PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

121-2025-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°121	Fecha: 24-05-2025
		Página: 4 de 6

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Nuevo actor malicioso dedicado al secuestro de recursos cloud no utilizados		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

Los investigadores de ciberseguridad de Infoblox Threat Intelligence han publicado hallazgos críticos sobre una amenaza recientemente identificada, denominada Hazy Hawk, que ha estado secuestrando activamente recursos en la nube olvidados desde al menos diciembre de 2023.

Los investigadores señalaron que este grupo avanzado es conocido por sus tácticas de expertos en DNS y explota las brechas en los registros del Sistema de nombres de dominio (DNS) para redirigir a usuarios de Internet desprevenidos a sitios web fraudulentos y malware.

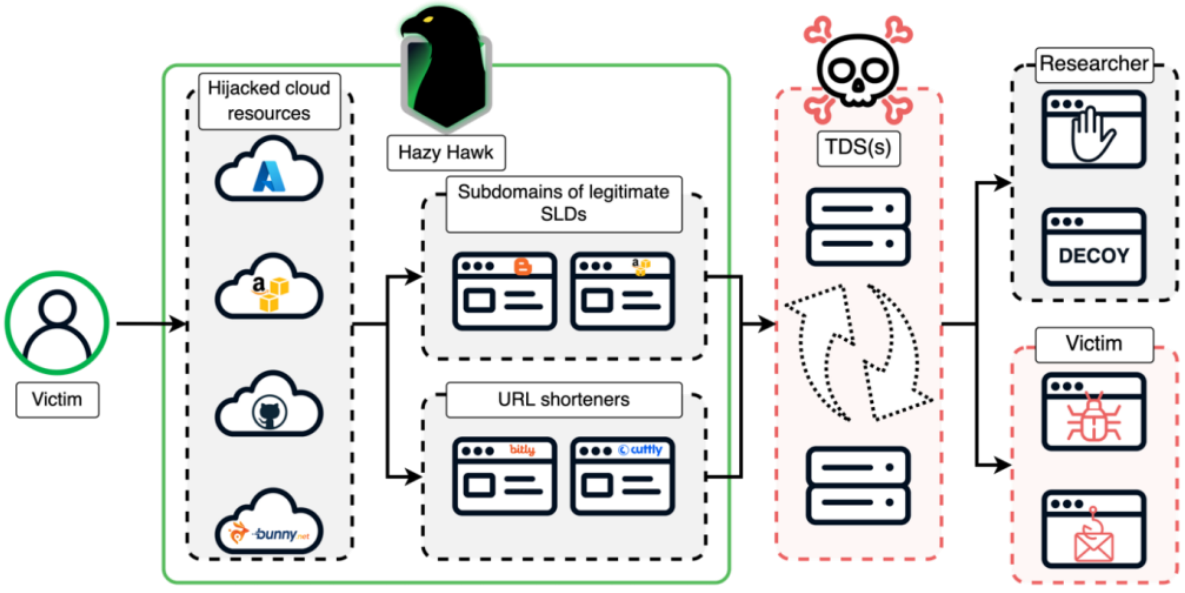
Infoblox detectó por primera vez las actividades de Hazy Hawk en febrero de 2025, cuando el grupo logró controlar subdominios pertenecientes a los Centros para el Control y la Prevención de Enfermedades (CDC) de EE. UU.

Investigaciones posteriores revelaron que agencias gubernamentales globales, incluidas alabama.gov y health.gov.au, importantes universidades como berkeley.eduy ucl.ac.uk, y compañías internacionales como Deloitte.comy PwC.com, también han sido blanco de ataques.

2. DETALLES:

El método de Hazy Hawk consiste en encontrar registros DNS olvidados, que son registros CNAME que apuntan a recursos en la nube abandonados, como buckets de Amazon S3, endpoints de Azure, Akamai, CDN de Cloudflare y GitHub. Registran estos recursos, obtienen el control y los utilizan para alojar numerosas URL maliciosas.

Basta con crear un recurso con el mismo nombre en servicios como Azure o AWS y el redireccionamiento DNS se completa automáticamente. El resultado: URLs aparentemente confiables que redirigen al usuario a trampas cuidadosamente encadenadas con sistemas de distribución de tráfico (TDS), notificaciones push maliciosas y páginas falsas que simulan sitios reales como PBS o incluso Honeywell.



Hazy Hawk emplea diversas tácticas para engañar a sus víctimas, como notificaciones falsas del navegador y aplicaciones fraudulentas, ofuscando URL para ocultar los destinos de los enlaces y reutilizando código de sitios web legítimos para que sus páginas iniciales parezcan fiables.

Estos sistemas están diseñados para maximizar las ganancias de los estafadores y dificultar que los expertos en seguridad rastreen los ataques al cambiar dinámicamente el contenido, lo que lleva a las víctimas a estafas como fraudes de soporte técnico o esquemas de tarjetas de regalo.

Entre las principales características de este actor se encuentran:

- **Uso de técnicas de hijacking altamente sofisticadas:** A diferencia de los actores de secuestro de dominios tradicionales, Hazy Hawk explota configuraciones incorrectas de DNS en la nube, para lo cual necesita tener acceso a servicios DNS pasivos.
- **Impacto a gran escala, geográfico y económico:** Los dominios secuestrados se utilizan para ejecutar campañas de estafas, como anuncios falsos y notificaciones maliciosas, que afectan a millones de usuarios en todo el mundo. Además, las estafas perpetradas utilizando dominios secuestrados por este actor suponen fraudes multimillonarios, especialmente entre determinados segmentos de usuarios.
- **Opacidad:** Hazy Hawk utiliza diferentes métodos de ofuscación, diferentes niveles de defensa para proteger sus operaciones, como son el secuestro de dominios de organizaciones de reputación reconocida, la ofuscación de URLs y el redireccionamiento de tráfico a través de múltiples dominios.

El secuestro de subdominios a través de recursos abandonados en la nube está en aumento. Hazy Hawk aprovecha la circunstancia de que identificar registros DNS vulnerables en la nube es mucho más difícil que identificar dominios no registrados. El gran incremento en la utilización por parte de las empresas de servicios cloud ha provocado que también se haya disparado el número de recursos abandonados que siguen ejecutándose automáticamente.

Esto sucede especialmente en casos en los que las organizaciones no utilizan una solución integral que les proporcione visibilidad y capacidad de gestión de sus activos de TI basados en la nube. Hazy Hawk es el responsable del secuestro de subdominios de diversas organizaciones norteamericanas, agencias gubernamentales, universidades y multinacionales desde diciembre de 2024.

3. RECOMENDACIONES:

- Llevar a cabo revisiones regulares de los registros DNS y eliminar los registros CNAME de DNS cuando se retiren los recursos en la nube.
- Implementar soluciones de DNS protectoras que bloquean el acceso a dominios maliciosos, incluso cuando los actores de amenazas cambian los nombres de los sitios web.
- Establecer capas de seguridad fundamentadas en servicios DNS, basados en inteligencia de seguridad, que impiden a los usuarios el acceso a medios y plataformas falsos.
- Formar a los usuarios para prevenir ser víctimas de fraudes a través de alertas push de sitios desconocidos.

Fuente de Información:	• hxxps://hackread.com/hazy-hawk-attack-abandoned-cloud-assets-since-2023/ • hxxps://www.estamosenlinea.com/2025/05/23/infoblox-identifica-un-nuevo-actor-malicioso-dedicado-al-secuestro-de-recursos-cloud-no-utilizados/?fbclid=IwY2xjawKi1mxleHRuA2FlbQIxMQBicmlkETFGNzhUY21JUUVmZ1ZHcWlHAR755JH5DkIWW4ArQ6VA55i_2hrrIn3RIF49jFyJwWgqlGm32vuZkEC4kCz5iQ_aem_6U0BUZuQCTOsDeNWViY5KA • hxxps://www.ventasdeseguridad.com/novedades/ultimas-noticias/21-empresas/25231-infoblox-detecta-nuevo-actor-malicioso-que-secuestra-recursos-en-la-nube-no-utilizados.html • hxxps://ciberseguridadtic.es/actualidadendpoint/hazy-hawk-el-grupo-que-secuestra-dominios-olvidados-para-propagar-estafas-desde-la-nube-202505269095.htm

Índice alfabético