Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

AXIOS Y KITS SALTY 2FA IMPULSAN ATAQUES AVANZADOS DE PHISHING EN MICROSOFT 365

12/ 09 / 2025

CONTENIDO

INTRODUCCIÓN

En los últimos meses, las campañas de phishing dirigidas a entornos corporativos han alcanzado un nuevo nivel de sofisticación. Investigadores han detectado el uso combinado de Axios, una herramienta legítima de desarrollo, junto con la función Direct Send de Microsoft 365, lo que ha permitido a los atacantes crear flujos de ataque capaces de evadir controles tradicionales y comprometer cuentas a gran escala. Estos métodos, además de aprovechar servicios confiables como Google Firebase, han elevado la tasa de éxito de los ataques hasta un 70%, representando una amenaza crítica para organizaciones de distintos sectores.

Paralelamente, la aparición de kits de phishing como servicio (PhaaS) —en particular Salty 2FA— demuestra cómo los ciberdelincuentes están imitando el nivel de planificación de las empresas legítimas. Este tipo de herramientas permite eludir múltiples métodos de autenticación multifactor y personalizar los ataques según el dominio de la víctima, incrementando la efectividad del engaño. La convergencia de estas técnicas subraya un panorama en el que los ataques ya no se limitan a correos fraudulentos básicos, sino que se transforman en operaciones avanzadas con impacto directo en la continuidad y seguridad de los negocios.

AXIOS Y KITS SALTY 2FA IMPULSAN ATAQUES AVANZADOS DE PHISHING EN MICROSOFT 365

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

ID de alerta:	DSOC-CERT_2025_09_12_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	12/09/2025
Es día cero (0 day):	No

RESUMEN

Un nuevo nivel en campañas de phishing corporativo

Investigadores de ciberseguridad han identificado un incremento alarmante en campañas de phishing dirigidas a entornos Microsoft 365, donde los atacantes están combinando el abuso de Axios —una librería popular de cliente HTTP— con la función legítima Direct Send de Microsoft. Esta técnica les ha permitido diseñar un "canal de ataque altamente eficiente" capaz de evadir controles de seguridad tradicionales y llegar de forma masiva a las bandejas de entrada de los usuarios.

Axios y Direct Send: combinación peligrosa

Axios, ampliamente utilizado en entornos de desarrollo, está siendo explotado para interceptar, modificar y reenviar solicitudes HTTP, lo que facilita la captura de tokens de sesión y códigos de autenticación multifactor (MFA) en tiempo real. ReliaQuest reporta que, al combinar esta herramienta con la función de Direct Send, los atacantes alcanzaron hasta un 70% de efectividad en campañas recientes, superando ampliamente otras técnicas de phishing.

Ingeniería social con códigos QR y plataformas confiables

Las campañas observadas utilizan señuelos relacionados con compensaciones económicas para inducir a los usuarios a abrir archivos PDF con códigos QR maliciosos. Estos, al ser escaneados, redirigen a páginas falsas de inicio de sesión de Microsoft Outlook alojadas en Google Firebase, aprovechando la reputación de la plataforma para evadir filtros. Con ello, los atacantes no solo buscan credenciales, sino también integrarse en los flujos legítimos de autenticación empresarial.

Salty 2FA: el phishing como servicio (PhaaS)

A la par, se descubrió un nuevo kit de phishing como servicio denominado Salty 2FA, diseñado para evadir múltiples métodos de MFA: SMS, aplicaciones autenticadoras, llamadas telefónicas, notificaciones push, códigos de respaldo e incluso llaves físicas. Este kit eleva la sofisticación de los ataques al incorporar:

- Verificación Cloudflare Turnstile para filtrar herramientas automatizadas.
- Geofencing e IP filtering para bloquear investigadores y proveedores de seguridad.
- Subdominios dinámicos por víctima, dificultando el rastreo.
- Branding dinámico que adapta la apariencia del portal falso según el dominio del correo corporativo de la víctima.

Impacto empresarial y sectores en riesgo

Los ataques inicialmente se dirigieron a ejecutivos de sectores financiero, salud y manufactura, expandiéndose luego a usuarios en general. Paralelamente, campañas similares se han detectado en la industria hotelera, con correos que imitan a plataformas como Expedia Partner Central y Cloudbeds, aprovechando la rutina de reservas y confirmaciones.

Recomendaciones para mitigar el riesgo

Las organizaciones deben reforzar sus defensas adoptando medidas clave:

Restringir o deshabilitar Direct Send si no es estrictamente necesario.

Configurar políticas de anti-spoofing en gateways de correo.

Fortalecer los programas de concienciación en phishing para empleados.

Bloquear dominios y subdominios sospechosos asociados a estas campañas.

Conclusión

La explotación de Axios y kits como Salty 2FA reflejan la evolución de los ciberdelincuentes hacia operaciones de nivel empresarial, capaces de manipular flujos de autenticación y explotar servicios legítimos para maximizar el éxito de sus campañas. La línea entre tráfico legítimo y malicioso se vuelve cada vez más difusa, lo que obliga a las empresas a repensar sus defensas de correo electrónico y autenticación frente a un panorama de amenazas en constante transformación.

NOTICIA COMPLETA

https://devel.group/blog/axios-y-kits-salty-2fa-impulsan-ataques-avanzados-de-phishing-en-microsoft-365/

CONTACTOS DE SOPORTE

Correo electrónico: teamcti@devel.group

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/