DomainKeys Identified Mail) para distribuir enlaces maliciosos. Estos redirigen a los usuarios a sitios falsos diseñados para robar credenciales, todo mientras aparentan provenir directamente de Google.

¿Cómo funciona el ataque?

El ataque comienza con un correo electrónico enviado desde la dirección **no-reply@google.com**, firmada correctamente mediante DKIM, lo que permite que supere filtros como SPF, DKIM y DMARC sin generar alertas. La víctima ve el mensaje como una notificación oficial de Google, informándole sobre una supuesta citación legal con enlaces a documentos relacionados alojados en un dominio de Google Sites.



El sitio al que se accede simula ser una página de soporte de Google, ofreciendo botones para “ver el caso” o “subir documentos adicionales”. Al hacer clic, el usuario es redirigido a una réplica del inicio de sesión

de Google, cuidadosamente alojada también en Google Sites. La plataforma permite la ejecución de scripts personalizados, lo que facilita la creación de sitios de suplantación sin necesidad de conocimientos técnicos avanzados.

Ingeniería social y manipulación técnica
Uno de los aspectos más astutos del ataque es su manipulación de los encabezados del correo. Aunque fue reenviado a través de un servidor SMTP personalizado desde una dirección de Outlook, la firma DKIM permanece intacta. De esta forma, el mensaje pasa los controles de autenticación sin levantar sospechas, ingresando a la bandeja de entrada del usuario como si fuera una notificación de seguridad legítima de Google.

Además, los atacantes aprovechan un detalle visual de Gmail: al nombrar su cuenta como “me@”, el cliente de correo muestra el mensaje como si hubiera sido enviado a “me”, reforzando la ilusión de legitimidad.

Medidas de contención y prevención
Google ya ha implementado medidas para bloquear este vector de ataque y ha reiterado que nunca solicita contraseñas, códigos de autenticación o credenciales directamente por correo electrónico.
Como recomendación, se insta a los usuarios a:

- Habilitar autenticación de dos factores (2FA) o passkeys.
- Evitar hacer clic en enlaces sospechosos, aunque aparenten ser de Google.
- Verificar siempre la URL antes de ingresar credenciales.
- Utilizar soluciones avanzadas de filtrado de correos electrónicos en sus entornos empresariales.
- Concientizar a los equipos mediante simulaciones de phishing y capacitaciones continuas.

Tendencia preocupante: Phishing mediante archivos SVG
Este incidente se suma al incremento de campañas de phishing que utilizan archivos adjuntos en formato SVG para ejecutar código HTML malicioso y redirigir a los usuarios a formularios falsos de inicio de sesión, especialmente imitaciones de servicios de Microsoft o Google Voice.

El uso de SVGs se ha popularizado entre los atacantes por su capacidad para contener código JavaScript y HTML incrustado, lo que permite una evasión eficaz de filtros tradicionales y soluciones antivirus que no analizan profundamente este tipo de archivos.

NOTICIA COMPLETA

https://devel.group/blog/una-falla-critica-pone-en-riesgo-la-seguridad-de-fortiswitch/

CONTACTOS DE SOPORTE

Correo electrónico: soporte@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group/