Un grupo de amenazas denominado Hazy Hawk ha sido identificado tomando posesión de recursos en la nube dejados sin uso por organizaciones reconocidas, como contenedores de Amazon S3 y puntos finales en Microsoft Azure, valiéndose de configuraciones incorrectas en los registros DNS.

Según Infoblox, los dominios tomados son reutilizados para alojar enlaces que conducen a estafas y malware mediante sistemas de distribución de tráfico (TDS). El grupo también ha tomado control de servicios en la nube como Akamai, Bunny CDN, Cloudflare CDN, GitHub y Netlify.

El hallazgo inicial se produjo cuando Infoblox detectó que el actor de amenazas había tomado varios subdominios relacionados con los CDC en febrero de 2025.

Posteriormente, se descubrió que la misma técnica fue utilizada para comprometer dominios de entidades gubernamentales, universidades de renombre y firmas internacionales como Deloitte, PwC y EY, desde al menos diciembre de 2023.

> *"Quizás lo más sorprendente de Hazy Hawk es que estos dominios vulnerables y difíciles de descubrir, vinculados a organizaciones prestigiosas, no están siendo utilizados para espionaje ni para ciberdelitos de 'alto nivel'"*, afirmaron Jacques Portal y Renée Burton de Infoblox.
>
> *"En cambio, se alimentan del sórdido inframundo del adtech, llevando a las víctimas a una amplia gama de estafas y aplicaciones falsas, y usando notificaciones del navegador para activar procesos que tendrán un impacto persistente."*

El uso de dominios legítimos y confiables permite al grupo disfrazar mejor sus actividades maliciosas, aumentando su visibilidad en los motores de búsqueda y dificultando su detección por herramientas de seguridad.

La técnica central consiste en aprovechar registros CNAME que apuntan a recursos inexistentes. Al registrar estos recursos faltantes, los atacantes toman control del dominio. Esta táctica fue señalada por Guardio a comienzos de 2024 como una vía utilizada para spam y monetización de clics.

Hazy Hawk va más allá: localiza recursos en la nube que han sido abandonados y los reutiliza con fines maliciosos. En ocasiones, emplea redirecciones de URL para dificultar la identificación del recurso comprometido.

> *"Usamos el nombre Hazy Hawk para este actor debido a cómo encuentran y secuestran recursos en la nube que tienen registros DNS CNAME colgantes y luego los usan para distribuir URLs maliciosas. Es posible que el componente de secuestro de dominios se ofrezca como servicio y lo utilice un grupo de actores»,* señaló Infoblox.

Los ataques suelen empezar clonando sitios legítimos en los dominios secuestrados, atrayendo tráfico mediante promesas de contenido para adultos o material pirata. Una vez dentro, las víctimas son redirigidas por un TDS que decide el contenido final.

> *"Hazy Hawk es uno de las decenas de actores de amenazas que rastreamos en el mundo de la publicidad afiliada. Estos actores ganan dinero redirigiendo usuarios hacia contenido malicioso, y fomentan que los visitantes acepten notificaciones push de páginas poco confiables»,* explicó la compañía.

El objetivo es saturar el dispositivo del usuario con notificaciones que llevan a múltiples estafas y software engañoso, e insisten constantemente en habilitar nuevas alertas.

Para mitigar estos riesgos, los propietarios de dominios deben eliminar los registros CNAME de recursos no utilizados. Los usuarios, por su parte, deben rechazar notificaciones push de

sitios desconocidos.

> *"Si bien operadores como Hazy Hawk son responsables del anzuelo inicial, el usuario que hace clic es conducido a un laberinto de adtech dudoso y directamente malicioso. El hecho de que Hazy Hawk invierta tanto esfuerzo en localizar dominios vulnerables y usarlos en operaciones de estafa demuestra que estos programas de afiliación publicitaria son lo suficientemente rentables como para justificarlo,"* concluyó Infoblox.